HOUSE OF LORDS

SELECT COMMITTEE ON COMMUNICATIONS

INQUIRY: CHILDREN AND THE INTERNET

Oral and written evidence

Contents

Anonymous – written evidence (CHI0003)

Looking at the questions the key points I would like to make are:

In general there **remains widespread misunderstanding** and often prejudice around adopted and looked after children. Often they need to be protected from exposure in social media in a way that other children don't, yet the Internet particularly social media seems to have created a society/environment where children can be filmed/photographed and put on social media without their knowledge or that of their families and the majority of people think it is ok.

Most of our friends some of whom work in schools etc. think nothing of posting pictures of their own children with other people's children without permission (even when they have been asked not to) and don't see a problem with it. Yet once a child is 'tagged' on the internet their name is out there. **We have lost the individual right to privacy and this needs to be recognised.**

Even organisations such as schools where policies and procedures are meant to protect the vulnerable, the reality is that social pressure is so great you become a 'problem' child or family if you are concerned about use of photographs and social media sites and your children are excluded from photos often in a way that is very unhelpful, cruel and singles them out further.

A clear message and duty of care in all organisations and for individuals to ensure that children's pictures are not posted on social media is important and would send a clear message. Often the individuals within these organisations haven't got a clear in-depth understanding of the potential for harm that social media and tagging of an individual child poses. This is a specialist area and one that we are gradually learning about by societal mistakes. Professionals who use social media outside their role view it as a norm and are often swept away by social pressures. Often the use of 'closed sites' is explained as a reason not to worry yet the realities of what closed sites mean and how photos can still be accessed and people still tagged are not understood.

Supporting parents with online use – Our school policy about the Internet is based on the children signing to say that they will abide by the rules the school has! This seems to miss the fact that children will push boundaries and again the most vulnerable may suffer. Also it removes the need for adults to be responsible and understand the in depth consequences and risks.

For parents who don't have in-depth knowledge of the internet and how it works (the majority of us) and its potential consequences we have to start using straightforward language and educating in an accessible way. It must be possible to regulate games for children in a way that prevents in game selling and blatant targeting of young minds. The trailers for young children's games are often bloodthirsty and don't seems to match the age group or type of game that is being played. Again often it is not clear to people not highly trained in IT what information is being transferred and where it is going/being used. Often the potential negative effect of games/apps don't seem to be considered and you can get away with sexism etc. in a way that you would not be able to in daily life

in public. Again in schools children are often able to bring in devices with none age appropriate games on and not be challenged when playing with friends for example.

We must find a way of ensuring that children remain able **to understand the difference between gaming and reality** and that risk assessments are done on all IT and social media activity within schools and public places by people who understand ALL the needs of EVERYONE involved and are not swept along by the behaviour of the majority.

People who film others distress or commit assault etc for entertainment reasons need to be arrested and there should be clear consequences for everyone who breaches the privacy of others. It is ironic that our security services have to follow strict guidance about privacy and data protection even when trying to prevent terrorist acts, yet our children can seemingly be filmed anywhere anytime with no respect for their needs and wishes in the use of those pictures.

Also large organisations assume that when children are in a large group then photos can be taken without regulation yet children can often still be identified. People use drone cameras over pools or play areas without any permission etc. We don't seem to be able to go outside the door even in our own gardens without a camera and pictures posted and this has altered the environment considerably especially for the most vulnerable.

I welcome your review, especially as an adopted mum who is constantly having to speak to schools and voluntary organisations about photos and social media, I am really concerned that in this time of austerity and limited resources we are pushing ahead and encouraging things like Amazon delivering through drones in half an hour it is very worrying. Also we all need to understand where our data is held and who by and the potential for huge mistakes to be made. We need publicity campaigns to make people think about the potential risks and consequences as things feel they are spiralling out of control. (On a wider point we have to understand the vulnerabilities of our infrastructure including banking/healthcare etc shoehorning people into computer systems and putting everything online has made us extremely vulnerable and I am sure/hope we are recognising this in government and looking at contingency plans).

Neurobiologically children need interaction and stimulation and an understanding of how to build relationships and gain a sense of 'self'. Especially in traumatised children this is especially important. It is imperative that we look at research into the effects of the online opportunities especially where they are unregulated and how this impacts on the development and parenting of our children and ultimately the health of the nation.

There are really large questions which need to be considered and debated which will impact on our children - Is 'Twitter' for example really a good way of gauging public mood, how many people does it really represent? Do we really want societal decisions based on short sound bytes that may or may not be understood in the context they were meant etc.....Social Media has the potential to mobilise people in a 'mob' like way as well as a positive way and also lives are 'on show' minute to minute and potentially judged harshly

especially for people in reduced circumstances, we need to help children understand the alternatives and try and keep things in a healthy perspective.

How can we ensure people can feedback what may be seen as a minority view without being attacked and demonised, what is the true effect of social media on democracy and gaining a balanced view and how to we maintain a structure that supports all opinions not just those with access to a computer/phone etc. who shout the loudest?

How do we ensure that we have Freedom to Act but also that we consider the consequences that may be detrimental and try and prevent them, especially if they impact of others, the environment etc.

Connection, technology and innovation are really important, but understanding of the consequences and being honest about our limitations is important too, the internet has developed in a way that hasn't enabled us to understand and legislate for the consequences. Who knows what our future holds but we must think about the consequences of technology as well as its benefits in an open and honest way which is why your review is welcome. I am not anti-progress but I object to albeit often unintentional harm being done to the most vulnerable through lack of consideration and majority pressure.

26 July 2016

Dr Akil Awan and Dr Sarah Marsden – oral evidence (QQ 122-128)

Tuesday 22 November 2016

Watch the meeting
Members present: Lord Best (The Chairman); Lord Allen of Kensington; Baroness Benjamin; Baroness Bonham-Carter of Yarnbury; Earl of Caithness; Bishop of Chelmsford; Lord Gilbert of Panteg; Baroness Kidron; Baroness McIntosh of Hudnall; Baroness Quin; Lord Sheikh; Lord Sherbourne of Didsbury.

Evidence Session No. 8 Heard in Public Questions 108 - 128

Examination of Witnesses

Dr Akil Awan, Associate Professor/Senior Lecturer in Modern History, Political Violence and Terrorism, Royal Holloway, University of London, and Dr Sarah Marsden, Lecturer in Radicalisation and Protest in a Digital Age, Lancaster University.

Q122 **The Chairman:** Dr Akil Awan and Dr Sarah Marsden, you are both very welcome. We are sorry to have held you back for 20 minutes, but we were having a very important discussion. If I may, I will ask you to introduce yourselves as we move on to the issue of radicalisation through the internet. Perhaps you would kindly tell us a little about yourselves and make any opening remarks that you wish.

Dr Sarah Marsden: Thank you very much for the invitation to be here. My name is Sarah Marsden. I am a lecturer in radicalisation and protest in a digital age at Lancaster University. Prior to that, I was a lecturer in terrorism studies at the University of St Andrews. I have spent the last 10 years or so researching terrorism and political violence, with a particular focus on engagement with and disengagement from violent extremism and militant Islamism.

Dr Akil Awan: Thank you for the invitation. I am Dr Akil Awan. I am a senior lecturer in modern history, political violence and terrorism at Royal Holloway, University of London. Over the last 10 years I have been looking at radicalisation, social movements, the role of religion and the history of terrorism, broadly speaking. My most recent work involves looking at terrorist propaganda. I also work with the United Nations on youth and radicalism, particularly Security Council Resolution 2250, which is all about youth.

Baroness Quin: This is very much a get-the-ball-rolling question. Thinking about the triggers for radicalisation, are young people more susceptible to being influenced online? If so, why do you think that is?

Dr Akil Awan: The brief answer is yes. To expand that, the internet, in particular social media and web 2.0 platforms, has emerged as the principal arena for youth engagement, politically and socially, over the last decade or so. That is largely a positive thing. It is conducive to egalitarianism and levelling of the field, if you like. There is a slight problem, in the sense that principally it is a function of young people being what are thought of as digital natives, as opposed to digital immigrants. Digital natives are those who are born into the digital world of computers, the internet, video games and that sort of thing. Conversely, the rest of us—I am sorry to point out how incredibly old all of us are—are digital immigrants; we have had to come into that world, sometimes kicking and screaming. We appropriate the language of the digital world, but not in the same way.

For that cohort of young people, any real-world activity, whether it is shopping, playing games, dating, reading or socialising, has a virtual counterpart that might be more appealing. Therefore, it should not be surprising if their political activism or radical escapism also takes place within that sort of arena, so in part it is because of their immersion in that sort of environment.

Baroness Quin: Sarah, do you wish to add anything?

Dr Sarah Marsden: It is important that in my comments I enter the caveat that I am not an expert in child psychology. My comments refer to the literature on radicalisation in respect of the question. The years up to 18 include a lot of variation. There will be a lot of variation in susceptibility and vulnerability along that age continuum.

In general, younger people have less digital literacy and fewer critical consumption skills. They have not necessarily had the opportunity to develop those skills, so the messages they receive may be critically engaged with to a lesser extent than for those who have received training or have had negative experiences. In addition, that period of adolescence, when people seek an understanding of themselves, how they interact with the world and their place in it, brings with it a series of vulnerabilities that are important to bear in mind. I reiterate the point that engagement with the online space can be a really positive thing for political activism and for learning about the world and about political, civic and social questions.

I reiterate the point that young people engage in and experience a lot of things that we might consider risky, but they do not necessarily suffer as a result. There is resilience in most individuals, so it is a case of balancing potential susceptibilities with recognition of the resilience that already exists and the extent to which different people will be affected in different ways.

Q123 **Lord Sheikh:** This subject is of great interest to me. I prepared a report on problems relating to Muslims, which has been sent to the Prime Minister. I also spoke about it in the House of Lords. We are talking about radicalisation online. There are a number of ways in which people are being radicalised, but we will confine ourselves to how things are done online. There are about 3 million Muslims in this country, nearly all of whom are doing well. They are peace-loving people who have

contributed to the advancement and well-being of this country. A lot of them are entrepreneurs like me, some of them are here, some are doctors, and so on, but we have a problem with online radicalisation. I have gone up and down the country and talked to imams. I have addressed meetings in Birmingham and Manchester. Online radicalisation is an issue that crops up.

We are limited by time, so I am going to come to the crux of my questions. First, has the internet allowed for an increase in communication by radical groups? Has that expanded because of what is available on the internet? How do those groups target young people in particular? How do they recruit them? It is not just propaganda from this country but what comes from other countries as well; for example, what happens in Belgium or France. As you very well know, this seems to be an international problem. Those are the points on which I would like information.

Dr Akil Awan: On the increase in communication online, I should point out that the idea of online radicalisation as the most important issue facing us has largely been debunked in academia. There are no real cases of completely autonomous online radicalisation. Children live in online and offline real worlds simultaneously, so in a sense it is pathologising the internet a little bit.

Having said that, one of the paradoxes of the new media environment, broadly speaking, is that we have before us a wealth of information in the form of various languages, various viewpoints and various ideological perspectives. Increasingly, we tend to silo ourselves into the particular viewpoints that seem to corroborate or confirm our world view. We are all guilty of that in our own news media practices. I use the BBC as my touchstone, generally speaking. Therefore, there are spaces online where young people in particular find themselves cocooned, and they end up in a kind of echo chamber. The same sorts of views are reiterated ad nauseam, in effect, without debate, dialogue or challenge. That environment is very conducive if you are trying to bring someone round to a particular way of thinking.

We could add to that the issue of the long tail of the internet. That term is taken from marketing or business, but the idea is that if you are a young person in a community and you hold particular views, or are inclined towards particular views, you will probably not meet someone who shares those views in your school or community. However, online you are far more likely to find someone who corroborates those views and, by some sort of reciprocal legitimation, you end up reinforcing each other's beliefs. That is an issue. Of course, the internet allows you to do that anonymously. If you were to express those views in a community, you would open yourself up to scrutiny from law enforcement, parents and teachers, but also perhaps to ridicule and satire. Online you can be anonymous. We have seen cases of people pretending to be something they are not as well.

Dr Sarah Marsden: I would like to reiterate the first point you made. The scale of the problem is small, in the sense that relatively few people actually move towards violent extremism. Since 2001, maybe 500 people

have been convicted of terrorism offences in the UK. For the under-18s, it is a very small number, about 3%. You are dealing with hundreds, not thousands. That is an important point. When you think about the implications of responding to radicalisation and the online environment, it is very important that proportionality of response is kept front and centre.

In answer to the second point, as for everybody the internet has extended the boundaries by which we can communicate. It increases the number of people we can talk to, the types of people we can talk to and the sorts of views we encounter. Of course, radical groups use that facility for propaganda to promote their particular ideas; they use it to communicate with and to recruit, in an effort to try to bolster their cause, people who are already immersed in extremism or are in a particular radical setting.

Lord Sheikh: How do they establish whom they should target?

Dr Sarah Marsden: If I may just finish the first point, it is important to bear in mind that there is a range of factors in the way radical groups communicate. It is important to bear in mind, too, that the internet is not without constraints for radical groups. There are constraints that operate on them. The capacity for trust in online settings is constrained because you do not know who you are engaging with, and there is a high degree of suspicion that most people are from the CIA or MI5. Alongside that, online venting and communicating in extreme ways might not necessarily move somebody towards violence. It is probably not reasonable to assume that there is a process at work all the time. Availability of messages does not necessarily equate to impact. Just because something is available does not mean it is necessarily having an effect on people. We come across all sorts of media advertising that we do not necessarily engage with.

To respond to the second point, research on this particular issue, which it is fair to say is limited, has identified a range of ways in which people will try to seek out individuals who might be of interest to them and who might be interested in radical ideas. For example, on social media they might hijack particularly popular hashtags and include their own content as a bridge to start communication. They link to other radical accounts that are just this side of legal in order to try to identify a wide number of people who might be interested in their ideas. Where people respond—most obviously do not—there is evidence of an attempt to create what has been described as a micro-community. A huge amount of effort is put into trying to engage with individuals who show some kind of interest. Then there is a move to the offline space, or at least the encrypted space, so that communications can take place out of the public eye. Beyond that, there is an effort to try to move people to action.

Lord Sheikh: How do we combat what is going on? What is your remedy?

Dr Sarah Marsden: I do not have a remedy.

Lord Sheikh: You know we have a problem.

Dr Sarah Marsden: Yes.

Lord Sheikh: For instance, what do you want people like me to do?

Dr Sarah Marsden: First, keep that question of proportionality in mind. Positive responses are far more appropriate than negative ones, in the sense that, rather than taking down content all the time, we should try to develop individuals' digital literacy and critical consumption skills. Find alternative positive ways of engaging in civic and political activism. In my own work, in the effort to support people moving away from extremism who have already been involved in radical settings, it is far more effective to find positive ways of directing that initial motivation to become involved in extremism in the first place. If the motivation is related to group belonging and relatedness, finding alternative ways of supporting that is a really helpful way forward. Similarly, if people are genuinely committed to questions of social justice, finding positive ways of pursuing that seems more appropriate to me than a cat-and-mouse game of taking down content and censoring what is available to people.

Q124 **Lord Allen of Kensington:** Turning to logistics, is the internet being used as an online recruiting opportunity? We have seen press coverage that Daesh published a guide about how to get to Syria, safe houses, flights or whatever. Has the increased use of the internet enabled it to be much easier for people to access logistics information and find data that take young people to conflict areas? If that is the case, is there something practical that we can do to deter them?

Dr Akil Awan: That has certainly been our experience. Sites such as ASKfm, JustPaste.it and many other social media sites are almost catering to the desire to know about how to go about engaging in that sort of thing. If you are searching for flights online and looking at how someone else managed to cross the Turkish border, for example, you have a precedent. Some of that also happens in the real world, in peer networks. Some of the individuals who have gone to Syria come from the very same town, despite not being numerically or in any other way significant.

There is one other thing the internet has allowed, over the last couple of decades at least. Typically, a crime needs both motive and means. The means have become a little easier, in the sense that there is a whole swathe of DIY manuals and all sorts of instructables on the internet that allow individuals to go beyond the idea of visiting a training camp or having real-world training. Often, they are not very good. That is one of the reasons why we have not seen many success stories for wannabe terrorists who follow DIY guides, for example. There are pros and cons as regards the leaderless or lone-wolf-type attacks.

Dr Sarah Marsden: I agree that logistics have become facilitated by the internet. There are barriers to mobilisation, particularly for young people, such as parental oversight, passports and financing it. There are constraints on radical groups about the extent to which they can facilitate it in a practical way. Although there are reports of people receiving money and tickets, there are still limits on the extent to which that is feasible. I agree that the limits of the internet as an instructional tool are significant. The internet is not necessarily a virtual training camp; it is hard to create viable bombs, and we have seen people fail as

a consequence of trying to do so via the internet. Those real-world experiences are vital to the move to violence.

Earl of Caithness: Dr Marsden, to follow up an earlier reply you gave, do you have any evidence that the attempt at radicalisation is increasing or decreasing on the internet?

Dr Sarah Marsden: The short answer is no, I do not have an indication of whether things are increasing or not. There is some evidence that the internet has not necessarily increased violent extremism. The most recent research on that has tracked the relationship between the number of people in the UK or the West who have become involved in violent extremism and the development of the internet. There has not necessarily been a correlation. It is not a case of saying that the internet has caused an increase in terrorism per se. That is probably as far as I would be confident in going.

Q125 **Baroness Benjamin:** You said earlier that the numbers who become radicalised are quite small, but those who do can destroy the lives of many. I am sure you agree that we all need to be vigilant, and to be aware of those who have become radicalised. How engaged is industry, such as the ISPs, search engines and social media platforms, in tackling online extremism?

Dr Akil Awan: There is a range of measures. Of course, we have the take-down policies and the filtering, some of which we heard about today. Some of the social media platforms, such as Twitter, have been very active in taking down hundreds of thousands of accounts. There is always a tension in whether you go in with a heavy hand and take down everything. There is some value in having the presence of those sorts of organisations in public fora in a sense, because they provide intelligence; it also prevents them going underground, in effect.

Another point I want to bring up relates to the recent election in the United States. It is not really about online extremism per se but it is related to that: the circulation of news and stories that are not necessarily extremist per se but are conducive to creating an enabling environment that results in the growth of those sorts of problems. I'm not quite convinced I heard a reassuring answer earlier from the Facebook representative about fact checking. A number of reports have spoken about the effect some of these stories have had on the post-factual era we are now living in. "Post-truth" was voted word of the year by the *Oxford English Dictionary*. We have to be aware of the challenge this now poses for us. If you take a tabloid newspaper, there is still some recourse to the PCC, or IPSO now, but in this case, when a large proportion of individuals are getting their news and form their world view based on completely fabricated stories, what responsibility do social media platforms, which allow those stories to circulate, have in response to them?

Baroness Benjamin: Do you think there is a legal case for taking them to court?

Dr Akil Awan: It is outside my purview, but I do not think so. We need to be a bit more creative about some of the solutions we propose. This is a relatively new problem. We were not talking about it a year ago.

Dr Sarah Marsden: Industry is increasingly engaged. As Dr Awan says, information is taken down; millions of videos have been taken off YouTube; hundreds of thousands of Twitter accounts have been closed down, and so on. They have trusted flaggers who identify inappropriate content, but innovation and thinking creatively is key. Google is doing a little bit in that regard to bolster positive voices. The online civic courage initiative, which has been developed with some think tanks in the UK, has tried to facilitate and support counter-speech—I am not sure whether that was covered earlier because I was not here; it is emboldening people to engage, criticise and debate the ideas people present online.

The effort to try to support that process so that information and ideas are challenged constructively is useful. However, it comes with the caveat that it needs to be done carefully and thoughtfully; it needs to be transparent, because the wider question about industry's engagement with it is the extent to which we wish our online experiences to be manipulated for what are political ends. Who is most appropriate to do that is a really important question. It demands transparency and thought about how we engage with that question appropriately. It is not the same as child sexual exploitation where you can easily take down content. It is a political question. There is a spectrum of political content online, so trying to think about what should be removed, or how it should be engaged with, is a challenge, and transparency sits at the heart of that.

Baroness Benjamin: Do you think filters are effective in stopping extremism? Are they working? How do ISPs effectively detect extremism in a foreign language and in foreign form?

Dr Sarah Marsden: The short answer is that you would probably be wiser to ask Facebook and Google. I do not know the answer to the particular question about language. My understanding is that most of the social media companies rely on community reporting, primarily working on the assumption that people in the community identify content that they think is inappropriate. That is flagged and then reviewed by a human being and taken down. There are trusted flaggers who are part of that process, some of whom are state actors such as the police and so on. I do not know how effective it is. The research on it is nascent. I would be cautious about saying how effective it is, because there are unintended consequences. The move to encrypted spaces, or spaces that are less protected online, is a potential negative consequence. It is also important to bear in mind intelligence gathering and surveillance. There are pros and cons, and, as that question is explored further, it is important to keep a balanced view of both the potential positives and negatives.

Baroness Benjamin: What more could the industry do to monitor and prevent access to extremist material?

Dr Sarah Marsden: It is very difficult. My response tends to sit around developing young people's critical thinking and political consumption skills and their digital literacy so that they are better able to assess and interpret the content they find online. Taking things down and responses that sit more within the censorship space are less desirable than developing resilience in young people.

Dr Akil Awan: I corroborate that. There is a whole host of things we might do that are not necessarily about content but about how young people engage with it. That is the key. We have to think about the role schools play in developing critical thinking and young people's abilities, and teaching them methods and skills so that they can weigh evidence and contextualise the knowledge they receive, and engage with it in a much more sophisticated and nuanced way. That is fundamental. It involves digital literacy and media literacy, too.

There is a whole host of other things that we could do. Perhaps we are entering the schools section. One of the things we are working on at Royal Holloway at the moment is a project about teaching the crusades in schools. The crusades are used quite problematically by a whole swathe of extremists from all sorts of different political and ideological spectrums. The bin Ladens of the world talk about themselves as chivalrous knights fighting against the crusaders. Anders Breivik, the Norwegian terrorist who killed 77 people in 2011, talked about himself as a Knight Templar, a modern-day crusader resisting the incursion of the new Muslim waves. Both of those are reciprocally legitimating in a sense; they work towards the same outcome, which is a very unhelpful thesis on the clash of civilisations. They are in a sense more than the sum of their parts. Young people, as far as I understand it, do not encounter the Crusades. I certainly did not study the Crusades at school. I think that at key stage 3 you have the option of coming across the topic. If you encounter very tendentious, skewed and polarised views of the world, for example about history, you do not have anything to push back on; you have no resource to challenge and contest that in any way. If we were able to teach some of these topics in a much more nuanced way, making them compulsory in part of the curriculum, we would provide students with the tools to be able to push back on some of those things. We would almost be providing some kind of inoculation against very poisonous messages.

Another crucial thing that we might do in schools is promote progressive and inclusive ideas of citizenship, belonging and civic identity. We tend to think that political socialisation begins when children turn 18, but it does not; it is a continuous process. If someone feels that the Iraq war was unjust and carried out for ulterior motives, you might not be able to change their mind cognitively but you might teach them how they might respond. Teach them that there are other ways. Teach them political socialisation and how they might be part of their community and the political process. That can be quite helpful. If you teach those sorts of things at school, you are dealing with some of the problems quite early on.

Q126 **Bishop of Chelmsford:** You anticipated some of the questions I was

going to ask about schools, but what you say is very interesting. It is interesting to me that at a time when religion, often for all the wrong reasons, is driving this conversation and is on the front page of newspapers, in other bits of the world religious literacy, and the more nuanced understanding of the things you are speaking about, is taking such a back seat. Religious education is not part of the national curriculum. We have just heard in the past week that the BBC is further cutting back its profile of religious broadcasting. Aaqil Ahmed has lost his job, and there is now nobody in the BBC with any real knowledge of religion working as a commissioning editor. That question is rather wider than this topic, but it is very relevant to the place of schools in education to help people get a world view that might give them other narratives with which to interpret and deal with some of the stuff they encounter.

Sarah, you may want to say more about the role of schools, and this question is very specific: given that the Government's Prevent strategy places a high responsibility on schools to do something, do you wonder whether schools have ended up being overcautious? Has it gone the other way? I would love to hear your reflections on all of that.

Dr Sarah Marsden: The Prevent duty has certainly presented challenges to schools. One of the primary ones is securing schools' place primarily as a safe space for educating young people. The challenge there is resisting the increasing security agenda being presented to schools as part of their responsibilities. That is not to say that safeguarding does not matter; of course it does. It is not to say that safeguarding is not an important part of a school's role, and extremism is part of that. Front and centre, schools are places for education, the development of thought and young people's well-being and flourishing, and sometimes the security agenda can get in the way of that.

I agree that to some extent, with the Prevent agenda and the demand that schools report people at risk of radicalisation, there is a tendency to be overcautious. We are only at a very early stage of the policy rollout, so the full effects will play out over time, but there is a risk that people will be overcautious and assume that things are problematic when they are not. It takes courage for educators to be conscious of their responsibilities to put education at the heart of all those questions. If somebody is asking difficult questions, that is fundamentally an educational issue, not a security issue first and foremost.

The capacity to resist that demands also that teachers and schools have the training, resources and skills to feel confident about having what are potentially very difficult conversations. That is why it is important that schools remain safe spaces for those difficult conversations. The implication of that is that young people not only develop knowledge about particular historical events—those critical thinking skills are very important—but think about how to engage with difference in an increasingly globalised world, so that we learn and teach how to engage in a robust pluralism. We will not all agree, so how do you engage with young people and enable them to have those difficult conversations with their peers and parents when they do not necessarily agree? It is also about enabling and providing mechanisms and support for young people

to explore those questions and resisting the securitisation of the educational space.

Dr Akil Awan: The Counter-Terrorism and Security Act 2015, which added to the Prevent duty, creates a statutory duty for those in the public sector to prevent radicalisation. Essentially, it puts the onus on them to identify the early signs of radicalisation. It has been quite problematic for all sorts of reasons, particularly for children. There has not been sufficient training of those in the public sector about how they might spot the signs of radicalisation, whatever that might mean. Just before I came, I printed off the Government's vulnerability assessment framework, which is one of the things they use to identify the signs of radicalisation; I want to refer to four that relate to young people in particular. One is being at a transitional time of life; another is a need for identity, meaning and belonging; another is a desire for excitement and adventure; and another is a desire for political or moral change. There are others, but those things could apply not only to every student in this country but to every child on the planet. When there is such a broad swathe of risk factors, or things that might predispose you to recognise a radical, it becomes almost nonsensical.

We have seen a number of referrals under Prevent, and they do not get followed through, because we are talking about false positives. And really what we are doing then, is looking at markers of religiosity, and often ethnic-based, which is one of the reasons why the National Union of Students has refused to implement Prevent. That is the kind of problem that results from that intense focus. It is not very helpful.

As Sarah said, young people need to be allowed to explore ideas, particularly at university. There is now a statutory duty on university lecturers like Sarah and me to report anything that could tick some of those boxes, but universities are supposed to be safe spaces in which you can explore ideas, and make mistakes politically and ideologically. There is the famous adage that if you are not a radical when you are young you have no soul, and if you are still a radical when you are old you have no sense. That is part of our political socialisation. We go through that process as young people.

Q127 **Baroness Kidron:** I was going to raise the issue of Prevent, too. There is one particular criticism I would like both of you to comment on very briefly. I refer to the anxiety that parents are unable to discuss issues at home; it creates the fear that kids will then talk about them in educational institutions and be noticed for that. Have either of you come across that phenomenon? It seems very interesting to me. It came from the UN special rapporteur. The other thing is whether you have any suggestions for government, given that Prevent is somewhat problematic. What would you like to see from government particularly as it relates to young people?

Dr Sarah Marsden: I have seen evidence of the alternative conversation, with parents saying to young people, "Do not discuss these things because you could into trouble". From a Muslim parent's perspective, somebody described it as, "I'm going to have to have that difficult conversation with my 12 or 13 year-old about what not to talk

about publicly", because of those very concerns. That is the challenge. When you introduce security questions in an educational setting, the bonds of trust start to break down, and the extent to which parents and teachers feel confident in their capacity to engage with such issues starts to erode. The more we can do to embolden teachers and parents to engage with these very difficult questions, the better.

More generally on Prevent, it has a chequered history. I still believe that the intention of the policy is a good one. Nobody wants to see people become involved in violent extremism and hurt others. The policy has been hampered by mistakes: weak conceptualisation, poor focus and inappropriate targeting, particularly of communities. I am sure these things are not new to you. There are some good news stories that we do not hear much about. When it comes to practice on the ground on the part of grass-roots actors, youth workers, community activists, police officers and probation officers, although there are examples of poor practice—there is no doubt about that, and mistakes are made in the referral process—there are also some good news stories. There are dedicated people doing some really important work. The challenge is that nobody wants to hear about their work. Equally, because of the security framework that sits around Prevent, nobody wants to tell those stories, because as soon as you are identified as being associated with Prevent it becomes impossible to tell the stories in a way that enables you to continue your work. Essentially, the community loses faith in you as an independent interlocutor within particular spaces. It is exceptionally difficult. The history of Prevent is going to make it hard for it to move forward in a productive way, but that is not to say that its intention is not appropriate and that there are not important things being done at the grass roots that could be celebrated more.

Q128 **Baroness McIntosh of Hudnall:** What has just been said is such an important thing. You say that the policy has its heart in the right place, to paraphrase, but what would you recommend to take forward that policy, or a policy, so that it did not have those slightly toxic connotations? In particular, given what you said about bringing the notion of security into an educational context, can we reverse that, or in your view has it got to the point where we cannot easily do that?

Dr Sarah Marsden: It has become extremely difficult. People have become incredibly entrenched on both sides of the debate. I am trying to think about how the positions in the anti-Prevent lobby could be assuaged or addressed. I do not think it will be at all easy to depoliticise Prevent. One way is to focus on the question of safeguarding and incorporate the strategy more cohesively within the safeguarding framework, so that it is in the list of things that parents and teachers need to take account of, along with child sexual exploitation and other things. More generally, it will be very difficult to rebrand it or rethink it in a meaningful way. I am not sure I have the answer to that question.

The Chairman: Do you, Dr Awan?

Dr Akil Awan: I am not sure I have an answer to that question. I would be making a lot of money if I did. I agree with Sarah in the sense that Prevent starts from a laudable place, but it has become a toxic brand,

particularly among the communities that it really needs to have on board for it to work. That is fundamental. Irrespective of the successes, if you do not have those communities on board—the National Union of Students and many of the major Muslim organisations—I cannot see a way forward.

If I was to give any advice, you need a strong evidentiary basis for whatever you do next. That is fundamental. One of the issues is the focus on ideology being central to violent extremism. Pretty much every study that has been conducted has disproved that or at least says that ideology is not the starting point. People appropriate and imbibe ideologies later on, but if you are talking about how—not why—people become radicalised, peer networks, social networks and spaces and all those sorts of things are far more important.

If we are talking about the narratives of extremist groups, narratives in and of themselves have no power; they have power only when they intersect with real-world issues or circumstances. Someone mentioned France or Belgium earlier. I have done a number of studies on people from France and Belgium who joined ISIS. Some of the propaganda and messages that come from ISIS target the lived experiences of those people. France is a particularly good case study. There is a general antipathy towards Muslims or Islam. There is growing xenophobia, whether that is seen in the rise of the far right, or sartorial restrictions on Muslim women's dress—the burkini ban and that sort of thing. It is really about belonging. If groups are offering a kind of Utopian state with welcoming arms, it can be particularly appealing to young people.

Conversely, if you look at socioeconomic marginalisation, in France Muslims make up about 8% of the population but 70% of the prison population. I can give you examples of a couple of ISIS social media campaigns. One is: why be a loser when you can be a martyr? If you are appealing to someone who is potentially socially, politically and economically marginalised, that is a very powerful message. I am not sure why contesting that message without doing anything to change the structural conditions in which that individual finds himself would have any power at all. Why would it?

We need to think hard about some of the reasons why people become involved in those sorts of groups but we also need to take a look at the evidentiary basis. We do not need to reinvent the wheel. We have been dealing with political violence for a very long time. Before the Islamist threat, we had the Troubles. We have a whole swathe of literature that deals with some of the very rich reasons why people are involved in these groups, and how they disengage afterwards. We should be looking at that rather than basing things on anecdotal evidence, putting forward policies and realising in hindsight that perhaps they were not the best thing.

Lord Sheikh: I want to raise an issue regarding Prevent. I have a strong feeling, talking to the community at every level, that it needs revision. You describe it rightly as toxic. In your studies, how much does the fact that the West is involved in Syria, Iraq or Afghanistan contribute to

people being radicalised? It is not all ideology. What is your feeling about overseas policy?

Dr Akil Awan: To clarify, is your question about the role of foreign policy in radicalisation?

Lord Sheikh: Yes. People see what is happening in Syria or Iraq. How much does it contribute to radicalisation? As you know, the invasion of Iraq went down very badly. How much does that influence people?

Dr Akil Awan: It is very hard to measure something like that. We have to be careful that what we say and what we do match, and that there is no cognitive dissonance between our aspirations and ideals and how we act in the real world. For example, if we engage in military intervention in Iraq and that leads directly to the rise of ISIS, as it did, those two things are related and people recognise that. If we decide, for example, to cut our international development aid, but continue to arm pretty nasty regimes around the world, there is a gap between aspiration and reality. Young people in particular are quite savvy about recognising some of those disconnects. Groups prey on that as well. Groups are very keen to play that out in any number of ways as being an attack on Islam. I mentioned the Crusades earlier. The jihadists of the world talk about the current conflicts as the Zionist crusader alliance. A problematic foreign policy is very easy to package as part of the extremist narrative. No doubt.

Lord Sheikh: But it does influence people.

Dr Akil Awan: It is hard to measure, but yes, of course.

The Chairman: Thank you both. I for one have learned an awful lot from you two. We are very grateful to you. Thank you very much for coming in. It has been an excellent session.

Barnardos – written evidence (CHI0013)

Summary

This response draws on Barnardo's services and expertise in this area and includes the following key points:

- Whilst bringing many benefits, the Internet has also created significant risks for children's welfare – particularly in the propensity for children to be sexually exploited and exposed to inappropriate material that could harm their development.

- Although there is little firm evidence yet, there is cause to be concerned that the internet may be affecting children's neurological development. Even small changes, such as the manner in which job applications have migrated online, appear to be impacting on children's mental health and wellbeing.

- There are growing risks of children's data being misused and they should be helped to exert more control over the use of content they place online.

- There are huge challenges in restricting access to inappropriate content on the internet. Censorship is not a panacea and can only be a part of the solution – adults must help children to manage and process what they see online to avoid adverse consequences. Effective, age appropriate Sex and Relationships Education (SRE) is crucial to helping with this.

- Currently not enough analysis of future technology considers the impact on children. There should be more push towards 'child impact assessments' to be applied to new technologies as they are introduced.

- The potential effects of the Second Machine Age on employment prospects for young people should be considered now, with suggestions being that vocational education should be more greatly prioritised.

- The UK Council for Child Internet Safety (UKCCIS) should be expanded to consider child internet welfare as well as child internet safety.

Questions:

Risks and benefits:

1. What risks and benefits does increased internet usage present to children, with particular regard to:

i. Social development and wellbeing

1.1.1 Barnardo's works directly with vulnerable children, young people, parents and carers in communities around the UK. From this experience we have gathered firm evidence about negative impacts, including for children and young people who have been sexually exploited. Here we are seeing a pattern where the internet and smartphones have enabled perpetrators to more easily access, groom and abuse children. This abuse can happen both offline, when the child meets the abuser after communicating online, and online, through non-contact sexual abuse and the sharing of images. The internet has allowed abusers to take on false personas and become "friends" with young people, earning their trust and luring them into a false sense of security, which creates conditions in which abuse to take place easily. It has also enabled new forms of abuse to develop, such as non-contact abuse.

1.1.2 Research conducted by Barnardo's[1] with practitioners supporting children at risk and victims of sexual exploitation showed that the demographic of those requiring support has changed. While many of the children are still from backgrounds where they are vulnerable to abuse due to being disadvantaged, abused or neglected, children are also now presenting from homes where they have secure attachments to their parents and a protective environment around them. Increased access to the internet – particularly via smartphones – and, commonly, a lack of awareness among parents about their children's online activities, is leaving more young people at risk of forming relationships with abusers online.

1.1.3 Barnardo's also knows from our frontline work that children and young people often view pornography, including extreme pornography, online. Not all children are severely affected by this, but in some cases it can affect a young person's sexual development, and more widely it is felt that this could be changing young people's understanding of sex and relationships. In some cases, the internet is where children first 'learn' about sex, meaning they can attempt to imitate what they have viewed online, which may be extreme and violent. The recent Parliamentary Inquiry into Harmful Sexual Behaviour (HSB), which Barnardo's provided the Secretariat for, highlighted this as a matter of concern in its concluding report *Now I Know It Was Wrong*.[2] Additionally, one Barnardo's service noted that YouTube, but also other sites, are poor

---

1 Palmer, T (2015) *Digital Dangers: the impact of technology on the sexual abuse and exploitation of young people* http://www.barnardos.org.uk/onlineshop/pdf/digital_dangers_report.pdf

2 *Now I Know It Was Wrong* (2015) https://www.barnardos.org.uk/now_i_know_it_was_wrong.pdf

influences for young people who are self-harming or have concerns over their body image.

1.1.4 Finally the internet age may well be impacting children's wellbeing in significant but less tangible ways. For instance Barnardo's services report that online job applications may be contributing to a sense of hopelessness among young job-hunters – as the increased accessibility and ease with which an application can be found and a CV submitted suggests that countless more people are able to apply for substantially more jobs than in a paper-based world. Practically though this means that employers are swamped with applications for many positions – particularly unskilled positions – and most young people are unlikely to even receive a response to the majority of their applications. This is causing demoralisation among many young people seeking employment, even at a time when employment rates are at a record high.

ii. Neurological, cognitive and emotional development

1.2.1 The positive impact of the internet cannot be understated in relation to children being able to have access to information, learn and socialise with friends. However, we are still grasping to fully understand what some of the negative impacts might be. There currently appears to be minimal concrete evidence about how the internet – and social media in particular – may be affecting social development in areas such as attention span, empathy or self esteem, although these are all issues which are raised as of active concern.[3]

1.2.2 An area that warrants further investigation is the impact of the internet – and the decline of offline or 'screen-free' time – on relationships and attachment. We know that strong relationships and secure attachments are the foundation of good mental health, yet it seems inevitable that the nature and quality of relationships between family, friends and partners is changing, as communication moves increasingly online and face-to-face contact diminishes.

1.2.3 Some experts question how worried we should actually be about changes in thinking behaviour created by the internet – pointing to similar concerns throughout history (such as the printing press for example) which have not proved counter to social progress. However, Barnardo's would caution that many of the same commentators conversely also point to the internet as creating unprecedented changes for childhood and

[3] Nicholas Carr's *The Shallows* (2010), for instance, makes a persuasive case for how use of the internet may be rewiring our brains. Sherry Turkle's *Alone Together* (2010), paints a compelling picture of young people being made increasingly anxious and ill at ease in 'real life' social situations as a byproduct of constant connection online. Teachers in particular point to what they see as changing experience of young people's behaviour in classes: https://www.theguardian.com/teacher-network/teacher-blog/2013/mar/11/technology-internet-pupil-attention-teaching

youth – if this is so then it is surely reasonable to be concerned at the potential effects this juncture.[4]

iii. Data security

1.3.1 This is not an area in which Barnardo's specialises, but more generally we would be concerned that as 'big data' becomes a more important part of society – particularly with the Internet of Things – that sufficient thought is given to how young people might be protected from their data being obtained or used without their consent.

1.3.2 In particular Barnardo's is concerned that when young people reach adulthood they should have the ability to 'delete' from the internet aspects of their adolescence which they feel no longer represent them. Although it is now possible to request for search engines to hide certain information, it may be that young people might need specific support to help them to achieve this. This may be a subject on which guidance or training might be helpful for youth professionals working with young people.

2. Which platforms and sites are most popular among children and how do young people use them? Many of the online services used by children are not specifically designed for children. What problems does this present?

2.1 It is important to be aware that more recently the sheer scope of the internet and its ubiquity means that Barnardo's understands that today's children increasingly may not even distinguish 'the internet' as one holistic defined arena that can contrast to physical life. Instead it is believed that increasingly many young people are conceptualising individual platforms such as Facebook, Whatsapp, or Snapchat as different spaces in their life in the way previous generations might have identified 'school', 'scouts' or 'dance class'.

2.2 Given the tendency for children to frequently migrate at speed to new platforms as they emerge and rise and fall in popularity, it is highly unlikely that adults will ever be fully up to date with which websites young people use them. However, Appendix A contains a list of platforms, sites, apps, and games popular with children and young people based on feedback from practitioners in our services.

2.3 There are many problems due to children accessing sites and apps that are not suitable for their age. Apps that enable live broadcasting and the sharing of images can result in children and young people sharing information to strangers, as well as disclosing their location through geo-location. Platforms that enable communicating with strangers online, or are specifically for dating, enable children to build up a 'relationship' with someone, who may not be who they claim to be. Whilst many older

[4] An example of this thinking for instance can be found in John McWhoter's fascinating TED talk about how texting is leading young people to create a whole new syntaxes. https://www.ted.com/talks/john_mcwhorter_txtng_is_killing_language_jk?language=en

children may be aware that someone they meet on the internet could be masquerading as someone else, younger children, or those with special developmental or emotional needs, are more likely to take an internet identity at face value. The recent case of Kayleigh Haywood clearly illustrated how she had met a man through Facebook, was groomed and then agreed to meet him.[5] With younger children increasingly accessing the internet – and social platforms in particular – this issue may become of greater concern going forward.

2.4 As well as being able to communicate through various apps and platforms children and young people are also able to communicate while playing games. While in the majority of the cases those playing games are doing so just for fun, research by Barnardo's on the sexual exploitation of boys and young men[6] found that boys were particularly vulnerable to being groomed online while gaming, such as in the tragic case of Breck Bednar.[7] While the communication during gaming can be problematic, the content of the games can also be inappropriate for young children. While games are age rated there are few controls over who can play them. As noted in Appendix A, one game – *Grand Theft Auto* – has been particularly referenced in referrals to a Barnardo's service dealing with HSB.

2.5 The lack of age - verification in relation to accessing inappropriate platforms and websites (including pornographic websites) enables children to easily access inappropriate content or engage in risky behaviours. Although the industry standard for accessing social media is to require a minimum age of 13, in practice this is not enforced. Much more needs to be done by industry and through domestic and international regulation to translate age restrictions from theory into practice.

3. What are the technical challenges for introducing greater controls on internet usage by children?

3.1 Barnardo's imagines this question will be far better considered by individuals and organisations with greater expertise in this field, and closer proximity to developing technology. However we would make two observations:

- Firstly, most of the current literature by futurologists anticipating the effects of technological advance is not written with a specific narrative about the potential impact on children in mind. This is an issue Barnardo's highlighted in *Youth and the Internet*[8] where we suggested experts in the tech and children's sectors should be brought together more regularly to conduct 'Child Impact Assessments' on tech developments perhaps similar to the way current policies across Government are already subject to Equality Impact Assessments.

---

5 http://www.bbc.co.uk/news/uk-england-leicestershire-36685923

6 https://www.barnardos.org.uk/what_we_do/policy_research_unit/research_and_publications/hidden-in-plain-sight/publication-view.jsp?pid=PUB-2801

7 http://www.bbc.co.uk/newsbeat/article/35364026/breck-bednar-friend-murderer-told-me-hed-killed-him

8 Rallings, J (2015) *Youth And The Internet: a guide for policy makers* https://www.barnardos.org.uk/youth_and_the_internet_report.pdf

- Secondly, finding technical solutions is likely to be problematic as children and young people do not use the internet in a uniform way. As we have seen recently with certain platforms – such as Twitter's Periscope app – what can be a positive means of live streaming to communicate, has been misused by some young people. This will potentially present difficulties. It must be remembered that we are only able to exert limited controls on young people's exposure to the outside world as they grow older – the role of adults is to help children navigate 'real life' as safely as possible, not lock them in a house for fear of the risks it presents. This should also be the principle on which any controls on internet usage should be based.

4. What are the potential future harms and benefits to children from emerging technology, such as Artificial Intelligence, Machine Learning and the Internet of Things?

4.1 The merging of reality and the virtual world, such as in the recently published game *Pokemon Go*, raises concerns about personal safety and young people being brought into contact with strangers they feel they can trust because of a common interest.

4.2 Some of the particular challenges ahead though are likely to arise from the impact that new technologies will have on employment opportunities in the future – particularly as more routine tasks in traditionally 'safe' professions (such as conveyancing law for example) are replicated by machines. Books such as *The Second Machine Age*[9] suggest it is probable that the young people best equipped to survive in this world may well be those with versatile skills cutting across both academic disciplines, such as English and Maths, but also a vocational ability to work *with* machines either through programming or even more directly in partnership than we have previously imagined.[10] It is important that it is considered now how the education system can improve delivery, particularly of vocational disciplines, to reflect what is being suggested about the future world that children and young people are likely to be competing for jobs in. Barnardo's is currently preparing a report on this topic to be published in the autumn, an advance copy of which will be sent to the committee.

5. What roles can schools play in educating and supporting children in relation to the internet? What guidance is provided about the internet to schools and teachers? Is guidance consistently adopted and are there any gaps?

5.1 Schools have a key role in educating their pupils about the internet. While many are now teaching e-safety, this is dependent on the school and is often a one-off session. To ensure all children are given high

9 McAfee, A & Brynjolfsson, E (2014) *The Second Machine Age: work, progress and prosperity in a time of brilliant technologies*

10 For example at a recent seminar on the topic of future tech, Barnardo's staff were able to experience a robot's mimicking their movements from distance just by wearing a Virtual Reality Headset. This raises many interesting questions about the fusion of man and machines in the future economy.

quality, age-appropriate information about the risks associated with the internet, and how to stay safe, the subject should be made compulsory in the school curriculum, both at primary and secondary school. It could be taught within PSHE (or equivalent) and greater emphasis should be placed on internet-related activity within Sex and Relationships Education.

5.2 The latter is because some aspects of taking risks online, such as sexting, are often linked to 'relationships' or when relationships are developing or when young people want to start exploring having sex. Crucially though, safe and responsible use of the internet should be embedded throughout the school curriculum, and of course reflected at home. Online safety and sex and relationships education should include clear information about the consequences of risky behaviour. For example, many young people do not realise that sharing indecent images of themselves or another child under 18 is illegal, even in the context of a consensual relationship.

5.3 With technology constantly evolving, lessons must be up-to-date with emerging trends and e-safety education should be delivered regularly. The recent HSB Inquiry[11] particularly highlighted that specialists should deliver these lessons as they are more likely to elicit the confidence of young people to speak freely than class teachers charged familiar to pupils from other lessons. However, this should not detract from all teachers being trained so they are confident to respond to difficult situations which pupils may approach them with on such topics.

6. Who currently informs parents of risks? What is the role for commercial organisations to teach e-safety to parents? How could parents be better informed about risks?

6.1 Parents are currently informed by voluntary agencies, CEOP and schools, among others, as well as websites such as *Parentzone*. However, there is a not a standard approach and parents often have to find the information out for themselves. It must also be remembered that internet technologies are changing constantly. A pre-requisite of any information going to parents is that remaining up to date is an ongoing task.

6.2 In our report *Digital Dangers*[12] we recommended that commercial companies provide safety information to buyers when they get new phones, tablets, laptops etc. that is easy to access. Providing support online may not always be the best means to get information to parents or guardians as it relies on them accessing specific webpages in the first place. Information that is more easily accessible, such as a leaflet with the purchase might be more effective. Another way that parents could be provided with information is through the same routes as those that are used to get information to parents about the health of their children. This information arrives through the post, and is therefore accessible to parents and does not rely on the adult going online to search.

---

11 *Now I Know It Was Wrong* (2015) https://www.barnardos.org.uk/now_i_know_it_was_wrong.pdf

12 Palmer, T (2015) *Digital Dangers: the impact of technology on the sexual abuse and exploitation of young people* http://www.barnardos.org.uk/onlineshop/pdf/digital_dangers_report.pdf

7. What are the challenges for media companies in providing services that take account of children? How do content provided differentiate their services for children, for example in respect of design?

7.1 As suggested earlier technological development seems often to be conducted in isolation of experts on childhood, which often can lead to a narrow perception of children as 'rational consumers' rather than emerging human beings whose understanding may lead them to misuse internet technology. We would urge that the Government does more to help facilitate communications between media companies and the children's sector perhaps through the existing forum of UK Council for Child Internet Safety (UKCCIS) (see question 12).

8. What voluntary measures have already been put in place by providers of content to protect children? Are these sufficient? If not, what more could be done? Are company guidelines about child safety and rights accessible to parents and other users?

8.1 Most mainstream apps and platforms enable users to block other users or report content. However, this relies on the user reporting inappropriate content, which a young person may not do. Signing up is often reliant on being over 13 years of age, but there are no age-verifications to enable this to happen.

8.2 This is a difficult area to regulate. There is potentially scope for credit cards or similar to offer some form of age-verification which may be helpful in certain circumstances – such as controlling access to pornographic websites. But for social media this may be excessive, and given young people's desire to socialise online may even drive them towards shadier sites with less moderation than platforms such as Facebook etc.

Legislation and regulation

9. What are the regulatory frameworks in different media? Is current legislation adequate in the area of child protection online? Is the law routinely enforced across different media? What, if any, are the gaps? What impact does the legislation and regulation have on the way children and young people experience and use the internet? Should there be more consistent approach?

9.1 It is important that all parties realise that regulation will never be a panacea for the myriad challenges presented to children by the internet. It is tempting to see the proliferation of inappropriate content and/or usage by young people as merely the latest incarnation of an ongoing public debate which has previously taken in 'moral panics' around "Punk Rock", "Video Nasties", or "Gangsta Rap". But that would be to misunderstand the scale of the change which the internet may be bringing to childhood itself – a theme explored in Barnardo's 2015 paper *Youth And*

The Internet.[13] Most importantly this cannot be a matter for censorship policy alone, as much of the inappropriate material being created nowadays is instant and user-generated often by young people themselves.

9.2 That is not to say that regulation should not play *a* role. It is important that the Government should continue to pursue all available routes to restrict access to harmful content. However, this is not an easy area. For example the recent parliamentary inquiry into Harmful Sexual Behaviour considered whether it would be possible to hold parents legally responsible if it could be proved they had proved neglectful in allowing their children access to inappropriate material on the internet in much the same way as they might be responsible for a young child consuming a bottle of whiskey carelessly left open at home. But the National Police Chief's Council felt this would be extremely difficult to prosecute and also problematic to legislate for.

9.3 Instead the clear advice the Inquiry received was that any regulation will only work in tandem with clear ongoing age-appropriate support, advice and guidance about safe internet usage for children, young people and their parents either through schools or within wider public education work.

10. What challenges face the development and application of effective legislation? In particular in relation to the use of national laws in an international/ cross-national context and the constantly changing nature and availability of internet sites and digital technologies? To what extent can legislation anticipate and manage future risk?

10.1 The reality is that some sites operating outside of UK law may not be subject to UK legislation – this could be particularly problematic with pornographic sites, where the recent HSB Inquiry heard that the majority of providers are based outside of the UK.

11. Does the upcoming General Data Protection Regulation take sufficient account of the needs of children? As the UK leaves the EU, what provisions of the Regulation or other Directives should it seek to retain, or continue to implement, with specific regard to children? Should any other legislation should be introduced?

11.1 It is crucial that leaving the EU does not result in any reduction in protections for children. The UK must continue to work in partnership with EU members and other international partners to make the internet safer and to ensure companies are more effective in tackling online grooming.

11.2 Article 8 of the General Data Protection Regulation (GDPR) would mean that the personal data of children under 16 could not be processed, for example for social networking sites, without the permission of a parent or carer, though member states could lower the age to 13. The preamble to

---

13 Rallings, J (2015) *Youth And The Internet: a guide for policy makers* http://www.barnardos.org.uk/youth_and_the_internet_report.pdf

the GDPR rights states that: *"Children deserve specific protection of their personal data as they may be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal data."* This is clearly correct, and the GDPR sends the clear message that stronger safeguards must be in place to prevent images of children and other private information being accessed and shared.

12. What more could be done by the Government? Could there be a more joined-up approach involving the collaboration of the Government with research, civil society and commerce?

12.1 UKCCIS is a helpful arena created by the Government to bring together organisations from private, public and voluntary sectors to discuss matters and build relationships between specialists in technology and specialists in childhood. However, it may benefit from broadening its remit to consider not just internet matters directly related to child safety but also to those around child wellbeing.

APPENDIX A

Platforms, Sites, Apps, Games popular with children and young people based on Barnardo's service experience.

- *Whatsapp* is used to enable group chats and the sharing of photos and videos
- *Snapchat* is used for sending pictures and has been associated in one service with young people sending nude images of themselves
- *Twitter* is used to communicate with and update 'followers'
- *Facebook* is still used to some degree to chat, make new friends, watch videos but is also seen as 'uncool' by some young people
- *Instagram* is used to share images
- *YouTube* is used to watch videos, but users can also set up their own channel and broadcast their own films, one service stated that they had noticed a rise in primary school children using YouTube and not using any security settings when broadcasting as they want to be 'discovered' and 'become famous'.
- *Minecraft* and *Lego* were games specifically referenced by one service that work with children who display Harmful Sexual Behaviour (HSB). This was in relation to under 10 year olds.
- The game *Grand Theft Auto*, which includes sexual violence, racism and drug taking, was mentioned as featuring heavily in service referrals for younger children with HSB. Although the game is not specifically internet-based it allows users to play together on the internet via a games console.
- *Pokemon Go* is a new game that relies on users walking around outside to catch virtual animals associated with the game.
- *Instachat* is used to instant message friends and meet new people.
- *Meow chat* has been used by a few young people to meet new people and chat.
- *Oovoo* and *Kik* enable users to chat and call peers and new people
- *Skype* is used to video chat and meet new people
- *Tinder* is a dating app and enables users to meet new people and go on dates (over 18s only)
- *Viper* is used to talk to people on a contact list
- *Hot or Not* is used to rate other people's photos
- *Kids Chat* is an open chat room for young people.

August 2016

BBC – written evidence (CHI0053)

We welcome the opportunity to contribute to this very important inquiry. Members of teams across the BBC have provided their knowledge, experience and insight for this submission. We have answered the questions which were most relevant to the BBC and our experience.

What risks and benefits does increased internet usage present to children, with particular regard to:

Social development and wellbeing

1. Increased internet usage presents benefits for children. While TV has a bigger positive impact on pre-school children, 39% agree that they have used online tools to help them with their reading and writing. We know that linear TV is important to this audience and they are not using a wide array of media at this age. For the 6-12 audience 46% said they use online to help with maths or numbers and 46% to help with homework. There are specific examples of online impacting something they do in the 'real world' e.g. Mister Maker website makes them want to draw. YouTube also appears to be an inspiration for children with one child using it to help make a card for her Mum, a young girl was using it to help her dance and another to help her sing. (*Source: Children's Impact Report).*

2. 80% said Bitesize made them feel more prepared for their exams, 57% said Bitesize helped them achieve better grades and 51% said they would have found it harder to get through their GCSEs without it. (*Source: Impact of Bitesize Report).*

3. Children are more likely than teens to speak to family members about online pressures. We know from other research that teens are the heaviest users of social media where much of this online pressure will occur. Dixi, created by CBBC and learning was online content intended to raise awareness of dangers online. Those that used it thought it was fun and recognised that it was teaching them about being safe online. After watching Dixi 64% changed the information available publically about them on Twitter and Facebook. 53% of 11-13 are worried about what they share on social networks and girls are more likely to care about what is said on social networks. (*Source: Safer Internet Day Evaluation).*

4. However, there are risks. In a meet the audience session we heard teens mentioning illegal sites for getting the content they want to watch e.g. Putlocker *(Source: Bitesize meet the audience session 2016).*

5. Parents were asked about eight different technical tools and whether they thought their child could "get round them". Around one in five parents of 5-15s who used each tool felt that their child was able to bypass the tools. A quarter of parents felt that their child could get

around their ISP's network-level home filtering, and about one in 12 parents who used each of the eight tools said they were unsure whether their child could bypass it.

6. Children's levels of critical awareness – about advertising messages, about how services are funded (and therefore whether they are being sold to) and about the extent to which they can trust information – are relatively low, given the ubiquity of internet use. Set alongside the wider range of sources of content children have access to, their increased exposure to advertising and the use of services like social networking raises challenges for how parents help children keep their personal information safe, understand the implications of sharing personal information and content and navigate the increasingly complex online environment safely in a way which will allow them to get the benefits and minimise the risks.

7. Children are more likely than in 2014 to think that information on websites I apps used for school work and on social media sites is "always true". Since 2014, 12-15s are less likely to say they would not want anyone to see their personal information (42% vs. 54%) and are more inclined to share this information with friends only (46% vs. 39%) or with friends and their friends (7% vs. 3%). They are also less likely to say they would not want anyone to see information about what they are doing (23% vs. 33%) and are more inclined to share this information with friends and their friends (10% vs. 6%).

8. One in six 12-15s and one in ten 8-11s who go online say they have seen something online in the past year that was worrying, nasty or offensive, unchanged since 2014. The majority of 8-11s and 12-15s would tell somebody if they saw something online that was worrying, nasty or offensive, but the proportion of 8-11s and 12-15s who say they would not tell anyone if they saw this kind of content has gone up since 2014, to about one in 20, similar to the proportion of 12-15s who say this.

9. Three in ten 12-15s (28%) said they knew of someone who had had any of a range of negative experiences asked about, including online/mobile contact or conduct, in the past year. One in seven (14%) say they have personally experienced at least one of these negative experiences in the past year. Around one in 12 12-15s (8%) say they have been contacted online by someone they do not know and one in eight (13%) know someone this has happened to. Two per cent say they have seen something of a sexual nature, either online or on their mobile phone, rising to 5% saying they know someone this has happened to.

10. Only one in ten 8-11s and 12-15s say they have personally experienced any kind of bullying in the past 12 months, including face to face. Bullying is more likely to happen in person rather than via text message, social media or online games.

11. Some older children (12-15s) do have knowledge of potentially risky behaviours, for example one-third of internet users know how to delete their browsing history. While this is not inherently risky, it might limit parental supervision of sites visited by the child. However, very few report having done so. Only one in ten say they have deleted their history records. Knowledge of more complex tactics to get around parental controls such as disabling online filters or controls, or use of proxy sites or VPNs to access filtered sites or apps is lower. One in ten internet users say they know how to disable a filter or control, 6% say they know how to use a proxy site or a VPN. However those reporting that they have actually done so is far lower than the claimed knowledge, in all cases only 1% say they have done it.

12. A quarter of parents of 5-15s are concerned about the online content their child is exposed to. One in five parents of 5-15s are concerned about whom their child is in contact with online, a decrease since 2014. A third of parents of children aged 5-15 are concerned that their child may be giving out personal details to inappropriate people. Around three in ten parents of 5-15s are concerned about online bullying.

13. A quarter of parents of 12-15s are concerned about their child sharing inappropriate or personal photos or videos online. One in four parents of 5-15s are concerned about their child seeing content which encourages them to harm themselves. One in eight parents of 12-15s feel they don't know enough to help their child manage online risks. (*Sources for paragraphs 5-13: OFCOM's 'Internet Safety Report (2015)' and 'Children's online behaviour: issues of risk and trust - Qualitative research findings (2014)' which was undertaken for OFCOM by Sherbert).*

14. Most older children recognise that YouTube vloggers may receive payment from product owners but they are not concerned. (*Source: Advertising (Scoop))*

Data security

15. With regard to data security, increased Internet usage presents no real benefit to children. However, increased Internet usage may present a number of data security risks to children, including:

16. Children becoming the target of online criminal activity, where they do not have the necessary level of maturity or experience to be able to identify such activity as criminal, or to be able to safely protect themselves from such activity. This could result in them divulging personal information belonging to themselves, their family or their friends to such criminals.

17. Children have access to multiple legitimate online services either directly through the internet, or indirectly via services built into many electronic devices (computers, smartphones, tablets and smart TVs). These services may collect data from children either directly by asking for personal data, or indirectly by analysing internet or device usage,

websites visited and so on. If data is held across a wide range of organisations, there will always be the risk of a loss or breach, which could result in information falling into criminal or inappropriate hands.

18. It is possible for children to access legitimate online "social media" services, and in so doing they may supply or communicate personal, or even sensitive, data and images.

19. In all the above cases, a failure of data security can result in:

20. Increased or specifically targetted criminal activity against children, their family or friends; increased or specifically targetted malicious activity (e.g. trolling); the current location of children in foster or adoptive care being tracked by unauthorised persons; an increased risk of children being targeted for grooming by people falsely representing themselves.

Which platforms and sites are most popular among children and how do young people use them? Many of the online services used by children are not specifically designed for children. What problems does this present?

21. Some facts: Watching video / clips and playing games are the most popular activities done online. (*Source: Chatterbox Digital Tracker Wave 11).* In 2015 there were 75k education apps available in the app store.

22. Data and adaptive learning offers opportunities for students, pupils and teachers to track their goals and improve performance. Gamification in the learning world is blurring the lines between education and entertainment, meaning that media time is as much about learning.

23. There are also entertainment brands that are embracing this and using their characters to encourage learning e.g. Disney. *(Source: BBC Learning Key Trends)*

24. YouTube is widely used by teachers in the classroom and we see that that they use it to provide inspiration in the classroom. Teachers such as Mr Hegarty have embraced YouTube to deliver engaging educational content. Most are using YouTube rather than YouTube for schools therefore there are some risks that inappropriate advertising appears or inappropriate recommended content. Children are using generalist sites such as Wikipedia and YouTube more than specialist sites such as Bitesize. Anecdotally we hear children say they use Wikipedia as a starting point and verify the information - something we suspect is being reinforced by teachers. Websites like Bitesize and Mathletics are making learning fun and encourages children to want to learn more. *(Source: School Tracker Spring Term)*

25. Children have a circle of trust on social media. What's App, Snapchat and Instagram to an extent are kept to a closed group of friends. Facebook is open to a wider group but is thought to be a network for

older people. There is pressure to receive affirmation on social networks such as Instagram. Users need an instant amount of 'likes' otherwise they will take content down. (*Source: Scoop BBC Media Jan 26th presentation)*

26. YouTube is the ultimate content destination making content discovery for kids really easy. 88% of 5-16 year olds claim to use YouTube and almost half use it on a daily basis. For the first time in 2015 12-15 year olds that use YouTube were more likely to say they preferred watching YouTube clips than TV programmes. It would be remiss to say that YouTube is exclusively for short form content, it fulfils the role to inform, entertain and educate this generation. 58% of 12-15s use YouTube to listen to music and a third are watching TV programmes on there. (*Source: Childwise Monitor, 2015)*

27. 90% of 5-16s claim to use YouTube to help learn things and 9% choose it as their favourite resource to do this. *(Source: School Tracker, July 2016)*

28. 51% of 6-12s claimed to use Minecraft. Minecraft allows children to be creative and develop and master their skillset, providing challenge and complexity. YouTube and Minecraft are the two brands that they love, 66% of 6-12s say they **Love** YouTube and 63% say they **love** Minecraft. *(Source: BBC Children's Trackers).*

29. Social media becomes really prominent in secondary school when the mobile phone becomes the most important device. 87% of 12-15 year olds have a Facebook profile and over half are using Instagram. It is social media that drives up the time spent online for the teen audience, at 12 years old 43% are using their mobile for social media and by 15-16 this is 71%. They are proficient are using all networks, Facebook has the largest reach among this audience but they don't necessarily think it is exciting. It is the network where they are most likely to engage with brands as well as friends and family. Snapchat is for their friends and they don't have large networks on here, it is fast paced and funny. Instagram is where they curate their online personas and they can spend hours creating the perfect selfie. *(Source: Childwise Monitor 2015)*

What are the technical challenges for introducing greater controls on internet usage by children?

30. Conventions such as parental gates, pins or passwords can be implemented to prevent children gaining access to content that involves payment or data usage, or wandering off into the wider internet or other apps on mum and dad's tablets.

31. Children use services designed for adults and can accidentally access unsuitable content. Having tools such as profile switching such as is provided by Netflix can allow parents to filter and limit the content children can see within a service.

32. Parents often have a desire to respect the privacy of their children but this may mean they are unaware of the potential nasty behaviour that may be affecting their child. Parents can't monitor or have visibility of their children's social activity online, e.g. Snapchats that disappear after 1 view, or conversations made up solely of emojis, that parents don't understand.

33. Children use multiple devices used to access digital services and can connect from their home network, school, friends' houses, or by using public wifi and mobile networks. These can all have different levels of filtering and present challenges to parents who want to try to control their child's use of the internet.

34. For service providers, maintaining content filters (black lists and white lists) is likely to be resource heavy and after-the-fact. Overblocking may also be a significant issue whereby network level controls are so strict that children don't have adequate access to the internet necessary for their schoolwork for example, or cannot access help and support services about sexuality or other sensitive issues that they might not want their parents to know about.

35. With regard to age verification, we do not know of a formal way of confirming or knowing a child's age without parental verification. Parents can verify on a child's behalf, but we are not aware of a foolproof way of knowing whether the person verifying the child is actually their parent. Furthermore, requiring this level of verification can be unattractive to users and very time consuming.

36. The BBC aims to build gold-standard safeguarding features into our products and services. However it will be a challenge if other providers have a lower bar, which may mean that children simply switch services and use the ones that requires less effort.

37. There is a complexity in helping parents and children to understand what the different technical 'controls' are. In research carried out for BBC iPlayer, we found there was a misunderstanding about what the existing controls were and what they did, for example there was a belief that all post-watershed content would be blocked when a parental PIN has been set up, when in fact it is only content marked G for Guidance which can be blocked.

38. It is also difficult to design a one-size-fits all solution. Different parents have different beliefs as to what is appropriate for their child. Again previous research for iPlayer showed where as some parents were nervous about their child watching anything but CBeebies - others were happy with them watching anything, and doing the monitoring themselves. There are EU PEGI rules for some apps and digital offerings, but this isn't universal.

Who currently informs parents of risks? What is the role for commercial organisations to teach e-safety to parents? How could parents be better informed about risks?

39. There are a wide range of resources available to parents informing them about risks and how to mitigate them. Information is provided by the BBC as well as other industry organisations. It is also provided by a host of 3rd sector organisations, most notably Internet Matters and Parentzone, and it is provided by government bodies as well.

40. Any industry organisation providing digital services to children has a responsibility to provide information for parents and users about how to engage with the company's services safely and responsibly, and what to do if there is a problem. Accordingly, the BBC provides this information through a variety of output, but goes further in that we also provide information regarding other services, and about the digital environment generally.

41. There is such a wide range of help and resources, the landscape may be confusing. To that end, the BBC has recently proposed a new service on bbc.co.uk which will draw together under one banner not only all the BBC's resources, but will also highlight, amplify and signpost resources offered by 3rd sector bodies and industry organisations. The BBC hopes to launch this new service in the first quarter of 2017.

What are the challenges for media companies in providing services that take account of children? How do content providers differentiate their services for children, for example in respect of design?

42. One of the challenges of using the word 'Children' is that it suggest a single group of users with similar needs. However between the ages of 0 and 18, children's developmental, emotional and social needs change dramatically as they get older. So media companies need to think of their users and audience in much more granular terms e.g. toddlers, preschoolers, 6-8s, 'tweens', teenagers, and then identify the different opportunities to create content and experiences aimed for each group.

43. The BBC does this by using research to create audience segments and using personas during the development of products for children. We user-test and pilot content with children, to get both usability and qualitative feedback. Challenges here are around a child's ability to articulate what they are thinking or feeling – young children in particular often struggle to explain what they think or feel. Therefore a lot of our studies involve observation techniques, so looking at what children do rather than what they say – this is more time-consuming and expensive than questionnaires and surveys of users.

44. Some of the user experience and design challenges include:

45. Children can't read when they first encounter media and devices, so they rely heavily on pictures and sound. Any messaging around safeguarding is usually textual, which means that children can't read it. At this young age, you are relying on parents and guardians being involved and mediating their child's experience. However if devices are

used without adults to mediate (such as on a long car journey where the parent is driving and the child has a tablet), children will continue to encounter messaging and instructions that they can't respond appropriately to.

46. Children of a young age have poorer motor skills and lack dexterity, so designing for children means allowing for greater error. For example if you design a jigsaw game, the proximity of the pieces in relation to their target position, must have some tolerance to allow a child to get near the spot but not be exact. So we need to balance challenge and difficulty, so they have a good experience, whilst mastering new skills.

47. Legal restrictions around children's data can also present challenges, as understanding children's use of a software product and optimising the product is difficult when the child's data cannot be used to measure their interactions and behaviour without parental consent. Rightly, the restrictions around data are intended to help protect children, but they can also act as barriers to a better understanding of who and how our users are using these services, so that products and services can iterate and improve.

48. There is often a feeling that adapting content for children is 'difficult', and so there can be a reluctance to include this audience when thinking about content that's not directly for them - but used by them, e.g. 'family' content or sport content. Clear guidelines and rules regarding design and content that apply beyond content explicitly aimed at children could help open up wider ranges of content to younger audiences.

49. Similarly digital products or content are often not user tested with a young audience, due to the complexity of reaching the broad range of ages with different abilities. This, combined with the need to include a range of diversity characteristics, means a lot of sessions are needed to properly and conclusively test with children.

What voluntary measures have already been put in place by providers of content to protect children? Are these sufficient? If not, what more could be done? Are company guidelines about child safety and rights accessible to parents and other users?

50. We have developed the G for Guidance system which provides both parents and children with information about the digital video content on BBC platforms that they come across, where it might be unsuitable for a range of reasons.
http://downloads.bbc.co.uk/commissioning/site/Guidance_labels_final.pdf

51. iPlayer has a parental lock functionality that parents can use to protect children from accessing inappropriate BBC content.

52. We have very clear and specific guidelines about what content should appear on different areas of BBC online – for example any content on or

one click away from the BBC Home page should be suitable for a general audience; we signpost BBC sites that are specifically designed for an older audience such as BBC Taster.

53. With the launch of myBBC, which requires children under 13 to link their accounts to their parents, we have begun to draw up a more focussed policy towards child protection.

54. Our editorial policy guidelines include substantial advice and policy about child protection are available to an internal and external audience. http://www.bbc.co.uk/editorialguidelines/guidelines/children-young-people

55. We have a number of roles with the organisation, the function of which is to ensure advice and decision making is appropriate in this area. There is also a number of training courses for staff to ensure that they too are comfortable and familiar with the issues.

56. We share tips and advice to both parents and children about how to stay safe online – both in CBBC and elsewhere on BBC Online. We are about to launch a new resource supporting myBBC which includes updated advice and links to external organisations. http://www.test.bbc.co.uk/usingthebbc/

57. We are members of a number of partner organisations that work together to develop best practice in this area – such as Childnet, the South West Grid for Learning and Internet Matters. We are also a founder member of the ICT Coalition – an industrywide organisation across Europe that has similar aims and also to work with the EU on legislation in this area. We are on the board of UKCISS.

58. Our guiding principle remains that it is for parents to oversee or 'regulate' the consumption of our online and digital content by their children as they see fit. However we should provide them both with the information and the tools to enable them to make those decisions.

59. We believe strongly that these measures work, as evidenced by the relationship with our audiences and that the voluntary/self-regulatory measures that we have developed ourselves and in conjunction with wider industry continue to be effective.

What are the regulatory frameworks in different media? Is current legislation adequate in the area of child protection online? Is the law routinely enforced across different media? What, if any, are the gaps? What impact does the legislation and regulation have on the way children and young people experience and use the internet? Should there be a more consistent approach?

60. While children are embracing new internet services faster than any other demographic, the legislative and regulatory framework lags behind. One particular concern relates to the increasingly outdated

regime for the prominence of public service broadcasting. It was introduced via the Communications Act 2003, in the markedly different TV landscape of 2003 – 4 years before BBC iPlayer, 8 years before digital TV switchover, and 7 years before the iPad. It created PSB prominence principles for broadcast TV sets but not for connected TV sets, and PSB channels but not PSB catch-up services.

61. Regulatory gaps have become increasingly clear. If the regime has not kept up well with the multichannel world (Cbeebies and CBBC are behind 12 US cartoon networks on the leading pay TV platform's channel listings), it has certainly not kept up with the online world where easily finding trusted services like those of the BBC is more important than ever before for children and parents. No prominence at all is guaranteed for the new BBC iPlayer kids' service offering access to the best BBC kids' content. Nor would prominence be afforded to our new service proposal, iPlay, which will offer a front-door to the best British kids' content from any provider. This lack of PSB prominence for on-demand content is contrary to audience expectations. Ofcom's last PSB Review (2015) recommended this be rectified and did this Committee in its report on Media Convergence (2013). This month, Government modernised the licence fee to cover on-demand (BBC iPlayer) to respond to the same trends that are undermining PSB prominence. We believe a similar response is now required for PSB prominence and believe the Digital Economy Bill presents an opportunity for such a debate.

62. All BBC content – whether broadcast, online or on BBC channels on social media platforms – is governed by our Editorial Guidelines. The wider regulatory environment is of course different.

63. The one key area where there are issues is social media – which for many children and young people remains their central experience of the internet.

64. Social media organisations are almost exclusively US-based and therefore subject to COPPA, which sets the minimum age for participation at 13 years. That is not a legal age limit in the UK, but is an age limit with broad industry-wide acceptance in the UK.

65. However, a BBC survey earlier this year suggested that more than two thirds of 10-12 year-olds have a social media account http://www.bbc.co.uk/news/education-35524429.

66. In the BBC we are very clear that we must not and will not target children under 13 and we are very careful about how we respond to children aged 13-16 on social media.

67. For issues relating to the EU and the AVMSD, we support the broad thrust supporting co/self-regulation in this area

Does the upcoming General Data Protection Regulation take sufficient account of the needs of children? As the UK leaves the

EU, what provisions of the Regulation or other Directives should it seek to retain, or continue to implement, with specific regard to children? Should any other legislation should be introduced?

68. The key provision of the GDPR in relation to children's use of online services is Article 8:

69. Where consent is the basis of the offer of information society services directly to a person under 16 years old, the processing of any personal data will only be lawful where the consent is either given by the holder of parental responsibility over the child, or the consent is authorised by that person.

70. A Member State may by provide by law for 16 to be reduced to a lower age, provided it is not below 13.

71. The data controller shall make reasonable efforts to verify that consent is given or authorised by a holder of parental responsibility over the child, taking into account available technology.

72. There are some points to consider. The UK could legislate to lower the age where parental consent is required to 13. The BBC should consider whether or not it wants to support this on the basis that it would assist the BBC in meeting its public purposes.

73. Even if the age is lowered by the UK to 13, other Member States could retain the age of 16, leading to a lack of harmonisation and a need to either have systems which allow the age where parental consent is required to be altered to meet the requirements of different Member States when offering services in those Member States or organisations simply adopting the higher threshold for simplicity.

74. There are potential operational concerns over the obstacles this provision places on the BBC's ability to reach children who may not be well placed to obtain parental consent. This could exclude children from our online services.

75. The current DPA approach does not define 'children' but the ICO recommends parental consent is obtained where children are aged under 13. The ICO also takes a risk based approach to the processing of children's data. This allows for flexible regulation which meets the needs of children as individuals whilst balancing the risk of harm.

76. A fixed age where consent is required fails to take into account: The interests of the children in accessing the service; the risk of harm; the fluid nature of maturity; and the rights of the child as an individual, separate to those of their parents.

77. There is a lot of policy and legal debate around the imposition of the requirement of parental consent in this way. For example, the EU Commission states "Article 24 of the Charter of Fundamental Rights of the European Union guarantees the right to such protection and care as

> is necessary for the well-being of children. An important principle of the Charter is that when decisions are being made on the best interests of children, children may express their views freely and their views shall be taken into consideration on matters which concern them in accordance with their age and maturity."

16 September 2016

BBC Children’s – oral evidence (QQ 72-78)

Tuesday 1 November 2016

Watch the meeting

Members present: Lord Best (Chairman); Lord Allen of Kensington; Baroness Benjamin; Baroness Bonham-Carter of Yarnbury; Earl of Caithness; Lord Gilbert of Panteg; Baroness Kidron; Baroness McIntosh of Hudnall; Lord Sherbourne of Didsbury.

Evidence Session No. 6 Heard in Public Questions 72 - 86

Examination of witnesses

Alice Webb, Director, BBC Children's, BBC.

The Chairman: Welcome, Alice. Thank you very much for joining us. Your reputation precedes you. We are delighted to have you with us. Since other people do not have in front of them the excellent CV that we have, I am going to ask if you would put on the record your background, and where you are coming from in relation to our very special inquiry on children and the internet. Could you start us off with that?

Alice Webb: Yes, absolutely. It would be my pleasure. First of all, thank you very much for inviting me here this afternoon to talk about this hugely important subject.

I am Alice Webb. I am the director of BBC Children’s and of BBC North. I have been with the BBC for 12 years and I have worked across many parts of production. I was the chief operating officer when we moved the BBC to Salford. I moved up there with my family and 18 months ago I took on the role of director of BBC Children’s. In addition to that role, in recent months I have also taken on the role of director of the BBC across the north.

I was delighted to be able to come and speak to you this afternoon, because children and the internet is such an important topic. It is something that we worry about a lot at the BBC. We provide UK public service content for children, which we worry about day and night, and making sure that we can do that in the digital space and with as much access for children as we have done in the linear space is also very important to us. We know, and you know through the work you have been doing here, that there are no easy answers to how we do that.

One of the things that is incredibly important is that children have as much access to the UK public service content in the digital world as they have on TV, so that they have high quality content available to them. We cannot take on the role of supervisors, parents and carers, so we give people the tools and the education for them to have a healthy attitude and connection with digital content. I am delighted to be here to talk about that further.

Q72 **The Chairman:** Thank you very much for that. We are all very dependent on the BBC, the wonderful CBeebies and CBBC—he speaks as someone with six grandsons.

What are the key principles that guide you in deciding on the content that you then deliver? Do you have an evidence base that tells you what you should be bringing before us?

Alice Webb: Yes. First of all, we are absolutely governed by our mission, so we are there to inform, entertain and educate children. We add a fourth for BBC Children's, which is to inspire children to participate, to be active. We then look across the array of what we create for children to make sure that we are doing exactly that: informing them with documentaries, current affairs and news that is specifically for children. We look at our dramas, making sure that we also provide entertainment. We are across every genre, and one of the things we hold incredibly dear to ourselves, no matter what pressures are on us, is that we still maintain a broad range of content for children.

We look at different age groups for children as well. As you know, we have CBeebies, which is for our nought to six year-olds, and CBBC for our six to 12 year-olds. We also look at subdivisions within that: what is specific for the six to nine year-olds; what might we have that is going to engage and entertain? We make sure that all our content is suitable. It may not hold their attention, it may not be attractive to them, because each child likes and enjoys different things, which is why giving them a variety of things is important, but we make sure that it is suitable for whichever age range it is targeted at.

On your point about what evidence we use in deciding what content to create, we talk to many children. We do something that we call stepping out; we go into schools every week and talk to children. We take over the class—we have some teachers who work for us—to talk to children, and not only about what they are watching or what might they like; we also take some shows before they have been created and show them to children. What is going on in their lives? What is the chatter in the playground? What are they talking about? What are they worried about?

We also do audience research once a quarter with children who do not know it is the BBC. We have a survey called Chatterbox. We go to about 2,000 children, so that they have an objective and independent input. Of course, we have our own audience research team, which means that we study charts and numbers, just as you would expect anyone else to do, to make sure that we have that broad range. We have things like our statement of programme promises; I am required to deliver 85 hours of news for children every year, for example. We deliver way over that, but

there are a few other checks and balances in the system to make sure that we are giving that breadth to children.

Lord Allen of Kensington: Alice, can I pick up on one thing about practical examples? There has been coverage recently of the programme "Just a Girl", which is about children's sex change and an 11 year-old's struggle to find hormones and such. This is not being judgmental, but you have MPs and family campaigners at one end of the spectrum saying that it is age inappropriate and people like Mumsnet saying that there is never an age for it to be too young. I would welcome your views on how your programmers make that judgment in what is an incredibly difficult area. This is a CBBC programme, and I think the age range you mentioned was six to 12.

Alice Webb: Yes, six to 12.

Lord Allen of Kensington: Could you help the Committee to understand how you get to that very delicate judgment?

Alice Webb: Yes, absolutely. "Just a Girl" is a show that is primarily about bullying, which is a hugely important issue. We look at those things very individually and very carefully. We take expert advice from psychologists about the content that we put together. We put it together in a format that is appropriate for the age, and we also cover the storyline in language that we think is appropriate. We make sure that we go on to offer forward journeys, so that if there are questions that children—or indeed parents—have about it they can go on. You will see underneath "Just a Girl" there are a number of links that you can follow for that.

Part of our role is to convey information in an age-appropriate way, which we believe we have with that one—I am very proud of that show—but also to make sure that we are stimulating conversation. That is part of our public service role. We do that by talking to experts, and we have our own people who have decades of experience about how to tell stories to children in an age appropriate way.

Baroness Benjamin: I know how passionate you are about getting it right for kids, especially online, which is even more important. Would you consider having an advisory group that meets three or four times a year, with psychologists, programme makers and so on speaking to you and your team about whether you are getting it right or not? Do you think it would be a good idea to look not just per programme but generally about having an advisory group like the one we have with the BBC? I am on there for diversity. Would you consider doing that for children?

Alice Webb: Absolutely. I am always open to finding the right way to make sure that we are improving what we are doing. We do that internally within the BBC, so I sit down with colleagues across the BBC who are not in Children's to see that we have that check and balance. But I would always welcome the opportunity to broaden that further if we all believe that will help.

Q73 **Baroness Bonham-Carter of Yarnbury:** Moving on to the internet, we heard a lot, particularly last week, about the negative impacts of the

internet on children. I am interested in what you think the benefits are of internet usage to children.

Alice Webb: Yes, absolutely. First and foremost, it is an amazing source of learning for children. It gives them fantastic access. One thing that is a huge positive is that every child learns in a different way. If you are a visual learner, you can go to somewhere like YouTube and watch a video about something; if you want to read about something, it gives you access to all that.

We know from our own experience with BBC Bitesize, our own learning platform, that 85% of children come to that during their GCSE time and say they benefit from it being there. That is access that we could not otherwise have for children. So, first of all, it gives them that access. It gives them an opportunity to express themselves, whether it is film-making or online creativity. It gives them a real opportunity to see a world much wider than their own, which they might otherwise not see, to help them to understand the world around them and to increase their tolerance and understanding as they grow into adults, and it gives them access to content to make them just laugh out loud.

Baroness Bonham-Carter of Yarnbury: Are you concerned that restrictions being imposed might impair these opportunities?

Alice Webb: That is what I was referring to right at the beginning. We need to find the right balance between building in safeguards for children, finding ways to allow children and their parents and carers to have further recourse if they are not getting help from the safeguard, and allowing sufficient freedom. Every child is different. Again, right at the beginning I said that I do not believe that media providers like the BBC can be the people who sit there and say that they should or should not watch this or for this long, because that has to be done much more locally by the parents and carers.

Q74 **Lord Sherbourne of Didsbury:** Quite understandably, in your evidence you divide the very broad term "children" into what you call divisions and subdivisions of age. What is your evidence, from the extensive research that you have mentioned, for the different ways in which these divisions or age groups interact with the internet? In particular, how consistent are your findings for each group? As you have said in answer to the previous question, children learn in many different ways, so I wonder whether a consistent pattern emerges from the research or whether it is very varied.

Alice Webb: It is by and large consistent, so there are main tracks of children. There will always be children whose behaviour is above age or indeed below age. Sometimes children will flip between the two, but there is always a main chunk of children. At the youngest in the preschool end of things, children are making simple interactions. One of the things that is another positive of digital is children are able to exercise choice at an earlier age. It used to be that you had to be able to read, but with the invention of touch screens you simply have to have a finger that is strong enough to touch a screen to start choosing what you watch. It is about simple interactions about choosing, "I would like to

watch this over that". It is about simple interactions with games, about dropping shapes in. It is all about that kind of simple interaction.

There is a progression as children get older. At about five to seven they are moving on into the next level of interaction and are playing slightly more complex games. Children at that stage want to start to learn things, to repeat things. With that we see that the learning side of things gets more complicated as they move up, because they move from learning a skill to mastering a skill. That mastery may be, "I know every name in a football team and I am a master of that", versus, "I know how to play the piano incredibly well". Their interaction becomes broader. They start to follow passions into that space as they get older. They play more complex games, and the breadth of what they are using is wider too.

The crucial thing that goes alongside children's interaction is also how their parents interact with them. You can put alongside what children do what parents do as well. In the early years our research and experience shows us that much of that interaction is supervised and parents still have heavy interaction in the choices that are made. In the middle age group, the seven to nine year-olds, they start to make a switch. By the time children are about nine upwards they start to be much more independent and make choices with parents a bit more in the background.

Lord Sherbourne of Didsbury: That is very helpful. This may be a difficult question because your research may not cover it, but do you have any evidence that the learning mastery development that you have talked about is greater now with these age groups than it would have been pre-internet?

Alice Webb: I do not feel that I can comment on that. One thing, though, that is not specific to that point but we know is that children want to be children as much as they ever did. Digital and the internet give them access to a broad range of things, but our research shows that four out of five children still read books for themselves outside school; four out of five children still play sport for themselves. My personal favourite is that four out of five children still want to spend their pocket money on sweets. So they want to be children as much as ever. We have not seen those things being different, but I do not know about your learning question.

Baroness Benjamin: You come from an engineering background.

Alice Webb: I do.

Baroness Benjamin: That is a great skill to have, because it means that you have to use your imagination. What prompted you to develop the iPlayer Kids, the iPlayer and CBeebies Playtime services? What sort of challenges did you encounter in designing these services?

Alice Webb: Why do we not start with the CBeebies applications—the Playtime Storytime and our new one, Playtime Island—which are specific apps for our youngest audience, our CBeebies audience? We developed them partly because they give us the opportunity to allow children to play in the way that I just described. They are all touch screen and allow

children to interact and play, so it gives us that opportunity. It also allows us to create standalone playgrounds, online playgrounds for children that they can go and play in and enjoy those things in. Apps are very popular with our youngest audience, and we see people gravitating away from websites and on to apps, which is why you will see that we have more applications, and our more substantial apps sit in that end of the age spectrum.

We developed iPlayer Kids to be an environment that was child-centric, so our absolute focus was making sure that our design was child-centric for those. We created iPlayer Kids, which is particularly targeted at children who are at that crossover age between CBeebies and CBBC, to help them to navigate between. We were finding sometimes for children it was a daunting task about, "Where do I start with CBBC? I might be at the top end of CBeebies". We created the iPlayer Kids app to give them an environment that was just for them, which they could feel at home in, to help them get content that way, and it has further safeguards against them wandering off into content that is not necessarily age appropriate.

Baroness Benjamin: Some witnesses we have had have said that being online has taken children away from books and being creative in the conventional way rather than this new way that children are being introduced to. What risks does gamification—if it is called that—

Alice Webb: Yes. Gamification, yes.

Baroness Benjamin: —present to children? Are you concerned about the amount of time children are spending online and the potential for apps to encourage compulsive behaviour? Do you put anything in place for children to limit themselves, rather than waiting for the parent, because they know when to put a book down? How do they know when to stop there?

Alice Webb: There are a few things. On that last point first, we do not have timers built into our apps. When we developed them we talked to parents a lot. That was not one of the first features that they asked for with our apps. We absolutely promote—and I use them for my own children—overarching devices that limit time and things like that and we promote the education of that. But the flipside of that is why this inspiring part is so important for us for children: it is to inspire and call out to children to go and be active, to read a book, "We have a book club, so put this down and go and do that instead. Draw us a picture and send it in". Our content is absolutely littered with the call to action for children to go out and be active as well as enjoy things online.

On your question about gamification, that is something that we all need to be very aware of and to think carefully about. From a BBC perspective, gamification is another way to help children to engage with learning activities; it puts it into more of a game scenario. That is a minority aspect of what we do, but I observe it more widely on the internet, which is what might be described as sticky content—content that requires children to stay online a long time, because that is the only way they are going to receive the reward that they are desperately searching for, or that requires them to stay online and then pay for

further upgrades. That is something that we all, as an industry, need to be very careful about.

Baroness Benjamin: The compulsive element of all that that brings.

Alice Webb: Yes, absolutely. With anything, your use of digital content online or in apps has to be part of a varied diet in life. Anything that is sticky that requires habitual behaviour, anything that requires you to come back every day because your pet is going to die or anything online are things that we all have to be very careful about.

Q75 **Baroness Benjamin:** This leads on nicely to the next question. What is the main barrier to more services being designed specifically with children in mind to combat the kind of discussion we have just had? Do you think it is realistic to expect commercial designers to develop products in a child-friendly way, and do you develop products in this child-friendly way that we are talking about?

Alice Webb: Yes, we do absolutely. There are always developments in this space, which is why we made iPlayer Kids to take the big grown-up iPlayer and make it more child-specific. I would sit here and say, yes, absolutely, people should be designing their products and services with children in mind. It is a responsibility that people have. I also think that it is something that people will be demanding of commercial services, as these subjects are discussed more widely and there is greater awareness in the public about them. I see no reason why you cannot put the child front and centre with your designs of apps. One of the things that is hugely important in the digital space is about there being transparency about who is funding what, how things are paid for: are you advertising; do you have product placement? That is another very important aspect when we look particularly for children.

Baroness Benjamin: The BBC told the Committee that legal restrictions on children's data can prevent problems when trying to understand a child's use of a software product. What exactly did you mean by that?

Alice Webb: There are a number of things. Obviously there are incredibly important restrictions on collecting data on what children are doing online. We have seen recently in America people being fined for doing that subtly. It is possible that people will tell you that they cannot design a product to its best potential without being able to track some of the behaviour of what people are doing. For example, if I am a games maker, if I cannot track what children are doing I cannot tell you whether they get frustrated at that particular level or what they are doing with it, but I do not think those are good enough reasons not to be putting children first when we are designing things.

Baroness Kidron: I want to pick up on this idea about timing and time limited. You said you did not do that because parents were not interested or it was not at the top of their list. Then you went on to explain how other people use gamification. I absolutely accept that the BBC does it for the good of the child and in a child-centric way, but do you not think that it would be quite useful for the BBC to introduce time limits or timeouts in a very visible way as an example of best practice in an environment that has the child's best interest at heart? Is it not the case

that most parents do not understand the whole issue of compulsive behaviour and that, in terms of what you could offer as an institution, it would be a huge win for the community because we would have something to point at?

Alice Webb: Yes, you are absolutely right. We do have a responsibility and we have a real role because we reach so many people, which is why we are so involved in making sure that we are educating parents with what is the right thing to do for their children. I completely accept your question about the BBC and where it is at the moment. I take that on board and we will look at that.

Baroness Kidron: Thank you.

The Chairman: I will just stay with this a little bit longer. When you are commissioning a programme or a game—and we have heard quite a bit about the compulsive or addictive behaviour that can follow from that—what do you do that is protective of the child that is different from other people whose interest may be to hold the child glued to the screen for as long as absolutely possible? What are you doing differently?

Alice Webb: We do a couple of things. Our games are secondary to the first iteration of that content. Take, for example, our Danger Mouse game, which is so very popular but is not the primary driver that we connect with children. We are already engaging them in a narrative that starts, "It is 11 minutes long. It starts here. It finishes there". That gives an opportunity for it to stop. That goes for our cartoons too. Our games do not have 697 different levels that just go on and on and on; they are bound. They are engaging and interesting but they stop. They do not then take you on. There is no in-app purchase, no unobtainable goals at the end of it. We create them as simple add-ons to what we already do.

Lord Allen of Kensington: If I could stick with the theme of parental understanding, your own research shows that there is probably a lot of misunderstanding in relation to the internet. For example, a number of parents felt that if they had a parental PIN it would protect more children from post-watershed content rather than the need for guidance. In a practical sense, I would like to understand what work you have done in that area and, practically, what you think the BBC should do to help with that challenge. I think there is a high level of misunderstanding there.

Alice Webb: Absolutely. We participate in a number of moments through the year. We use our channels for grownups and for children to make sure that we are publicising and helping to raise awareness. We do that through our news content and at particular times of the year. We participate wholeheartedly in Internet Day, for example, or on anti-bullying, which is about the cyberbullying side of things. We commission research ourselves that can then generate new stories and further awareness of that. We create the material for our own online guide. Crucially, we are also increasingly playing a wider role in helping to connect together other parts of the industry. The BBC has a huge reach and has an important role to play, but I believe we also have a convening power that we are doing more. That is why you will see that the BBC recently became a founding member of Internet Matters, which is something with industry, ISP providers, alongside Google and now the

BBC, about raising awareness that is connecting on to many of the resources that exist for parents.

It is a bit like the Forth Road Bridge; we can never do too much and we just need to keep doing it until it is ubiquitous and everybody understands it, and we will use all our channels and any convening power. We participate with members of this Committee—I also sit on other taskforces—to help to try to push this forward. It says in our submission that the BBC is looking to launch a new portal in the first half of next year, not to be the one-stop shop but to bring together all the power of the BBC and further connections to others out there. There is more for us to do, but it is something that I hope you will increasingly see, as well as what we describe as making sure that our public service is as strong in the additional space for children as it is in the physical and linear space.

Q76 **Lord Gilbert of Panteg:** Chairman, before I ask a question could I declare an interest? I advise Finsbury, which is a financial PR company, and they advise Telefonica UK.

Thank you for your submission, which is very detailed. I will pick up on Lord Allen's question. We are interested in the wider well-being of children, not just preventing danger online. In your view, does the BBC have a role in developing tools for the wider industry to look after the wellbeing of children, particularly technologically, and making them available to others outside the BBC?

Alice Webb: Could you say a bit more about what that might be?

Lord Gilbert of Panteg: We have heard from quite a lot of witnesses about the tools that are available to protect children online. You clearly have a whole suite of services for children. As part of that, you are developing tools. Do you see that the BBC has role, much like the initial development of the iPlayer, in providing tools to the industry?

Alice Webb: Yes, we absolutely do, and one of the areas that we do a lot in—it is front of mind—is helping to develop the emotional and physical resilience of children. That goes hand in hand with the protection, stopping the harm, but also with allowing them to be okay if they are exposed to those kinds of things. That is another area that I would absolutely see us partner with, and indeed we already do partner with, people. For example, Lifebabble for our CBBC audience is all about building that resilience and not just for the digital world; it is about loneliness, grief, bullying. We are already talking to further partners about how we might use that as a format and platform to be able to help build that side of children's lives as well.

We are always open to areas where people think, "Actually, we would like to partner". It is one of the things for the BBC generally, not just within BBC Children's but across the BBC—and with Lord Hall, our director-general, being very clear—that we are here to provide a platform not just for our own content but for other people's content, and to partner with people and be as open as we can. Where there is opportunity to do that, we absolutely will do so.

Lord Gilbert of Panteg: Thank you. In your submission and in your previous answers, you told us about your role in bringing together resources from a variety of different organisations. Why do you think that is a role that the BBC should undertake? Do you see any conflict at all between your role in providing content, your editorial role, and bringing together guidance for particularly parents? How did the BBC decide to take on that responsibility?

Alice Webb: I do not think that is specific to children. It is part of our role in being there to make sure that we are signposting people to appropriate specialist people who are more experienced in particular areas. You see that across all the BBC's outlets. We are incredibly clear that our editorial content is independent of that. We will never be influenced by one particular provider, charity, whatever it is. It is always independent of that. It is then about providing further journeys where there might be something ongoing. For very specifically that reason, the BBC cannot be the answer to everything, but we do have an obligation, because we have such enormous reach across the organisation, to make sure we are connecting people where appropriate.

Q77 **Baroness Benjamin:** We talked about bullying, loneliness, mental health and so on. How do you ensure that the content that you are putting out, and whatever you are going to provide after you have put it out, ensures that children are at the point where they are using their imagination and they might think they are all like that but in fact it is not really? How do you balance the children who might be drawn into thinking that they are bisexual, that they are mental, and so on? What do you provide to ensure that there are children who—

Alice Webb: Yes, I understand.

Baroness Benjamin: But there are also children who would like to be—

Alice Webb: Yes, absolutely. This goes back to something I mentioned earlier, which is that throughout our content we encourage children to ask questions, to both follow for themselves but to talk to adults, whether that is an adult they know or specialist providers who can then talk to them—a child line or an NSPCC—to help them to express these questions and to understand whether it is real or something that they are exploring with their imagination. It is about putting in safeguards and this net, but also asking questions is a really important tool for the critical thinking and critical awareness that we want children to develop. There is not one specific thing that I can point to because that is something that we try to sow in throughout our content.

Baroness McIntosh of Hudnall: I want to ask you, as a precursor to the question I have written down here, particularly on CBBC, which I think you said is aimed at the six to 12 age range. Do you have any evidence about whether there is an off the cliff cut-off at 12 when puberty kicks in and people are starting to think that it may not be very cool to watch stuff that is branded for children, or is there a tail so that you have kids on into their teens still watching CBBC material? Do you track that in any way, obviously not person by person?

Alice Webb: Yes, our research shows that by the time you are about 10 you are probably starting to be aware, and is CBBC—I do not want to say too worthy—cool enough for you? By about the age of 10, and particularly when they transition into secondary school, we see children's exposure to media not quite explode but there is that cliff, if you like. We have children who are far beyond the age of 12 who come to us consistently, particularly with some of our dramas. Some of our most popular, such as "The Dumping Ground", "Wolfblood" and "Hetty Feather", draw in older children too.

Baroness McIntosh of Hudnall: On that point, I have to say that I did not know about "Dixi" until it came up as a result of this. I have not seen it all, but I see what it is and I see that it is specifically designed to try to get kids to think about some of the issues that we have been discussing. Do you think it hit the right age band? Was it getting to children? Is it getting to children at the point at which that is becoming an important issue for them? You have given us some figures that suggest that it has had a direct and measurable impact on children's behaviour. How did you collect that data and what would you say overall about that particular kind of content? As I understand it, it is designed for kids who are perhaps getting to the point where they may not be sharing their worries with their parents in the way that younger children maybe would, but perhaps do not yet have a network that they can turn to that will help them. How does it work?

Alice Webb: First to your question about did it really hit the right spot. The primary audience for it was 10 to 12 year-old girls. The storylines were slightly above that, which is part of the norm in being slightly aspirational, because that is what children find engaging. It hit that spot for the audience who came to it.

On your second question about the measurement and exactly why we see two-thirds of them and how we know, I will have to write to you and let you know about the surveys and the follow-up that we took with those children, because that is a level of detail that I am afraid I cannot share with you today.

Baroness McIntosh of Hudnall: Okay. But it is quite critical, is it not, for two reasons? One is obviously the stats. If you are going to disseminate them they have to be backed up, and I am sure they can be.

Alice Webb: Yes.

Baroness McIntosh of Hudnall: But more, as I perceive it, in this case you were using drama to be a drama with an end in itself but also to disseminate ideas in a very specific way. How did that come about, and is more of it envisaged?

Alice Webb: It came about in the same way in which we commission all our dramas, as I described right back at the beginning. We look at the whole range of what we do and look at whether there are needs out there for children that we are not fulfilling. We know from our research and from others that two-thirds of children above the age of 10 are on social media. They should not be because of the age limit of 13, as we know, but they are. It is about making sure that we are playing our part

in raising awareness of the right way to engage, to be digitally safe and healthy. Things like "Dixi" were specifically targeted in that light.

On your question about whether there will be more of those, we always use our dramas and all our content to raise awareness, whether about online issues or other issues. We will do that in the same way for our grownup drama and for children.

Baroness McIntosh of Hudnall: You have a section that goes with "Dixi", which I am looking at right now, and says, "Do you have any questions?" It points people towards Lifebabble, which you mentioned, and towards an advice helpline. Is there a lot of take-up for those direct helpline types of opportunity?

Alice Webb: I do not know, is the honest answer to that. Again, I will provide that information to the Committee.

Baroness McIntosh of Hudnall: Good. Thank you.

Earl of Caithness: I want to follow up your answer to Baroness McIntosh about age limits for children, social media accounts and getting parental consent. Are you in favour of a 13 year-old cut-off or a 16 year-old cut-off?

Alice Webb: I think that 13 is an age that is well understood. It is an age that coincides with a significant transition of children's development as they move on to secondary school and the years beyond that. We know that a lot of children are already on social media below that age, and it would be incredibly difficult to move to 16 because we are already struggling to keep them to 13. I think that is an age that is well understood and we are better to try to make that one work than move it up.

Earl of Caithness: You did that research and showed that, I think, three-quarters of 10 to 12 year-olds had social media accounts. Did you also do any research as to whether they had parental consent for that?

Alice Webb: No, we did not. That was not part of our research.

Earl of Caithness: Moving back to the first question then, if we are going to have an age of 13, how are you going to enforce it? Is it enforceable?

Alice Webb: It is incredibly difficult. I can tell you how we do it at the BBC, if that is helpful.

Earl of Caithness: That is a good start.

Alice Webb: I can tell you what we do. First of all, we have an active policy that we do not engage with anybody on social media who is a child. The verification of their age obviously sits with the platform provider, but if they interact with us and we have any hint of the fact that they may be a child we will not engage with them. We actively do not do that. That is our policy there. We have to get parental verification for children who then come to us at the BBC for sign-in to the BBC. For a child who wants to come to the BBC and have an account with us, we e-mail their parents, and their parents, under our new system that has just come in, already have to have an account with the BBC, and we link

them to their parental account. It used to be that the parent simply had to verify, go on to their own e-mail and say, "Yes, I am happy that my child has an account". We have moved that further to make it harder and to close some of the loops between a child sitting there with another inbox going, "Thank you very much", and hit that as well. That is how we do it at the BBC as we are always moving on and making sure that we try to find the right safeguards.

Earl of Caithness: You have just been transposed to being Secretary of State and you are going to introduce a Bill. Minister, are you in that Bill going to recommend that everybody else uses the BBC's standard for checking on 13 year-olds? That is the first part of the question. The second part of the question is: are you also, as Secretary of State, going to put a time limit on what you were saying earlier about apps and play games being too long or going on to charge a bit more money? Are you going to put a control on that, and how are you going to work it if you are?

Alice Webb: I will answer your second question first, if I may. I am not going to put a time limit on things, because content is different and the quality of content is different, just in the way quality of food is different, and it is about what you consume. It is too easy for us to stick to a time limit and to feel that we have done the job. It is about the quality of the content, the interaction that children have with that content and the parental supervision. My worry is that with a blanket restriction we then allow people to step away from the supervision of children and their overall education, so I am not going to do that.

On the first question, I do not feel qualified, as Secretary of State, to decide whether others should. I can only tell you what we do, and that is why you will find the BBC may not be the fastest to market. We may not have the fastest moderation, but we will always err on the side of caution for children in this space.

Earl of Caithness: That is what is so important to us in the Committee. How do you get that spread more widely?

Alice Webb: I think it is by this important work, raising public awareness of the issues out there. We must make sure that children have access to high quality content. In the digital world it is not just about the kinds of content. It is the distribution of content as well. If you go on to a connected television now I can tell you if you are, for example as I am, a Sky user, it will take you 11 clicks at minimum to get to CBeebies; sometimes above 20 clicks depending on where you start. It is making sure that we still allow children to have access to this content so that when we do not have those time limits, which I think are a false economy, they have access to free-from-advertising, UK public service high-quality content.

Lord Gilbert of Panteg: You describe the sort of process that you take to make sure that you are not engaging through social media with anyone under the age of 13 coming to you from other social media platforms. Can you tell us how that works? Is it a technological process? Do you have some process that enables you to do that or is it very labour intensive? It seems that it must be one or the other.

Alice Webb: Everything that we do is labour intensive, absolutely. That is why I say that we may not have the widest breadth of everything because we pre-moderate. If somebody posts on our website, we moderate that first with human eyes looking at it. A child cannot even sign up with a user name and inadvertently give a name that might indicate who they are because we will pre-moderate that. The same with the way that people interact with us on our social boards. There are people at the other side of that who look at it and worry, not just about whether we think you are a child but do we think you are an adult posing as a child? Do we think there is anything that gives us any cause for alarm? We will act on that.

Lord Gilbert of Panteg: So the answer is basically very intense moderation?

Alice Webb: Intense moderation, absolutely. We, like others, look to see how technology can come behind us with that, because we will always want to stay as relevant and as close to the front end of children's interaction as possible. We are not simply saying we will be a cottage industry forever, but we will always put that line of human intervention in as well.

Baroness Benjamin: CBeebies and BBC Children are the most trusted if you ask any parent, and you have heard from our Chairman, when he first introduced himself, that his grandchildren watch CBeebies because it is a trusted brand. What can you do to make parents feel that you are a trusted brand when it comes to online content and for other people in the industry to follow what the BBC is doing? What can you do to headline, apart from raising awareness, to say, "This is what we are doing that is different from everybody else"?

Alice Webb: I guess a few things. One is by completely bringing all our standards to bear in our online content as well as our linear content, by playing an active role in the industry, making our voice heard, and I have mentioned a few of the ways that we are doing that already. One of the things that we are doing as the BBC is the global children's media summit next year in Manchester. This is something that happens every three years. The last one was in Kuala Lumpur and next year it will be in Manchester, hosted by the BBC, specifically looking at children's media in the digital age. That will bring together content makers, platform providers and policymakers to specifically raise this and make it more of an issue; to continue to build public awareness; to continue to showcase the good things, the best practice that I believe we follow, and there are others out there too; to use our convening power to bring some of the highest level parties from the west coast of America to these shores to have these conversations. Many of the answers lie over there with the way that digital is international. I do not think there is one thing that we can do, but we will continue to push in every way we can.

Q78 **Baroness Kidron:** I think you have answered this question in fragments in answer to other questions, because you have mentioned the phrase "critical awareness" several times. The evidence that was put forward said that advertising messages about how services are funded and, therefore, whether they are being sold to, and about the extent to which

they can trust information, which is what Floella was just talking about, are relatively low among children. I am interested in who you think has responsibility for making sure that children know, which is a slightly different question. Who should be labelling things in a very transparent way?

Alice Webb: It is a really good question, and I think that platform providers have a huge responsibility in this space. They are just that, the platform. They provide the stage by which these items, these people and these games stand on that platform. I think they have a responsibility to be transparent and clear about the basis on which they stand on that stage. I am sure that does not catch it all, because one of the great advantages and disadvantages of digital is that people can start their own. The new outlets and new apps come so quickly and it becomes very difficult, which is why it is not an easy problem to solve. I cannot help feeling that there are significant platforms out there that are well established, that have more to do in that space in transparency and making sure that they are allowing children to exercise their own choice, their own critical awareness.

Baroness Kidron: On top of that, a lot of the time when we demand those sorts of behaviours, people scratch their heads and say, "This is technologically very difficult". Would you care to tell us whether transparency, terms and conditions, pointing out what an advert is and so on are technologically difficult or whether, like the answer you gave my colleague just now, it is about the effort you put into doing it?

Alice Webb: There will always be a gap between technology and behaviour, and that is where you have to invest the money and the human effort to go through it. If what you want to do is to provide technology all the way up to the human eyeballs, there are always going to be gaps. The net is never going to be closed enough. It is about effort and prioritising, and I believe that it is possible to bridge any gaps between what technology and algorithms and all the rest of it might give you with human effort.

Baroness Kidron: One last little question, which we have not really touched on. I know the BBC does an awful lot about education, but do you feel that you are doing enough to explain the internet itself? You just used the word "algorithms", but most of the young people I talk to think of them as "neutral" and, as we know, they are designed to determine people's behaviour. Is that something that you in your capacity as teacher/informer—

Alice Webb: It is a really good question. We cover some of those areas. "Absolute Genius" was a show specifically designed to unpack those ideas. This goes back to my Forth Bridge analogy. We can absolutely do more of that, and I will take that away and have a look at it, too.

The Chairman: Alice, colleagues told us that you would bring us all kinds of really useful and positive stuff, and you have, so thank you very much indeed for spending an hour with us. It is much appreciated.

Alice Webb: It is my real pleasure and, as you can tell, it is something that I feel strongly and passionately about. It is a huge responsibility on

all of us for children, so thank you for giving me the opportunity to come and talk to you.

The Chairman: Thank you very much.

BBFC – written evidence (CHI0025)

1. The British Board of Film Classification (BBFC) welcomes the Lords Select Committee on Communications decision to undertake an inquiry into Children and the Internet.

2. The BBFC is the independent regulator of film and video in the United Kingdom. It operates a transparent, trusted classification regime based on years of expertise and published Classification Guidelines. The BBFC conducts regular large scale public consultations to ensure that its Guidelines continue to reflect public opinion. The BBFC's primary aim is to protect children from harm through classification decisions. It also empowers consumers, particularly parents and children, to make informed viewing choices through consumer advice and education.

3. The BBFC is a member of the UK Council for Child Internet Safety (UKCCIS) Executive Board and works with international partners on projects to improve the protection of children from potentially harmful media content online.

4. Below is the BBFC's response to those inquiry questions relevant to its work:

Risks and Evidence

1. What risks and benefits does increased internet usage present to children, with particular regard to:

i. Social development and wellbeing;
ii. Neurological, cognitive and emotional development;
iii. Data security

5. The BBFC believes that it is too easy for children and young people to access inappropriate and potentially harmful content online. The regulatory framework that has developed in the offline world to protect children from content - for example dangerous and imitable behaviour, self-harm, suicide, drug misuse and violence - that is likely to impair their development and wellbeing has not transferred to the online space. Pornography is of particular concern. It is well regulated in the offline world but for the most part unregulated online.

6. Most online pornography accessible in the UK is unregulated and easily available to children in the absence of filters. A significant proportion of this pornographic content would not be classifiable by the BBFC (because for example it features content that would be deemed obscene under CPS guidelines; involves violence and/or implied lack of consent; involves the infliction of pain or acts which may cause lasting physical harm; or features material likely to encourage an interest in sexually abusive activity). This

has led to the normalisation of largely unfettered access to the strongest, sometimes unlawful, pornography by children online.

7. Research suggests that the impact of this new societal 'norm' has been significant and detrimental to the wellbeing of children and young people. The Government's consultation 'Child Safety Online: Age Verification for Pornography' highlights research that found 'adolescents who viewed violent pornography were six times more likely to report engaging in sexually aggressive behaviour than their peers who did not'.[14]

8. Girlguiding's 'Girls' Attitudes Survey 2015', a survey of young women aged 7-21, found that 'Seven in ten think that pornography gives out confusing messages about sexual consent, or that it makes aggressive or violent behaviour towards women seem normal (both 71%). Two in three young women agree that pornography puts pressure on girls to have sex before they are ready (66%)'. 53% of young women surveyed by Girlguiding also agreed that 'boys are copying what they see in pornography when they try to coerce their girlfriends into sex acts'.[15]

9. In its 'Briefing on Pornography and Violence Against Women and Girls' (July 2014) End Violence Against Women (EVAW) notes that 'pornography and sexualised popular culture form a conducive context for violence against women, contributing to messages about gendered stereotypes and sex which normalise men dominating women.'[16]

Education

5. What roles can schools play in educating and supporting children in relation to the internet? What guidance is provided about the internet to schools and teachers? Is guidance consistently adopted and are there any gaps?

10. Schools have a crucial role to play in educating children about accessing the internet safely and teaching resilience. When we speak to children and young people and carers, the issue of online safety frequently arises, in particular around the sheer volume of inappropriate material and the lack of clear guidance and advice for the public when they are navigating content online.

11. The BBFC Education Team seeks to promote resilience in schools through its education outreach programme. The BBFC speaks to over 10,000 people a year, more than 75% of whom are under 18. We also provide classroom resources and offer a dedicated children's website, www.cbbfc.co.uk. Through these various platforms, we explain to children,

---

14 'Child Safety Online: Age Verification for Pornography' February 2016, Department for Culture Media and Sport, page 8

15 Girls' Attitudes Survey, 2015, Girlguiding, pages 16-18

16 'Briefing on Pornography and Violence Against Women and Girls' (July 2014) End Violence Against Women (EVAW), page 4

parents and teachers how to find out about age ratings and make safe viewing choices online. The BBFC works in partnership with organisations such as Childnet to provide parents and children with guidance, including through Safer Internet Day. The BBFC's children's website (www.cbbfc.co.uk) supports the 5Rights charter and the BBFC is part of the committee driving the 5Rights project.

12. The BBFC will be extending the information it offers to both younger (primary school) audiences, and their parents, about making safe, empowered decisions online, following BBFC research into families and their viewing decision-making processes planned for later this year. The BBFC will use video, with supporting web resources, designed to promote safe viewing, demonstrate how to avoid potentially harmful unregulated content online, and incorporate the online safety messaging of partner organisations about responding to inappropriate content online. The BBFC is also developing classroom resources, including a poster and stimulus material, for secondary aged learners and their teachers. This will combine our expertise in using film and TV extracts to encourage discussion around content and age suitability. We will also share 'insider track' insight on what techniques members of our examining team use in order to develop resilience when viewing strong material.

13. The BBFC's education outreach programme also offers schools information on the Mobile Network Operators' (MNO) voluntary, best practice filtering scheme regulated by the BBFC, based on classifications that are well understood by parents. Schools are in a good position to proactively encourage parents of school age children to ensure filters are in place for any online access.

6. Who currently informs parents of risks? What is the role for commercial organisations to teach e-safety to parents? How could parents be better informed about risks?

14. The BBFC offers parents a system of classification which provides solutions in the online space with age ratings which are widely understood and trusted. These age classifications can then be applied to parental filters.

15. Since 2008, the BBFC has been working in partnership with the home entertainment industry and others to bring, as far as possible, offline regulatory protections online. In doing so, it uses a number of best practice, voluntary self-regulatory models that apply trusted BBFC standards in ways that best fit the business practices of different providers and the requirements of their consumers, particularly parents.

16. The BBFC's industry partners in the online space include:

- content providers from the home entertainment industry, music industry and adult industry, such as Portland and Playboy
- online platforms such as iTunes, Netflix, Amazon Prime and YouTube
- access providers, including all the UK's mobile networks.

17. These models involve the BBFC setting content standards and classifying material. Those standards and/or individual classifications are given effect through signposts for parents and consumers generally, including age ratings and content advice; parental controls linked to age ratings or standards; and internet filters.

18. For example, the BBFC is the independent regulator of content delivered via the UK's four Mobile Networks Operators (EE, O2, Three and Vodafone). Using the standards in the BBFC's Classification Guidelines, content that would be age rated 18 or R18 by the BBFC, is placed behind access controls and internet filters to restrict access to that content by those under 18. This includes pornography and other adult sexual content, pro-Ana (anorexia nervosa) websites and content which promotes or glorifies discrimination or real life violence. In 2015, the BBFC and EE also adopted a Classification Framework for EE's "Strict" parental setting, aimed at younger children, with filtering standards set at the BBFC's PG level.

19. The BBFC also provides an appeals service to respond in a transparent and timely way to reported cases of over and under blocking by access controls/filters. Customers may only remove the network filters on mobile devices if they are able to prove (using robust age verification methods, such as credit card or in-person verification) that they are aged 18 or over.

20. None of the above models offer a panacea, either individually or collectively. However, they do make a substantial contribution to online child safety and consumer empowerment, and have been welcomed by parents in particular. Independent research commissioned by the BBFC in 2015 found that 85% of parents consider it important to have consistent classifications off and online *(Bernice Hardie, 2015)*. The BBFC believes its commercial partners should be recognised for the way in which they have engaged with ratings and content advice in order to protect children. We look forward to continuing to work with industry to improve even further the use of BBFC symbols online, particularly to help parents filter content and set parental controls.

21. In terms of how these systems could be improved to ensure parents are better informed, the BBFC has argued for a more consistent approach across different media. For example, the current protections provided by MNOs based on BBFC classifications differ from those offered by public WiFi or home broadband. These different approaches and standards can lead to regulatory confusion which is not conducive to child protection.

Legislation and Regulation

9. What are the regulatory frameworks in different media? Is current legislation adequate in the area of child protection online? Is the law routinely enforced across different media?

What, if any, are the gaps? What impact does the legislation and regulation have on the way children and young people experience and use the internet? Should there be a more consistent approach?

22. The BBFC classifies films and videos works according to its Classification Guidelines, with ratings ranging from 'U' for Universal to 'R18'. The BBFC's Guidelines are the result of extensive public consultation, involving over 10,000 people across the UK in the 2013 Guidelines consultation. Research demonstrates that the public agrees with the BBFC's classification decisions more than 90% of the time (*Bernice Hardie and Goldstone Perl, 2013*). The 2013 Guidelines consultation found most respondents - 84% of parents with children aged 6-15 - consider that the BBFC is effective at using classification to protect children from unsuitable content. 89% of parents (and 76% of teenagers) rate classification as important, and 95% of parents with children under 15 usually check the BBFC classification.

23. While the BBFC's classifications have statutory force for video works and film exhibition, the BBFC has no statutory power online. However, independent research in July 2015 commissioned by the BBFC shows that the majority of viewers still consider it important to be able to check the suitability of audiovisual content they download. As more viewing takes place online, consumers expect that the same level of regulation will apply online as currently applies offline. 85% of parents consider it important to have consistent BBFC classifications available for Video-on-Demand (VOD) content, rising to 91% of parents whose youngest child is under 10. *(Bernice Hardie, 2015)*.

24. As stated in response to question 6, in recognition of these public demands for regulatory protection online, the BBFC has worked in partnership with the home entertainment industry on a number of voluntary, best practice self-regulatory services which bring trusted BBFC classification standards and well known age ratings online. The BBFC provides labelling and content advice for content providers and platform owners (aggregators). This service covers VOD, Download To Own, Streaming and all forms of Electronic Sell Through. The BBFC has rated over 200,000 videos for online distribution, with BBFC ratings used by platforms such as iTunes, Netflix, Amazon, TalkTalk TV Store and BT TV. Displaying BBFC labelling enables consumers to make informed choices when purchasing digital video, thereby empowering parents to protect their children.

25. The BBFC considers that, when protecting children from harmful content online, the three most pressing concerns are as follows: first, online pornographic content; second, online music videos; and finally, greater consistency of approach for online filters.

A. Online pornographic content

26. The BBFC classifies all pornographic content released on a physical format. It will not classify material that is potentially harmful or otherwise illegal, including so-called 'rape porn'. The BBFC's regulation of pornography offline is well established and largely effective at preventing access by children.

27. Online the situation is quite different. The BBFC works with a small number of UK adult content providers in the online space on a best practice, voluntary basis, to ensure that their content meets UK standards of acceptability and that it is kept away from children. The BBFC also supports Ofcom's work under the Communications Act 2003 to regulate online 'TV-like' adult content hosted in the UK by determining the standards that Ofcom applies and advising Ofcom in individual cases.

28. However, the work described above covers only a small proportion of pornographic content that is accessed in the UK. Most online pornography accessible in the UK is unregulated because it is hosted elsewhere in the EU or from outside the EU (particularly the US). It is therefore easily available to children in the absence of filters. A significant proportion of this content would not be classified by the BBFC if it was offline (because for example it features content that would be deemed obscene under CPS guidelines; involves violence and/or implied lack of consent; involves the infliction of pain or acts which may cause lasting physical harm; or features material likely to encourage an interest in sexually abusive activity).

29. The BBFC therefore welcomes the inclusion in the Digital Economy Bill of clauses that seek to ensure effective age verification by all commercial sites containing pornographic material to restrict users to those who are 18 or over. The Bill also places an obligation on the age verification regulator to review whether such sites contain content that would either not be classifiable in the UK or would be illegal. The BBFC agrees with Government that although no system to protect children from such content can ever be 100% effective, robust age verification is an important child protection measure that will reduce the chances of children accessing pornography online.

B. Online Music Videos

30. There are serious public concerns regarding online music videos which are not covered by the BBFC's statutory remit under the Video Recordings Act (VRA). For example, whilst the majority of music videos are appropriate for children, a report jointly commissioned in 2014 by EVAW, Object and Imkaan concluded:

> 'Some have argued that music videos use conventions of pornography: they are constructed around a 'pornographic imagination', featuring 'pornographic performances'. The ways in which women's bodies are relentlessly dissected and displayed makes music videos a form of 'everyday pornography', because they are based on 'representation of

> something which is recognised as pornographic in a context which is not itself pornographic'. This everydayness is precisely what concerns many, since music videos are integrated into everyday environments'.[17]

31. The report continues:

> 'Findings from studies that examine the impact of music videos are consistent and persuasive in highlighting associations between representations of women as sexualised body parts, and attitudes that condone sexual violence. Similar correlations are well documented in the evidence of access and exposure to pornography with respect to young people.'

32. In October 2014, the BBFC, the UK's three major record labels, Vevo and YouTube launched a pilot project with Government support for the age rating of online music videos featuring content that is unsuitable for younger children. (It is worth noting that the experience of this pilot suggests that a significant majority of music videos released by the UK's major record labels are suitable for younger children.) In August 2015, the Government announced that the UK music industry, Vevo and YouTube had agreed that the measures trialed with the BBFC would be made permanent for videos produced by artists signed to major UK labels and that independent labels would also pilot this voluntary initiative.

33. Clear age ratings are the first step to improve child protection with online music videos and were welcomed by the public in independent research into the pilot commissioned by the BBFC in 2015. The research found that:

- up to 60% of children aged 10 to 17 were watching music videos that they did not think their parents would approve of
- 78% of parents value age ratings on online music videos
- 75% would like online channels to link those ratings to parental controls
- there was a clear preference for more online platforms to carry BBFC ratings and for US labels in particular to be included in the age rating of online music videos *(Bernice Hardie, 2015)*[18]

34. The BBFC is therefore working with Government, the music industry and platforms to improve the effectiveness and coverage of online age ratings. However, the lack of coverage for videos by US-repertoire artists in particular is a serious gap in protection. The BBFC believes that if there is no further progress towards including any potentially harmful content by

---

17 'Pornographic Performances': A Review of Research on Sexualisation and Racism in Music Videos' by Dr Maddy Coy, July 2014, page 4

18 'Online Music Video rating Research Findings', pages 4 & 15

these artists the Government needs to set a deadline to ensure that US repertoire artists are included in the scheme. It also believes that video hosting platforms such as YouTube should improve signposting for ratings and consider linking them to effective parental controls.

C. Greater consistency of approach for online filters

35. As stated in response to question 6, it is vital that parents understand and respect the basis on which parental filters operate. There is presently a lack of consistency of approach across different platforms. The BBFC believes that its work with the MNOs represents a trusted and transparent system that is based on standards that are thoroughly researched and have widespread public support and could be used on other platforms.

10. What challenges face the development and application of effective legislation? In particular in relation to the use of national laws in an international/cross-national context and the constantly changing nature and availability of internet sites and digital technologies? To what extent can legislation anticipate and manage future risks?

36. There are significant technical challenges to the regulation of content online. In particular, the BBFC considers the issue of encryption to be of crucial importance. Encryption of websites is starting to degrade the child protection measures put in place by, for example, the MNOs and the BBFC as filters find it difficult to cope with the https protocol. In addition, increasingly children are downloading content through Apps and this also limits the effectiveness of any parental filters.

11. Does the upcoming General Data Protection Regulation take sufficient account of the needs of children? As the UK leaves the EU, what provisions of the Regulation or other Directives should it seek to retain, or continue to implement, with specific regard to children? Should any other legislation should be introduced?

37. In May 2016, the Commission published its proposal for amendments to the Audiovisual Media Services Directive to increase regulatory scrutiny of video on demand services and video-sharing platforms. Currently, the Directive only requires video on demand platforms to put in place measures to protect children from content that might "seriously impair the physical, mental or moral development of minors" (Article 12). Under the country of origin principle, this standard is set by the Member State in which the video on demand service is located. The proposed amendments retain this principle but increase the proportion of content on video on demand services that is subject to regulation to include any content which might "impair" rather than "seriously impair" children. To a lesser extent, video-

sharing platforms would also be required to implement measures to protect children from harmful content.

38. The BBFC welcomes the Commission's efforts to improve standards of online child protection and supports the decision to lower the benchmark to "impair". These proposals are likely to significantly increase the volume of content broadcast to UK consumers that is regulated on a statutory basis outside the UK. The BBFC is concerned that the implications of this new statutory oversight in other Member States have not been fully considered and have the potential to undermine current protections for UK children online.

39. Under the Commission's new proposals, it appears that UK consumers (including parents) would be required to address concerns about harmful content shown on a video on demand service to the regulatory body of the Member State in which the service is based. In most cases this would mean that a UK Regulator would not have jurisdiction to consider the complaint. This would confound the expectation of UK consumers who, based on the regulatory framework for linear broadcasters and the BBFC's system of classification, have a reasonable expectation that content is regulated according to UK standards that are set in consultation with the British public and enforced by a UK Regulator to whom they have the right to complain.

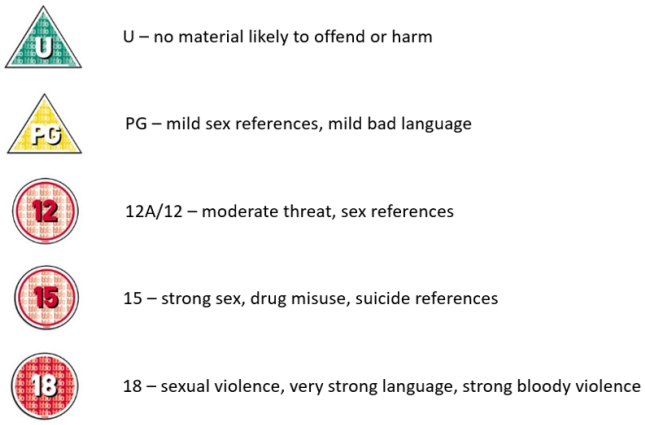
40. Under the terms of the proposed amendments, where the video on demand service is located in another Member State, the Regulator in that Member State would have no obligation to address the specific concerns and expectations of UK consumers with regard to content broadcast to the UK. Content standards set by other Member States differ markedly from UK standards on a wide range of issues, including dangerous imitable behaviour, pornography, sex, violence, language, self-harm and suicide. The Commission is also promoting the concept of developing an EU Code of Conduct for content descriptors which could be adopted by Member States across the EU which would be even further removed from reflecting national differences. Annex A contains a representative list of recent films and shows how age rating standards differ across the EU.

41. Currently, the BBFC works on a voluntary, best practice basis with all major video on demand services operating in the UK – many of them based outside the UK - to provide consumers with familiar, well understood and trusted age ratings and content advice. This voluntary system is based on UK standards expressed in the form of BBFC symbols and content advice and provides children with the level of protection expected by UK parents. Although there is no statutory basis for the BBFC's work with the platforms it is a logical extension of the BBFC's statutory role in the offline space and the BBFC believes its platform partners should be recognised for their commitment to offering the same high regulatory standards online which reflect the expectations of the UK public.

42. If the proposed amendments pass into EU law, the BBFC is concerned that the legal obligation on VOD services to comply with alternative, potentially

lower standards (set outside the UK, potentially on an EU-wide basis) risks the consequence that VOD services will be less willing to also engage on a voluntary basis to offer UK consumers more meaningful and helpful information. This would lead to a diminution of online child protection standards for children in the UK.

43. The Commission proposes that there should be a system of descriptors indicating the nature of the content on an audiovisual media service. The BBFC already provides this service for the home entertainment industry who have adopted BBFC classifications and content information voluntarily online as set out in our response to Question 9. Examples of BBFC symbols and BBFCInsight are set out below:



44. The British public would not be well served if these symbols and insight were replaced with unfamiliar age ratings and content descriptors online which would be treated with suspicion, poorly understood or ignored.

45. These EU Commission proposals could therefore inadvertently lead to a diminution of online protection standards for children in the UK. Instead of UK standards being reflected with UK symbols and content descriptors, the UK could move to VOD content broadcast to UK consumers with EU content descriptors and standards which are unlikely to offer the same level of protection or sensitivity to UK cultural norms. The UK has led the way in terms of child protection online and the BBFC believes the UK Government should continue to ensure that online child safety standards can be determined on a national level based on national standards.

46. It is unlikely that proposed amendments to the Directive will come into force before the expected date that the UK leaves the EU under the Article 50 process. However, the UK may opt to subscribe to the Directive on a voluntary basis or as part of a wider agreement on a free market in services. The BBFC notes that UK-based broadcasters consider the retention of the country of origin principle to be essential in securing their continued access to European markets and the BBFC would not wish to see the UK creative industry put at a disadvantage. However, the BBFC believes that the British public, in particular children, would not be well served by the regulatory framework proposed in the Directive in relation to protection from harmful content broadcast to the UK. The BBFC also

believes that retaining the country of origin principle in relation to broadcast rights is compatible with establishing the right of any Member State (not just the UK) who wishes to set national standards for online child safety in line with public policy and what it considers will impair the physical, mental or moral development of minors in their own country according to national concerns and sensitivities.

47. The BBFC agrees with the Commission that more can and should be done in relation to User Generated Content (UGC), irrespective of the UK's relationship with the EU. EU Kids Online research shows that children are concerned about accessing unsuitable content on UGC video hosting services. There is no reason why action should not be taken immediately by video-sharing platforms to better protect children online.

48. The BBFC and its Dutch counterparts NICAM developed YouRateIt (YouRI) at the request of the Brussels-based CEO Coalition to make the Internet a better place for kids, led by the former Commissioner Neelie Kroes. YouRI is a tool that provides age ratings for user-generated content (UGC) available via online video-sharing platform services. The tool is a simple questionnaire, designed to be completed by those uploading videos onto a site, or by the crowd, or both. Those who use it are asked a series of questions about the content to be rated. The tool, and the methodology behind it, is scalable on a global basis. The questionnaire itself would be the same in each country or territory but it produces bespoke, national ratings and content advice that take into account cultural and societal differences. It is a low cost means of capturing the enormous, and rapidly expanding, amount of UGC content that is not currently being rated, and is not susceptible to being rated, under other models operated by ratings bodies around the world. The tool can also be linked to parental controls.

49. The BBFC and NICAM have recently completed a pilot project with the Italian media company Mediaset, and now need new global partners to develop and test the questionnaire. The BBFC is willing to offer its expertise to any platform that is considering developing its own bespoke ratings tool to protect children from harmful content. YouRI is a voluntary initiative that could be pursued by the UK Government irrespective of our relationship with the EU.

Annex A - Different EU Classification Standards – August 2016

TP/AL = the work is suitable for all; broad equivalent of U rating.
TP! = the work is largely suitable for all, but caution is advised; broad equivalent of PG rating

Title	Netherlands	Germany	UK	France	Austria	Denmark	Sweden	Ireland
360	16	12	15	TP	16	-	11	15A
2012	12	12	12A	TP	12	11	11	12A
10 Cloverfield Lane	16	16	12A	TP!	14	-	15	15A
100-Year-Old Man Who Climbed Out…, The	12	12	15	TP	12	11	11	15A
12 Years A Slave	16	12	15	TP!	14	15	15	15A
127 Hours	16	12	15	TP!	16	15	15	15A
13 Hours: The Secret Soldiers of Benghazi	16	16	15	12	16	15	-	15A
22 Jump Street	12	12	15	TP	-	-	11	15A
300: Rise Of An Empire	16	18	15	12!	16	15	15	16
Abraham Lincoln: Vampire Hunter	16	16	15	12	14	15	15	15A
Albert Nobbs	9	6	15	TP	-	7	15	15A
Alice in Wonderland	9	12	PG	TP	6	11	11	PG
All Is Lost	12	6	12A	TP	10	7	-	-

Amazing Spider-Man 2, The	12	12	12A	TP	12	11	11	12A
Amazing Spider-Man, The	12	12	12A	TP	10	11	11	12A
American Hustle	12	6	15	TP	10	11	11	15A
American Pie: Reunion	12	12	15	TP	14	7	7	16
American Sniper	16	16	15	TP	16	15	15	15A
American, The	12	12	15	TP	14	15	15	15A
An Education	AL	AL	12A	TP	-	7	-	15A
Anchorman 2	12	12	15	-	-	-	11	15A
Anomalisa	12	12	15	TP	14	15	7	15A
Apollo 18	16	16	15	TP	12	11	-	12A
Argo	12	12	15	TP	14	15	15	15A
Attack the Block	16	16	15	TP	14	-	15	16
Avatar	12	12	12A	TP	12	11	11	12A
Avengers, The	12	12	12A	TP	12	11	11	12A
Avengers: Age of Ultron	12	12	12A	TP	12	11	11	12A
Bad Neighbours	12	12	15	TP	14	11	11	16
Bad Teacher	12	12	15	TP	12	AL	AL	16
Batman v Superman: Dawn of Justice	12	12	12A	TP!	14	11	11	12A

Battleship	12	12	12A	TP!	12	15	11	12A
Beginners	AL	AL	15	TP	6	AL	AL	15A
Big Hero 6	6	6	PG	TP	8	7	7	PG
Birdman	12	12	15	TP	10	11	11	15A
Biutiful	12	16	15	TP!	-	15	15	15A
Black Mass	16	16	15	12	16	15	15	15A
Black Swan	16	16	15	TP!	16	15	15	16
Blackhat	16	16	15	TP	14	15	15	15A
Bling Ring, The	16	12	15	TP	14	11	11	15A
Blue Valentine	12	12	15	TP	-	15	11	16
Bounty Hunter, The	12	12	12A	TP	12	7	11	12A
Bourne Legacy, The	12	12	12A	TP	12	15	15	12A
Bridge of Spies	12	12	12A	TP	10	11	11	12A
Buried	12	16	15	TP!	-	-	15	15A
Butler, The	16	12	12A	-	-	11	15	12A
Cabin In The Woods	16	16	15	12	14	15	-	16
Capitalism – A love Story	9	6	12A	TP	-	-	-	PG
Captain America: The First Avenger	12	12	12A	TP	12	11	11	PG

Captain America: The Winter Soldier	12	12	12A	TP	12	11	15	12A
Carnage	12	12	15	TP	10	7	-	15A
Carrie	16	16	15	12	14	15	15	16
Chappie	16	12	15	TP	14	15	15	15A
Chernobyl Diaries	16	16	15	12	16	15	-	16
Chloe	12	12	15	TP	-	AL	-	16
Chronicle	12	12	12A*	TP	14	15	15	12A
Citizen Four	AL	AL	15	-	-	15	-	-
Clash Of The Titans	12	12	12A	TP	12	11	11	12A
Company You Keep, The	12	6	15	TP	10	-	7	15A
Conan the Barbarian	16	18	15	TP	-	15	15	15A
Contagion	12	12	12A	TP	12	15	15	12A
Counselor, The	16	16	18	TP!	16	15	15	16
Cove, The	12	6	12A	-	12	-	11	PG
Cowboys & Aliens	12	12	12A	TP	14	15	15	15A
Crazies, The	16	KJ (18)	15	TP	16	11	-	16
Crimson Peak	16	16	15	12	16	15	15	15A
Danish Girl, The	12	6	15	TP	12	11	11	15A

Dark Knight Rises, The	12	12	12A	TP	14	11	15	12A
Das Weisse Band [The White Ribbon]	12	12	15	TP!	12	11	11	15A
Dawn Of The Planet Of The Apes	12	12	12A	TP	12	11	11	12A
Deadpool	16	16	15	12	16	15	15	16
Deliver Us From Evil	16	16	15	12	16	15	15	16
Desert Flower	12	12	-	TP	12	-	-	-
Devil	16	16	15	TP	14	15	15	15A
Dictator, The	12	12	15	TP	15	11	11	16
Django Unchained	16	16	18	12	16	15	15	18
Don Jon	16	16	18	12	-	15	15	18
Dracula Untold	16	12	15	TP!	14	15	15	15A
Dredd	16	18	18	12	-	15	15	18
Drive	16	18	18	12	-	15	15	18
Due Date	12	12	15	TP	14	11	7	15A
Duke of Burgundy, The	12	-	18	-	-	-	-	18
Edge Of Tomorrow	16	12	12A	TP	12	11	11	12A
Elysium	16	16	15	TP	14	15	15	15A

End Of Watch	16	16	15	12	16	15	-	16
Enter the Void	16	KJ (18)	18	16	-	-	-	18v
Equalizer, The	16	16	15*	12	16	15	15	16
Everest	12	12	12A	TP	12	11	11	12A
Evil Dead	16	18	18	16	-	15	15	18
Expendables 2, The	16	18	15	12	16	15	-	16
Expendables 3, The	12	16	12A	TP	16	11	15	12A
Expendables, The	16	KJ (18)	15*	12	16	15	15	15A
Extremely Loud and Incredibly Close	12	12	12A	TP	10	11	11	12A
Family, The	16	16	15	TP	16	15	15	15A
Fast & Furious 7	12	12	12A	TP!	14	11	11	12A
Fifty (50) Shades of Grey	16	16	18	12	16	15	15	18
Fighter, The	12	12	15	TP	12	11	15	15A
Final Destination 5	16	18	15	12	16	-	15	16
Flight	12	12	15	TP!	12	15	11	15A
Four Lions	6	16	15	TP	-	15	11	15A
Frankenweenie	6	12	PG	TP	10	11	11	PG
G.I. Joe: Retaliation	12	16	12A	TP	12	11	11	12A

Gamer	16	KJ (18)	18	12	16	15	15	18
Get Him to the Greek	12	12	15	TP	14	-	11	16
Girl with the Dragon Tattoo, The [US]	16	16	18	12	16	15	15	18
Godzilla	12	12	12A	TP!	12	11	15	12A
Gone Girl	16	16	18	TP!	16	15	15	16
Good Day To Die Hard, A	12	16	12A*	12	14	15	15	15A
Great Gatsby, The	12	12	12A	TP	10	11	11	12A
Green Hornet, The	12	12	12A	TP	14	11	15	12A
Green Zone	12	16	15	TP	14	15	15	15A
Grey, The	16	16	15	12	14	15	-	15A
Grown Ups 2	6	6	12A	TP	8	AL	11	12A
Guardians Of The Galaxy	12	12	12A	TP	14	11	11	12A
Hail, Caesar!	6	-	12A	TP	6	7	7	12A
Hangover Part II	12	12	15	TP	14	11	11	16
Hanna	12	16	12A	TP	12	15	15	15A
Hansel & Gretel: Witch Hunters	16	16	15	12	-	15	15	15A
Harry Potter and the Deathly	12	12	12A	TP	12	11	11	12A

Hallows Pt 1								
Harry Potter and the Deathly Hallows Pt 2	12	12	12A	TP	12	11	11	12A
Hateful Eight, The	16	16	18	12!	15	15	-	18
Her	12	12	15	TP	12	7	AL	15A
Hitchcock	12	12	12A	TP	10	11	11	12A
Hobbit, The: An Unexpected Journey	12	12	12A	TP	12	11	11	12A
Hobbit, The: Desolation Of Smaug	12	12	12A	TP	12	11	11	12A
Horrible Bosses	12	16	15	TP	14	11	11	15A
Horrible Bosses 2	12	12	15	TP!	14	7	11	15A
Hotel Transylvania 2	6	6	U	6	6	AL	7	PG
Hunger Games, The	12	12	12A*	TP!	14	11	11	12A
Hunger Games, The: Mockingjay Part 1	12	12	12A	TP	12	11	11	12A
Hunger Games: Catching Fire, The	12	12	12A	TP	12	11	11	12A
Hunger Games: Mockingjay Part 2, The	12	12	12A	TP	12	11	11	12A

I Spit On Your Grave (remake)	16	18	18*	-	-	-	-	18
Imitation Game, The	12	12	12A	TP	8	11	11	12A
Immortals	16	16	15*	TP	14	7	AL	15A
Impossible, The	12	12	12A	TP	12	15	15	12A
Inbetweeners, The	12	16	15*	TP	14	11	-	16
Incendies	16	12	15	TP	-	15	-	15v
Inception	12	12	12A	TP	12	15	15	12A
Informant, The	AL	12	15	TP	6	AL	-	15A
Inherent Vice	16	16	15	TP	16	15	15	16
Insurgent	12	12	12A	TP	14	11	15	12A
Interstellar	12	12	12A	TP	12	11	11	12A
Intouchables [Untouchable]	12	6	15	TP	6	7	7	15A
Iron Man 2	12	12	12A	TP	10	11	11	12A
Iron Man 3	12	12	12A	TP	12	11	11	12A
It Follows	16	12	15	12	16	-	15	15A
Jack Reacher	12	16	12A*	TP!	16	15	15	12A
Jack Ryan: Shadow Recruit	12	12	12A	TP	14	15	11	12A
Jackass Presents: Bad Grandpa	12	12	15	TP	16	11	11	16

Jeune & Jolie	12	16	18	12	16	-	-	18
John Carter	9	12	12A	TP!	10	11	11	12A
John Wick	16	16	15	12	16	15	15	16
Jurassic World	12	12	12A	TP!	-	11	11	12A
Karate Kid, The	12	6	PG	TP	6	11	11	12A
Kick-Ass	16	16	15	TP!	-	15	15	16
Kick-Ass 2	16	18	15	12	-	15	15	16
Killing Them Softly	16	16	18	12	-	15	-	18
King's Speech, The	AL	AL	12A	TP	AL	AL	AL	12A
Kingsman: The Secret Service	16	16	15*	12	16	15	15	16
Kon-Tiki	12	12	15	-	10	11	11	-
Kung Fu Panda 3	6	-	PG	TP	6	7	7	PG
La piel que habito [The Skin I Live In]	12	16	15	TP!	16	15	-	16
Last Airbender, The	9	6	PG	TP	10	11	15	PG
Law Abiding Citizen	16	16	18	12!	16	15	-	16**
Lawless	16	16	18	12	-	-	-	16**
Life Of Pi	12	12	PG	TP	10	11	11	PG
Lone Ranger, The	12	12	12A	TP	12	11	11	12A

Looper	16	16	15	TP	14	15	15	15A
Love	16	18	18	18	16	15	-	18
Love and Other Drugs	12	12	15	TP	14	11	7	15A
Love Punch, The	6	-	12A*	-	-	-	-	12A
Lovelace	12	16	18	TP!	-	15	-	18
Lovely Bones, The	12	12	12A	TP!	14	15	15	12A**
Lucy	16	12	15	TP	14	15	15	15A
Machete	16	KJ (18)	18	12	-	15	15	18
Mad Max: Fury Road	16	16	15	TP!	16	15	15	15A
Maleficent	12	6	PG	TP	10	11	11	PG
Maps To The Stars	16	16	18	12	-	-	15	18
Martha Marcy May Marlene	12	16	15	TP!	16	15	15	16
Martian, The	12	12	12A	TP	12	11	11	12A
Master, The	12	12	15	TP	14	11	15	16
Maze Runner, The	12	12	12A*	TP	14	11	15	12A
Maze Runner: The Scorch Trials, The	16	16	12A*	TP!	14	-	15	15A
Melancholia	12	6	15	TP	-	15	11	15A
Men in Black 3	9	12	PG	TP	12	11	11	PG

Men Who Stare at Goats, The	12	12	15	TP	-	11	11	15A
Millennium: Mannen die vrouwen haten [The Girl With The Dragon Tattoo]	16	16	18	12	-	15	15	18
Million Ways To Die In The West, A	16	12	15	TP	14	11	11	16
Mission: Impossible - Ghost Protocol	12	12	12A	TP	12	15	15	12A
Movie 43	12	16	15	12	16	11	-	16
My Skinny Sister			15				11	
My Week with Marilyn	12	6	15	TP	AL	AL	AL	15A
Nanny McPhee And The Big Bang	6	AL	U	TP	6	AL	7	G
Nebraska	6	6	15	TP	-	-	7	12A
Need For Speed	12	12	12A	TP	14	11	11	12A
Next Three Days, The	12	12	12A	TP	14	11	11	12A
Nightcrawler	16	16	15	TP!	16	15	15	16
Ninja Assassin	16	KJ (18)	18	TP!	16	15	15	18
No Strings Attached	12	12	15	TP	12	AL	AL	15A
Noah	12	12	12A	TP	12	15	15	12A

Non-Stop	12	12	12A	TP	14	11	11	12A
Nymphomaniac: Volume 1	16	16	18	16	16	15	15	18
Nymphomaniac: Volume 2	16	16	18	18	16	15	15	18
Oblivion	12	12	12A	TP	12	11	11	12A
Oldboy (remake)	16	16	18	16	-	15	-	18
Only God Forgives	16	16	18	12!	14	15	15	18
Oz: The Great and Powerful	12	6	PG	TP	8	11	11	PG
Pacific Rim	12	12	12A	TP	14	11	11	12A
Pain And Gain	16	16	15	12	-	15	15	16
Pan	9	12	PG	TP	10	11	11	PG
Paranormal Activity	16	16	15	TP!	14	15	15	15A
Paranormal Activity 2	16	16	15	TP!	14	15	15	15A
Paranormal Activity 3	16	16	15	TP!	14	11	15	15A
Paranormal Activity 4	16	16	15	TP	14	15	-	15A
ParaNorman	9	12	PG	TP	12	11	11	PG***
Parkland	12	12	15	-	-	-	-	12A
Percy Jackson: Sea Of Monsters	12	12	PG	TP	10	11	11	PG
Piranha 3D	16	KJ (18)	18	12	-	-	15	16

Pirates of the Caribbean: On Stranger Tides	12	12	12A	TP	10	11	11	12A
Potiche	12	12	15	TP	6	AL	AL	15A
Predators	16	KJ (18)	15	12	14	15	11	15A
Prince of Persia - The Sands Of Time	12	12	12A	TP	10	11	11	12A
Prisoners	16	16	15	12	16	15	15	15A
Project X	16	16	18	TP!	16	15	11	18
Prometheus	16	16	15	12	14	15	15	15A
Purge, The: Anarchy	16	16	15	12	16	15	15	16
Raid 2, The	16	18	18	16	-	15	15	18
Rango	6	6	PG	TP	10	7	7	PG
Real Steel	9	12	12A	TP	10	11	11	12A
Red 2	12	16	12A	TP	14	11	11	12A
Resident Evil: Afterlife	16	16	15	TP!	-	-	15	15A
Resident Evil: Retribution	16	16	15	12	16	-	15	15A
Revenant, The	16	16	15	12	-	15	15	16
Rise of the Planet of the Apes	12	12	12A	TP	12	11	11	12A
Road, The	16	16	15	12	-	-	15	16

Robin Hood	12	12	12A	TP	12	11	11	12A
Robocop	12	12	12A	TP	12	15	15	12A
Room	12	12	15	TP	12	15	15	15A
Run All Night	16	16	15	TP!	-	15	15	15A
Salt	12	16	12A*	TP	14	15	11	12A
Sausage Party	16	16	15	-	-	-	11	16
Savages	16	16	15*	12	-	15	15	16
Saw 3D	16	KJ (18)	18	16!	-	15	15	18
Saw VI	16	KJ (18)	18	16	-	15	15	18
Scott Pilgrim vs. the World	12	12	12A	TP	10	11	11	12A
Scream 4 [Scre4m]	16	16	15	12	14	15	15	16
Secret Life of Walter Mitty, The	6	6	PG*	-	-	-	11	PG
Selma	16	12	12A	TP	12	15	15	12A
Serbian Film, A	-	18v*	18*	-	-	15	15	-
Sex and the City 2	12	12	15	TP	12	11	AL	15A
Sex Tape	12	12	15	TP	14	7	7	16
Shame	16	16	18	12	-	15	15	18
Sherlock Holmes	12	12	12A	TP	12	15	11	12A
Sherlock Holmes: A Game of	12	12	12A	TP	12	11	15	12A

Shadows								
Shutter Island	16	16	15	12	16	15	15	15A
Sicario	16	16	15	12	16	-	15	15A
Side Effects	12	12	15	TP	14	15	15	15A
Silent Hill: Revelation	16	16	15	12	-	15	-	16
Silver Linings Playbook	6	12	15	TP	8	11	11	15A
Sin City: A Dame To Kill For	16	18	18	12	16	15	15	16
Skyfall	12	12	12A	TP	12	11	11	12A
Social Network, The	12	12	12A	TP	12	7	AL	15A
Sorcerer's Apprentice, The	9	12	PG	TP	10	11	11	PG
Source Code	12	12	12A	TP	12	15	11	12A
Spectre	12	12	12A*	TP	12	11	11	12A
Spotlight	6	-	15	TP	6	7	7	15A
Spring Breakers	16	18	18	12!	16	15	15	18
Star Trek Into Darkness	12	12	12A	TP	12	11	11	12A
Star Wars: The Force Awakens	12	12	12A	TP	12	11	11	12A
Steve Jobs	AL	6	15	TP	6	-	-	15A
Stoker	16	16	18	12	-	-	15	18
Straight Outta Compton	12	12	15	TP!	-	-	11	16

Submarine	6	12	15	TP	-	7	AL	15A
Sucker Punch	12	16	12A	TP	16	15	11	12A
Suicide Squad	12	-	15	-	-	-	15	15A
Super 8	12	12	12A	TP	12	11	11	12A
Survival of the Dead	16	KJ (18)	18	-	16	-	-	18
Taken 2	16	16	12A*	TP!	16	15	-	12A
Taken 3	16	16	12A*	TP	16	15	15	12A
Ted	12	16	15	TP!	-	11	11	16
Ted 2	12	12	15	TP!	14	7	11	16
Teenage Mutant Ninja Turtles	12	12	12A	TP	12	AL	15	12A
Terminator Genisys	12	12	12A	TP!	12	11	11	12A
Theory of Everything, The	9	AL	12A	TP	6	7	7	12A
Thor: The Dark World	12	12	12A	TP	12	11	11	12A
Three Musketeers 3D, The	12	12	12A	TP	12	11	11	12A
Tinker Tailor Soldier Spy	16	12	15	TP	14	11	15	15A
Tintin And The Secret of the Unicorn	6	6	PG	TP	6	7	11	PG
Tomorrowland	12	12	12A	TP	16	11	11	12A
Total Recall	12	12	12A	TP	14	11	11	12A

Town, The	16	16	15	TP	16	15	15	15A
Transformers: Age Of Extinction	12	12	12A	TP	12	11	11	12A
Transformers: Dark of the Moon	12	12	12A	TP	12	11	11	12A
Tree of Life, The	9	12	12A	TP	10	11	11	12A
Tron: Legacy	12	12	PG	TP	10	11	11	PG
True Grit	16	12	15	TP	16	15	15	15A
Twilight Saga: Breaking Dawn Part 1, The	12	12	12A*	TP	12	15	15	12A
Twilight Saga: Eclipse, The	12	12	12A	TP	12	11	11	12A
Un Prophete	16	16	18	12	10	-	15	16
Unbroken	16	16	15	TP	14	15	15	12A
Visit, The	16	12	15	12	14	7	-	15A
Walk Among The Tombstones, A	16	16	15*	12	16	15	15	16
Wall Street 2: Money Never Sleeps	6	6	12A	TP	10	11	7	12A
We Need To Talk About Kevin	12	16	15	12	16	15	15	16
We're The Millers	12	12	15	TP	14	7	11	16

Where the Wild Things Are	9	6	PG	TP	6	-	7	PG
Wild	12	12	15	TP	12	15	11	15
Winter's Bone	12	12	15	TP!	14	15	15	15A
Wolf Of Wall Street, The	16	16	18	12	16	15	15	18
Wolfman, The	16	16	15	12	14	15	15	16
Wolverine, The	16	12	12A	TP	14	11	15	12A
Woman In Black, The	16	16	12A*	12	-	-	15	15A
World Invasion: Battle Los Angeles	12	16	12A	TP	14	15	15	12A
X-Men: Apocalypse	12	12	12A	TP	12	11	11	12A
X-Men: Days Of Future Past	12	12	12A	TP	12	11	11	12A
Young Adult	12	12	15	TP	10	11	-	15A
Zero Dark Thirty	16	16	15	TP	14	15	-	15A
Zombieland	16	16	15	TP	16	15	15	16

August 2016

BBFC and Committee of Advertising Practice (CAP) – oral evidence (QQ 87-97)

Tuesday 15 November 2016

Watch the meeting

Members present: Lord Best (The Chairman); Baroness Benjamin; Baroness Bonham-Carter of Yarnbury; Earl of Caithness; Bishop of Chelmsford; Lord Gilbert of Panteg; Baroness McIntosh of Hudnall; Lord Sheikh; Lord Sherbourne of Didsbury.

Evidence Session No. 7 Heard in Public Questions 87 – 107

Examination of witnesses

David Austin, OBE, CEO, British Board of Film Classification and Malcolm Phillips, Regulatory Policy Manager, Committee of Advertising Practice.

Q87 **The Chairman:** We welcome Malcolm Phillips, the regulatory policy manager of the Committee of Advertising Practice, CAP, and David Austin, chief executive of BBFC. I have to declare an interest. My brother chairs the Committee of Advertising Practice, CAP. Does anyone else have any declarations?

Lord Gilbert of Panteg: I am a consultant to Finsbury, a financial PR company, which advises Telefónica UK.

The Chairman: Malcolm and David, perhaps you would just introduce yourselves and describe briefly where you are coming from. We have the background in the CV material we have been given, but those watching from the outside—because this is televised—will not have it in front of them.

Malcolm Phillips: I am the regulatory policy manager for the Committee of Advertising Practice, which is the sister body to the Advertising Standards Authority. CAP sets the standards that ASA enforces. The ASA is public facing and takes complaints from members of the public and industry about advertising. The CAP and BCAP committees set standards for advertising in broadcast material through the BCAP code and for non-broadcast material, including online, through the CAP code.

David Austin: I am David Austin, chief executive of the British Board of Film Classification and a member of the UKCCIS executive board. I have been CEO since March this year. The BBFC is the independent regulator of film and video in the UK, and its core mission is to protect children and empower consumers, particularly families, to make informed

decisions about what they view in both the physical and online world. Offline, our classifications have statutory force; in the online world, we have developed a number of voluntary best practice self-regulatory initiatives with a range of industry partners, in response to public demand, to bring trust in BBFC standards online. You will have seen that recently we have agreed with the Government in principle to be the regulator of online pornography in the UK under the Digital Economy Bill.

Q88 **Bishop of Chelmsford:** David, in a moment I may want you to say a little more about what you have just said. My first question is a general one to David. I want to quote from the evidence of the British Board of Film Classification. It says, "it is too easy for children and young people to access inappropriate and potentially harmful content online". A regulatory framework has been developed in the offline world to protect children, but although it is well regulated in the offline world, for the most part it is unregulated online. The general question is: what do you think are the greatest risks to children from online usage, but also what do you think are the greatest benefits?

David Austin: As to the risks, you can probably categorise them in three words: conduct, contact and content. At the BBFC, our focus is very much on protecting children from harmful content, whether it be online or in the physical space. In relation to online, there is a great range of content that could be harmful to children. Many of the offline protections do not exist online. We are working with a number of industry partners to try to provide, as far as possible, those protections online on a voluntary basis. For example, we are working with mobile operators in the UK to set the standard at which content goes behind adult filters. They apply our standards. When you take out a mobile phone contract, the filters are automatically turned on—we issue a default-on process—so parents can be reassured that when they obtain a mobile phone they do not need to think about child protection in relation to filters.

The core of all our online work is to try to bring offline protections online as far as possible. In many areas, self-regulation has worked well, but in other areas, as we have pointed out in evidence and as you said, they have not worked so well. Pornography is a key area where it has not worked well. In 2012, Claire Perry had an all-party parliamentary inquiry into online child safety. I said then that self-regulation could work to a large extent, but where industry would not engage—that was the case with the adult industry back in 2012—legislation would be required, so we are pleased that the Government have brought forward the Digital Economy Bill.

Bishop of Chelmsford: Before Malcolm has a go at the question, do you want to say anything about the benefits?

David Austin: I forgot about the benefits. I am not an internet evangeliser; I am a regulator. My goal is to protect children. There is a mass of content online that is great for children, and our role at BBFC is to help children access that great content without being exposed to harmful content.

Malcolm Phillips: That response indicates that perhaps the greatest risks to children online are not connected so much with advertising, but, relative to our remit, I think the ASA places particular emphasis on trying to prevent children from seeing content that might distress them or encourage irresponsible behaviour. One example is an ASA ruling on a case involving a trailer for a horror film that appeared on a games site as an ad before the games could be played. The audience for that site had a mixed profile and included young adults at whom the movie trailer was targeted but also younger children, and in that case the ASA upheld the ruling because they thought that too significant a proportion of the website's audience were children who should not have seen the ad. That is an example of the cases the ASA take most seriously because of the direct emotional impact on children.

Q89 **Lord Sherbourne of Didsbury:** Can I follow this up with a question directed to Mr Austin? Your evidence highlighted the fact that most online pornography accessible in the UK is unregulated—you have talked about this already—and this gives children online unfettered access to the strongest pornography. Can you spell out for us in some detail what powers you are being given in the Digital Economy Bill, and how far those powers will help you deal with the problem you have highlighted in your evidence?

David Austin: Would it help if I explain how we think regulation will work under the Bill as it stands? Our role will be to identify the most popular pornographic websites and apps accessed by children. Data is available so that you can see how many children are accessing which websites, so we will target the most popular with UK children. We will then ascertain whether it is pornography, because sometimes that can be disputed. Usually it is obvious if something is pornography, but not always. The first test is whether it is pornography. The second is: does the website or app have effective age verification? That does not mean just ticking "I am 18"; it has to be proper and effective age verification that can identify whether someone is an adult or child.

The second thing we are asked to look at under the Bill is whether the website or app contains any prohibited material. That is pornographic material that is either illegal under UK law or content that we will refuse to classify—for example, if it is released on physical DVD. That would be material that promotes an interest in abusive relationships, such as paedophilia or incest; material that features rape, or simulated rape; material that features violent abuse of women. This kind of content we will not classify, so we ask to look at the websites to see if they contain that material as well.

If the answer to either of those questions—does it not have effective AV, or does it have prohibited material?—is no, our duty is to notify the publisher of this pornography, wherever they may be. About 93% of pornography accessed in the UK is hosted overseas, a lot in the United States. We then contact that website or app owner to say, "You are acting in contravention of UK law. Please stop". Since the exchange of letters with the Government, we have started discussing these issues with some adult providers. We are confident that some will obey the

law—they have said that they want to obey UK law—but we know that some will not. We think we will get some compliance at that stage, but certainly not 100%.

We then have a second line of approach under the Bill. We are then required to contact the payment providers to see whether they can disrupt payments to that website or app and what the Bill calls ancillary service providers. Ancillary service providers are people such as ISPs, search engines and some social media sites. There is a whole range of organisations that facilitate the publication of pornography in the UK. As the Bill stands at the moment, we notify them, and under that notification we will ask them to withdraw their services. We cannot compel them to withdraw their services; we can ask them to do it.

I believe you heard evidence from Adam Kinsley of Sky that what the ISPs want is a clear legal requirement from the regulator to withdraw their services. That would be helpful to them and they would obey that instruction, but at the moment that is not in the Bill. Therefore, as part of the notification process, it would be helpful, from the child protection perspective, not just to have an ability to notify and request that an ISP withdraws its services and blocks a website but to notify and require it to do so. You have heard evidence from an ISP that it would prefer that. We certainly think it would increase the effectiveness of the Bill quite significantly. We know from our conversations with child protection groups that they would also like that requirement. An organisation called the Centre for Gender Equal Media did some research, published a few weeks ago, which showed that 78% of the public also think there should be a requirement. I am not a gambling man, but I believe that if a major publisher of pornography was sitting at this desk now they would most likely say that, yes, they also wanted to see compulsory blocking.

Lord Sherbourne of Didsbury: That is very helpful. If I were the Minister looking at the Bill and asking myself whether there was anything more I could ask you to do by way of further statutory powers or obligations in the online area, at least as an option, what would it be?

David Austin: We can achieve an awful lot with the Bill as it stands, because I think we can achieve an awful lot of voluntary compliance.

Lord Sherbourne of Didsbury: But in addition to what is in the Bill.

David Austin: In addition to that, if, as part of the notification process, we can require ISPs to block, that would be significant.

Lord Sherbourne of Didsbury: Would that be practicable?

David Austin: Yes. It happens in other spheres. The research on the effectiveness of blocking is pretty strong. There was some research published in the United States earlier this year in relation to ISP blocking for IP-infringing websites—for example, pirated films. The research found that there was a 90% reduction in traffic to those websites as a result of ISP blocking. The evidence published in the Government's consultation on this Bill highlighted that in one month in 2015, 1.4 million British children accessed a pornographic website. That is not 1.4 million visits; it is 1.4 million individual children. If you can reduce that by 90%, that is a significant child protection measure.

Lord Sherbourne of Didsbury: Is there anything else you want in addition to the Bill?

David Austin: The key thing is ISP blocking. That is the most effective measure in our view.

Baroness McIntosh of Hudnall: If I understand that bit of conversation, you are talking of blocking non-compliant websites that would fall outside permitted material. What about young people getting access to material that does not fall outside it? I still do not quite understand how that is going to be dealt with. You seem to be saying that lots and lots of young people access pornographic sites, for example. I imagine that not all of them are outside the law; plenty of them are not.

David Austin: All commercial pornographic websites come within the scope of the law. There are two things they need to do. First, they must have effective age verification. Secondly, they must not contain prohibited material. If they do not have effective AV or they have prohibited material and they refuse to co-operate with the regulator, we would look to the second tier: that is, payment providers.

Baroness McIntosh of Hudnall: You gave a rather alarming number; you referred to 90% of young people accessing this material.

David Austin: The 90% refers to the effectiveness of ISP blocking.

Baroness McIntosh of Hudnall: I see what you are saying.

David Austin: The 90% comes from ISP blocking in the United States. This is US research into ISP blocking of pirate websites. When ISP blocking was brought in to deal with pirate websites, traffic to those websites went down by 90%.

Baroness McIntosh of Hudnall: I understand that, but I am still puzzled by the stat you gave about the numbers of young people accessing this material.

David Austin: These are pornographic websites. This is a statistic I quoted from the Government's consultation document, which they launched in the spring.

Baroness McIntosh of Hudnall: But is that all sites: ie those that do have effective age verification? If so, it is not working. Or are you just talking about the sites that do not have that?

David Austin: I am talking about sites that essentially do not have effective age verification at the moment.

Baroness Bonham-Carter: I have a question about the degree to which it is accidental. The 1.4 million children, which I heard, are not searching for it; they are slipping into it, which is my experience of a young person.

David Austin: That data does not break down whether it is deliberately seeking porn or accidentally stumbling across it. The NSPCC and the Office of the Children's Commissioner earlier this year published research that highlighted the risk of inadvertent access.

Baroness Bonham-Carter: As to that, it seems completely obvious that there should not be the ability to do that. There should not be the ability anyway, but inadvertent access is something that should be looked at.

David Austin: I agree. The key thing that the Bill will achieve is preventing inadvertent exposure. If there is a determined tech-savvy teen who puts a proxy server in the loft, they will be able to access it, but we are talking largely about inadvertent exposure.

Q90 **Lord Gilbert of Panteg:** Can we turn our attention to advertising to children and young people? Therefore, it is Mr Phillips's turn. We have seen evidence that most younger children and many older ones fail to identify advertising particularly in search results. What evidence do you have about the age at which children become better at identifying advertising? If there is an issue, what more can be done to increase transparency so that children and young people are aware of advertising? Can you look across the internet, not just search results but website content?

Malcolm Phillips: This is an issue we are actively considering at the moment. The age at which children start to understand advertising appears to depend on what kind of advertising you are talking about. A lot of the classic studies about children understanding advertising were based on television advertising, but the internet involves greater and more sophisticated capacity for editorial and advertising to intertwine. Therefore, forms of advertising are now less obvious because they are less interruptible and less separated from editorial content.

It is important to note that it is not only children who require clarification where this happens. There are many cases before us about the intermingling of advertising and editorial content to adult audiences. There are also two separate but related issues here. One is the capacity of children to recognise an ad as an ad; the other is the question of children's understanding of persuasive intent, which is something else the studies we have been considering talk about. One needs to recognise that something is an ad, to adopt a more questioning approach and understand the persuasive intent of the communication. This is what we are considering now. We are in the process of developing guidance that we hope will address the kinds of communication where we think children are at greater risk of not recognising advertising and so not being able to activate their understanding of persuasive intent.

Our understanding from studies is that children's understanding of these issues develops most significantly between the ages of eight and 12. Interestingly, by the age of 12, children's understanding of advertising and their capacity to activate that kind of inquiring attitude begins to approach adult levels. Therefore, our guidance is going to focus on communications that might be targeting a younger audience or media consumed by younger children, and the focus will be on what we are beginning to think of as integrated or immersive advertising: that is, virtual worlds or advertising that mimics the website architecture around it, for example on a game site, or advergames. These are all things that have been studied and discussed by various academics working in the field of advertising.

Because of the dynamic nature of the internet, it is not always easy to get a current corpus of material to study: that is, before the eyes of children as you work. We have taken what we believe to be the appropriate time to work with industry to understand what is out there, and what kind of remedies might work for the techniques that are currently in place, because it is not always the same as the kinds of things that have been studied in the academic literature available to us. We hope to have a proposal for guidance towards the end of this year, or early next, to deal with this. It is likely to recommend enhanced disclosure to help children understand more clearly the nature of what they are seeing and explain to them a little more the context of what is happening.

Lord Gilbert of Panteg: Do you think the industry is open to that enhanced disclosure?

Malcolm Phillips: Absolutely. We have conducted working groups with the major parts of industry involved in advertising products of interest to children, such as the toy industry, but we have also worked with a CAP member, the Internet Advertising Bureau, which brings together different parts of the internet marketing industry, including social media platforms, agencies and so forth, to understand the more technological side of things, and we have had great co-operation.

Lord Gilbert of Panteg: You are going to make recommendations that impact at the point of content and the point at which it reaches children. Do you have recommendations on the role of wider education of children as to the nature of this content generally?

Malcolm Phillips: We collaborate with CAP members on educational resources. Most of the consumer education work is done by some of CAP's partners, such as the Advertising Association, which has a resource called Media Smart. They produce resources that are promoted through contact with schools and educators to try to educate children and young people on the internet and the issues connected with the use of it.

Q91 **Lord Sheikh:** We have discussed children of different ages. We were made to understand by the Internet Advertising Bureau that advertising regulations and self-regulation use different definitions and age-based categories from what we are discussing today. Do you think that the appropriate systems and advertising regulation are in place in regard to content to take into account different ages and stages of child development? Are there sufficient, proper systems in place bearing in mind the different ages of the children?

David Austin: If I may, I will speak first and then let Malcolm talk about advertising. In relation to content generally, yes. We have developed over many years a system for age categorisation. It is the core of what we do. We have age ratings going from U, meaning it is content suitable for everyone, all the way up to adults-only ratings.

Lord Sheikh: Are they in stages?

David Austin: We have developed these different ratings over many years and have refined them.

Lord Sheikh: In other words, it is one to five, or whatever. Is it categorised in that way?

David Austin: Our ratings are U, PG, 12, 15 and 18, and we have refined them over many years, with the help of the public. Essentially, we ask the public every four years. We go out and talk to 10,000 people and say, "What kind of content do you think is appropriate for children at these different ages?" We convert what they tell us into guidelines, and they form the basis of all our classification decisions. We also take input from child psychologists and people who are expert in how children develop from a young age to adolescence and beyond.

In addition to that expert advice, we incorporate advice in our classification policies from people such as the Samaritans, the NSPCC and selfharmUK, who are experts in particular areas. We are quite confident that we have a suite of age ratings. We know from our own research that those are quite well trusted. Eighty-four per cent of parents say that we do an effective job; and 76% of teens, many of whom are frustrated that they cannot see some of the content we have age rated, think we do an effective job and value what we do. We are pretty confident that the suite of age ratings we have developed has public trust.

Lord Sheikh: Is it a moving target? Would you tweak it, for example, depending on what is available?

David Austin: Yes.

Lord Sheikh: How do you do that?

David Austin: Every four years we go out to a major public consultation and look at what issues have arisen over the previous four years. Attitudes towards certain types of content shift. We started doing this public consultation in 1999. If you compare 1999 with 2016, you can see some quite big shifts in attitudes towards racism and other forms of discrimination and towards issues such as self-harm. I imagine that, when we do the next guidelines research in 2017-18, we will look at depictions of transgender issues in the media that were not an issue maybe 10 or 15 years ago. We track societal changes and changes in people's attitudes towards different types of content.

Lord Sheikh: It is important we do that because attitudes change and legislation changes. The legislation now compared with 20 years ago is quite different.

David Austin: Exactly. We track those changes and reflect public attitudes in our classification decisions on different emerging types of content.

Q92 **Baroness McIntosh of Hudnall:** I want to ask you about social media and the difficulty there must be in regulating the kind of material that gets uploaded on to Facebook, Twitter or whatever. I want to pull it together with what was talked about earlier. Mr Austin, earlier you raised the issue of piracy. It has been brought to our attention that a lot of young people use pirate websites and download from them, and those sites often contain advertising, sometimes of an extremely unsavoury

nature. Therefore, the general question is: how do you regulate video and advertising content on social media? Do you find that the platforms are willing to engage with you in trying to help that happen? More narrowly, on the issue of sites from which pirated material can be downloaded, do you have eyes on that and any thoughts about how that can be better regulated, or, to be more accurate, regulated at all?

David Austin: In terms of social media, our interaction with them is about to enter a new phase with our role under the Digital Economy Bill. Over the next few weeks and months, we will contact those social media outlets that allow pornography to encourage them to engage with us and see how we can work together to regulate pornography that appears on those social media outlets. We have not started yet; we have only exchanged letters with the Government recently, but we will be engaging with them on that issue.

Baroness McIntosh of Hudnall: Specifically on that issue, one thing that occurred to me when you talked earlier about pornography was the issue of user-generated content. Clearly, as far as social media sites, and pornography particularly in relation to those, are concerned, I assume that a lot of that will be user-generated.

David Austin: Yes.

Baroness McIntosh of Hudnall: Is that the kind of thing on which you are going to attempt to come to some sort of understanding with them?

David Austin: We will be looking at a range of pornographic content on their websites. In terms of user-generated content more generally, we were part of the CEO Coalition, which was created by the Commission in Brussels to make the internet a better place for kids. We were a third-party expert body on that. One of the things we were asked to do with our Dutch counterparts was to create a tool for age-related user-generated content on social media and video-sharing platforms. We have created that tool and have been trialling it in Italy for the past year. It has worked very well. Next week, we are going to Luxembourg to present to the Commission the outcome of that trial. We will be urging the Commission to encourage social media operators to look carefully at using this tool. It is a simple questionnaire.

The beauty for industry is that, if they operate in many territories, it is a single questionnaire that a member of the public, a crowd or the person uploading the video can complete. The beauty for the consumer is that that single output produces nationally sensitive ratings. So far, four countries are part of this project. In testing it, we have found that the same video content can produce different ratings. We looked at a pro-anorexia video that got an adults-only rating in the UK, but in the Netherlands it got a 12 rating. That reflects different societal concerns and national sensitivities about different bits of content. Therefore, the consumer in the UK, Netherlands or wherever they are, would get a rating they understand and would reflect their sensibilities. For industry, it is a single tool. We have trialled it and it has worked very well. We are presenting the results to the Commission next week, and we would very much like social media platforms and video-sharing platforms to look carefully at using this tool.

You asked about piracy. We were part of a campaign about 18 months ago to highlight to children the risks of going on to pirated websites. They might want to watch a pirated film but there is all sorts of other content. It is not regulated by us by definition; it is a pirate website, and there is a risk of coming across content that potentially could be quite harmful to them. We were part of this campaign. We go to schools around the UK and among the things we talk to students about is how to avoid potentially harmful content online, and piracy websites are places where they can come across content that is very problematic.

Baroness McIntosh of Hudnall: Since you are engaging in that quite actively in trying to bring that to people's attention, could anything be done at a more national level, or possibly even at government level, equivalent to a public health campaign, that would more effectively and widely bring that kind of danger to the attention of more people?

David Austin: There are a lot of campaigns already with lots of people engaged in informing children and protecting them online. We are just part of a much bigger ecological system represented by organisations such as ChildNet and InternetMatters that are set up by the ISPs, Baroness Kidron's 5rights and all sorts of people. A good place for all this work to come together, as it does, is UKCCIS. I sit on its executive board, but there are many members of UKCCIS who are not part of the executive board. UKCCIS has a number of working groups. I have been part of some of them—the BBFC continues to be part of some of those working groups—that look at things like building resilience. How can we help educate children to be resilient when online? What are the technical solutions? What are the educational solutions? UKCCIS brings together regulators, child protection groups, education experts, researchers, industry and government. This is a really good forum for developing helpful tools. I think you heard evidence from Ofcom a couple of weeks ago about the social media guidelines. That was something on which we worked as well under UKCCIS. I think UKCCIS is a very good body for co-ordinating this work.

Bishop of Chelmsford: Do you think it could be done?

David Austin: If you are asking me whether we should create a single portal for parents to go to for everything, my answer is that that might not be the answer. We tried it in relation to something called ParentPort. This was a recommendation by Reg Bailey's independent report on the commercialisation and sexualisation of childhood. One of the things he recommended and government encouraged all regulators to do was the creation of a portal where, if you had any concern about a particular issue, be it advertising—the ASA was part of this—a video game, broadcast TV, film, video or cinema, you could go to that portal, but the experience of all the regulators is that the public know where to go to complain or give feedback. From the BBFC's perspective, most of the feedback from the public continued to come to us directly rather than through ParentPort. We have established mechanisms. There is certainly scope for raising awareness of these, but whether there should be a single place for everyone to go I am not convinced.

Q93 **Baroness Bonham-Carter of Yarnbury:** Advertisers are obviously

about building up databases, building brand loyalty and so on. One assumes that, the younger they get you, the longer they have you, as it were. How do advertisers obtain data about online usage, and to what degree are they constrained, or not, by the age of the people they are obtaining data about?

Malcolm Phillips: The CAP code follows ICO guidelines in prohibiting advertisers from collecting information from web users under 12 without parental consent.

Baroness Bonham-Carter of Yarnbury: How can that be possible? I understand the point about prohibiting targeting, but how can you stop data being garnered?

Malcolm Phillips: I think the primary force of this rule is in places where there are online accounts or sign-in, but another important provision in the code relates to online behaviour and advertising where information related to web use is collected through cookies. Third parties, advertising agencies, collect online information about web users by planting cookies on browsers. It is possible in some cases to identify the age of a user by the kinds of interests they display. Our rules say that for interest segments, which are the plans that ad agencies use to target web users with particular products they think will be of interest to them, you cannot create an interest profile for under 12s; you just should not be targeting online behavioural advertising at an under-12 audience.

One of the concerns over time is that the capacity of anyone to identify child web users is imperfect at best, particularly during a period where children's access to the internet was mainly through a shared computer in the family home. One of the interesting positive developments over the past few years is that the increase in the use of smartphones and tablets means that children tend to have their own accounts; they access the internet individually. While that obviously carries risks as well, it does have benefits in terms of making it easier for people to identify a child internet user and modify their targeting accordingly.

In terms of online behavioural advertising, you talk about the idea of getting people early. When we speak to agencies involved in online behavioural advertising, they tend to think of their engagements in much more short-term ways, even when dealing with an adult audience. They are really interested in what any web user is looking for at that particular time when they are online.

Baroness Bonham-Carter of Yarnbury: Really?

Malcolm Phillips: They understand that that changes.

Baroness Bonham-Carter of Yarnbury: They do not have long-term plans.

Malcolm Phillips: One week it might be one thing; another week it might be something else. That is the real use of online behavioural techniques; it is display advertising featuring products. There are other methods of developing brand loyalty in the longer-term relationships you were talking about. Perhaps social media is one of the places where advertisers try to do that, but the information that is gathered and used

to target individual web users is much more about individual purchasing decisions on a very quick sequence.

Baroness Bonham-Carter of Yarnbury: I think you are saying that this is imperfect at its best. What is your view of business models that do not rely on advertising? Is that a reality?

Malcolm Phillips: I understand that they exist. We do not take much of a formal position on them at the ASA. I suppose Netflix, or a subscription service for audio-visual media content, would be an example. We tend not to take a view on those. There are circumstances where a subscription model can rely partly on advertising. I suppose there are examples of audio-visual media service providers that use their subscription information to target advertising to their audience. That is something in which we would obviously take an interest, but I guess we are content to leave alone a service where there is no advertising.

Baroness Bonham-Carter of Yarnbury: It is a good thing.

Malcolm Phillips: We are content to leave it alone.

Baroness Bonham-Carter of Yarnbury: Quite. Are there measures in place to prevent children being inappropriately targeted by advertisers?

Malcolm Phillips: Yes. I think the rules that I have mentioned on online behavioural advertising are relevant. We also have rules that address particular sectors where we think it would be inappropriate for advertisers to target children. We have rules that prevent advertisers from using children's media to promote gambling or alcohol, for example. Those work in tandem with content restrictions that we think mitigate the risk of children coming across those ads in media of broader appeal with a broader audience. It is important to have those two systems in place from our point of view.

Q94 **Earl of Caithness:** Can I take you on to parental filtering controls? We have had a range of evidence. I would be interested to know whether you think that the UK system, which is slightly unco-ordinated, although it is a voluntary system among the four top providers, is a good one. Would you prefer there to be a set system that works throughout all the providers?

David Austin: You are right to highlight that different providers have different systems, not just the four main ISPs. There is another system for public wi-fi; there is another system for the mobile network operators, which is the area in which we have expertise. You need to look at filters generally in the context of other measures. It is a technical measure among others, such as age verification. There are other issues, such as education and building children's resilience, which all contribute to making the internet a better place.

Our experience is that they are not enough on their own. They are imperfect, but they are by and large pretty good, but our experience is limited to the mobile networks where we set the standards of filters. When you take out a mobile phone contract, the filters are turned on and the standards that they apply are determined by the BBFC. We derive that standard from our large-scale public consultations. Essentially, we

ask the public what content should be blocked for children and what content is okay for them to see. We publish those guidelines and rely on the mobile network operators and the filtering companies that work for them to apply them. They do a pretty good job, but filters are not as good as humans in reaching nuanced decisions, so we have a backstop power to deal with difficult cases.

I will give you an example. One difficult case that we had involved the website Dignity in Dying. The filters identified this as a pro-suicide site. Dignity in Dying contacted us as the regulator and said, "Please take a look at our site. We are not a pro-suicide site", and we did. We agreed with Dignity in Dying. It is a legitimate organisation that is campaigning for a change in UK law about assisted dying. It is not a pro-suicide site. The kind of debate it is encouraging is one you would have in GCSE studies at school. It is not limited to adults. We said we would not classify this content as 18 and asked the MNOs to remove the adult filter, and they did. That is a kind of hard case where we get involved.

We think the MNO system works well; it is a default on. When, as a parent, you are taking out a contract for your child, you do not need to think about whether the filters are turned on, or what security safety measures you need to think about, because it is already taken care of. For an adult, it is easy to remove the filters; if you want to you can do so. At the moment you take out the contract you can say, "Can I tick the box to turn off the filters?" or at a later date you can contact them, give your credit card details and get the filter removed. Therefore, it is easy to get it removed. The MNOs find that that system works very well. We think it works well, and we are very happy to continue to work with the MNOs on the basis that we set the standards, deal with hard cases and the default is on.

Earl of Caithness: What do other countries do? What does America do for parental filters?

David Austin: I am not sure. I can check for you. The UK leads the world in filters. The ISPs have done a very good job. They all have slightly different filters. The MNOs have done a very good job, so we do lead the world. One area where I think we could improve the effectiveness of filters is public wi-fis in a café, restaurant, shop, or outlet where children can be present. There is an organisation called the Registered Digital Institute, which is essentially the regulator of wi-fi in these places. They will give a tick to anyone who has a friendly filter. The minimum standard an operator needs to have for a friendly filter is that it does not allow pornography—the RDI, with whom we work closely, takes our definition of pornography—and it will not carry images of child sex abuse; and on that it is advised by the IWF. Anything else is fair game for the minimum standard.

Many public wi-fi providers operate a higher standard that is much closer to our published guidelines for mobile network operators, but some do not. Therefore, the risk is that if you are a child out in the street and you are on your mobile network—02, 3EE, Vodafone—and go into a café and switch to the wi-fi, the level of protection will be different and often lower, never higher. We think there is a case for standard public wi-fi, in

order to get the tick, to align much more closely with our standard for mobile operators.

Earl of Caithness: Would that be easy to introduce?

David Austin: It could be done. A dialogue would be needed with public wi-fi providers, but many of them already operate to a much higher standard than the minimum standard.

Earl of Caithness: What happens to your mobile network providers if they do not comply, even with your little rap over the knuckles? What is your ultimate sanction?

David Austin: I would not say it is a rap over the knuckles. We work very closely and co-operatively with them. They want us to regulate them. They have said, "We have a headache. We are applying different standards. You are the experts. Take away the headache". We have a contract with all of them. The contract says that if we say that content would be rated 18 or higher, they are contractually obliged to put it behind adult filters. They always have. If we say that it does not need to go behind filters, such as Dignity in Dying, they have the option to keep it behind filters because they might want to operate an even higher standard of protection, but they never have. In every single case, they have followed what we have asked them to do.

Q95 **Baroness McIntosh of Hudnall:** Can I ask about public wi-fi providers? What you say is really interesting, because it is a very wide-ranging opportunity for lower standards to be applied. What would be the downside for those providers in introducing, as a matter of standard practice, a higher level of filtering? You said you thought they would have to be persuaded, and I am struggling to understand what they would be losing.

David Austin: Personally, I do not think they would be losing anything. I would need to have the conversation with the RDI who would be able to advise me better because they work more closely with these providers. We do not work with them; we work just with the mobile network operators, but technically it is definitely doable. All the mobile networks do it, and there is no technical reason why public wi-fi providers cannot do it.

Baroness McIntosh of Hudnall: Is there an economic downside to them?

David Austin: I cannot immediately think what it would be.

Baroness McIntosh of Hudnall: Good; thank you. I thought you might say that.

Q96 **Lord Sheikh:** We are discussing an international issue, because obviously other countries have similar problems. Are you liaising on what you and our European counterparts are doing to see if you can achieve some conformity? The problem applies to all countries.

David Austin: We work quite closely with a number of regulators around the world, many in Europe, the United States, Australia, New Zealand, Singapore and Korea.

Lord Sheikh: Are the standards different from ours?

David Austin: The standards are different. Each country has its own. There is the famous play "No Sex Please, We're British". We tend to be stricter in the depiction of sex than, say, the Scandinavians. The Germans tend to be stricter than anyone else in relation to depictions of discrimination and violence, given their 20th-century history. Everyone has different standards. As part of our written evidence, we have provided examples of how those standards can be different, but we can all learn from one another. Many of the methodologies and systems we use are very similar. We get together at least once a year with regulators from around the world and share best practice. Some of the innovations that we have adopted in the UK we have copied from other countries. I am going to South Korea next week to talk to the Koreans, Australians and representatives of a number of other countries in Asia about how they deal with online content and help to protect children online, so we are learning from one another all the time. Across the board, the UK probably has better and more comprehensive child protection than most other countries.

The Chairman: There may be an EU dimension to this.

Q97 **Baroness Benjamin:** Thank you for all the work you have done so far. With regard to our link with Europe, what are the BBFC's concern regarding the audiovisual media services directive? Are there some changes you would recommend the directive do to ensure that it does not lower protection standards for children in the UK, because it seems to look at things quite differently from the way we want to look at them? What is your view?

David Austin: The European Commission has brought forward proposals for a new audiovisual media services directive. One of the key goals behind the new proposals is to increase child protection online, and we very much support that. One of the things we argued for in our evidence to the Commission was a "seriously impair" test. Any content that would seriously impair the development of minors should be put behind access controls. That test has been reduced to "impair", so there is a clear desire to improve child protection. We think the methodology they are proposing, in which one member state would regulate for all the other 27, is not the right way forward in terms of child protection. We think there could be a risk of a rush to the bottom and VOD services moving to an EU member state where the protections are less stringent than elsewhere.

Baroness Benjamin: Who will decide which state will regulate?

David Austin: It will depend on where the VOD service is based. For example, we have seen that to an extent in relation to the adult industry. The Government have introduced legislation that requires Ofcom to regulate pornographic VOD in the UK. It does a very effective job. The result has been that many UK publishers of pornography have moved to the Netherlands where the rules are less stringent. We think there is a risk of a rush to the bottom and that British children are not best served by it. We think there is a risk that the protections we have designed, in partnership with industry, which have been developed

painstakingly over many years to achieve good online protection, will be disrupted and destroyed by a well-meaning desire to improve child protection.

Probably the best way of explaining it is that, if you look at a graph of where different EU member states are, we are near the top and there are some near the bottom. The Commission is bringing up the bottom and in doing that the risk is that they bring down our levels of protection. We think the Government should look at a derogation from the country of origin principle in relation to child protection only. We are not suggesting there should be a blanket derogation, because the country of origin principle is very important for the EU and for UK broadcasters, for example, who want to be able to provide their content all around the EU but, in terms of child protection, we would like to see a derogation to enable the British public to benefit from the existing protections they enjoy rather than see those protections diminished.

Baroness Benjamin: If we are not part of Europe, would that make it more difficult for us?

David Austin: When we are not part of Europe, presumably we would have the option of signing up to the AVMSD, in which case we would still need that derogation, or we would not sign up to it, in which case we would not need it because our standards would continue to apply.

Baroness Benjamin: But the material will still be able to come into this country.

David Austin: Yes, but if it was regulated by Ofcom according to UK standards that is better than not.

Baroness Benjamin: How could the BBFC or others work to prevent unsuitable user-generated content coming here?

David Austin: As to user-generated content, I talked about the tool we have developed with our partners in the Netherlands that we have been trialling in Italy. We think this is a very inexpensive and easy way of enabling platforms operating in many countries to have a robust system for age rating user-generated content. When we designed this tool, one thing we considered really important—the Commission said it had to be in there—was a report abuse button. If you see content on a video-sharing platform that you think is beyond the pale, you can press that button. In the Italian experiment we did—we would see it working on other platforms—that would send a message straight to the compliance team of that platform. They can take a look at the video and see whether they think it is beyond the pale, or not. We think it is a really good system. We have developed it over a couple of years and it has now been trialled. We would like to recoup some of our costs. We are a not-for-profit organisation, but, frankly, we would give it away. If people want to use it, we would give it away.

The Chairman: I am afraid we are out of time. Can I ask Malcolm Phillips whether he has any final thoughts he wants to share with us? Are there areas of greater collaboration and centralisation of resources from the perspective of advertising that might better protect children?

Malcolm Phillips: We welcome the opportunity to be here today, and what we look forward to most is a continued dialogue on regulatory matters connected with advertising and the protection of children, which is at the heart of what we try to do with the ASA and CAP system.

As to collaboration and centralisation of resources, David has probably pointed the way, in the sense that our experience, in common with the BBFC, is that people know where to come. We feel reassured that people know where to come to complain about advertising in the UK. We operate a one-stop shop for advertising complaints. While we are keen to continue to explore the possibilities that things like ParentPort might present, we feel that people know where to come to express their concerns about what their children might be seeing online.

The Chairman: Thank you both very much for a really helpful session. We have covered a lot of ground.

BBFC - supplementary written evidence (CHI0064)

Digital Economy Bill, Part Three: Regulation of Pornography Online

1. In the BBFC's original written evidence to the House of Lords Communications Committee 'Children and the Internet' Inquiry, we welcomed the inclusion in the Digital Economy Bill (DEB) of clauses that seek to ensure effective age verification by all websites that make pornography available commercially, to restrict users to those who are 18 or over (paragraph 29). These provisions will reduce the risk of children and young people accessing, or stumbling across, harmful pornographic content online.

2. On 6 October 2016, the BBFC exchanged letters of understanding with Government which will mean that if the Bill is passed, the BBFC will be the age verification (AV) regulator. Under the current terms of the Bill, the BBFC will be responsible for determining which websites to target. It will then assess these websites to determine (i) whether robust age verification is in place and (ii) whether it contains pornographic content that is prohibited. If a website is deemed to be non-compliant the BBFC will initiate a notification process to achieve compliance. The BBFC is also entitled to review Apps and social media accounts that make pornography available commercially.

3. Once a non-compliant website has been identified, the AV regulator may request that payment providers and ancillary service providers (ASPs) withdraw services from a non-compliant website for as long as it refuses to comply with the terms of the law. ASPs are those organisations that facilitate and enable the making available of pornography online. Social media platforms such as Twitter are ancillary services providers under the Bill.

4. On 28 November 2016, at Report Stage of the DEB in the House of Commons, an amendment to the Bill was passed, tabled by the Secretary of State, Karen Bradley MP, which would also give the BBFC the power to direct internet service providers (ISPs) to block access to pornographic websites that have been notified that they are operating in breach of UK law but refuse to offer effective age verification or remove "prohibited" material.

5. Research from the USA demonstrates that ISP blocking of websites with pirated content drove down traffic to piracy websites by approximately 90%[19]. The BBFC therefore believes that this new enforcement power will have a significant impact on the effectiveness of the DEB to protect children from harmful pornographic content.

6. There are 1.5 million new pornographic URLs coming on stream every year[20]. However, the way in which people access pornography in the UK is

[19] http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2612063 and http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2766795

[20] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/541366/AV_ConsultationDCMS_20160216_Final__4_.pdf, p.33

quite limited. 70% of users go to the 50 most popular websites[21]. With children, that percentage is even greater; the data suggests that they focus on a relatively small number of websites. The BBFC will develop a proportionality test to assess which websites to target in order to achieve the greatest possible level of child protection. The BBFC would focus on the most popular websites accessed by children in order to have the greatest impact.

Robust Age Verification

7. To fulfil the child protection objectives of the Bill, the BBFC will check whether a website has appropriate age verification procedures in place to ensure children cannot access pornographic content. These AV procedures must establish whether the person seeking access to the website is 18 or over, but not their identity.

8. The BBFC, as the AV Regulator, will publish Guidance about the types of arrangements for making pornographic material available that comply with the terms of the Bill. The BBFC will need to determine that the procedures in place are effective in establishing that the person is over 18 – a simple tick box exercise will not suffice.

9. This Guidance will also indicate the standards that the AV solutions need to meet to comply with best practice in terms of privacy and data security. The BBFC is currently consulting experts in this field including the Information Commissioner's Office (ICO) to ensure that the Guidance for AV solutions complies with all relevant UK law including the Data Protection Act, the Human Rights Act and with the General Data Protection Regulation when it comes into force.

10. AV is already used widely online and there are a range of solutions - for example, for UK regulated Video-on-Demand pornography - that already adhere to UK law. The BBFC is considering the most appropriate mechanism to audit AV schemes.

11. If a website meets the AV standard then it will be deemed compliant under the terms of the DEB, unless it contains "prohibited" content.

Prohibited Content

12. The Digital Economy Bill aims to create parity of protection online and offline. In making any assessment of online pornographic content, under the terms of the Bill, the BBFC will therefore apply the standards used to classify pornography that is distributed offline.

13. Under the Video Recordings Act 1984 the BBFC is obliged to consider harm when classifying any content including 18 and R18 rated sex works. Examples of material that the BBFC refuses to classify include pornographic works that: depict and encourage rape, including gang rape; depict non-consensual violent abuse against women; promote an interest

[21] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/541366/AV_ConsultationDCMS_20160216_Final__4_.pdf, p.33

in incestuous behaviour; and promote an interest in sex with children. The DEB defines this type of unclassifiable material as "prohibited".

14. Furthermore, under its letters of designation the BBFC may not classify anything that may breach criminal law, including the Obscene Publications Act (OPA) as currently interpreted by the Crown Prosecution Service (CPS). The CPS provides guidance on acts which are most commonly prosecuted under the OPA. The BBFC is required to follow this guidance when classifying content offline and will be required to do the same under the DEB. In 2015, 12% of all cuts made to pornographic works classified by the BBFC were compulsory cuts under the OPA. The majority of these cuts were to scenes involving urolagnia which is in breach of CPS guidance and could be subject to prosecution.

15. All the BBFC's classifications are assessed according to the BBFC Classification Guidelines which are based on large-scale public consultation and supplemented with expert research. The last review of the Classification Guidelines in 2013 involved more than 10,000 members of the public from across the UK.

Non-Compliant Websites

16. If a website that is making pornography available on a commercial basis is deemed by the BBFC to be non-compliant either because it refuses to put in place robust AV or because it refuses to take down "prohibited" material, the BBFC may notify ASPs and payment providers to withdraw services; and require ISPs to block the website. These services would be restored once the website had informed the BBFC that it had complied with the notification and this compliance had been audited by the BBFC.

December 2016

Dr Dickon Bevington, Dr Henrietta Bowden-Jones and Dr Angharad Rudkin – oral evidence (QQ 11-17)

Evidence Session No. 1 *Heard in Public* *Questions 1 - 17*

TUESDAY 19 JULY 2016

Members present

Lord Best (Chairman)
Lord Allen of Kensington
Baroness Benjamin
Baroness Bonham-Carter of Yarnbury
Earl of Caithness
Bishop of Chelmsford
Baroness Kidron
Baroness McIntosh of Hudnall
Baroness Quin
Lord Sheikh
Lord Sherbourne of Didsbury

Examination of Witnesses

Q11 The Chairman: Thank you for joining us. We move to part two and welcome to each of you. Before we get into our questions, would you say a few introductory words about yourselves so that we have it on the record. Dr Bowden-Jones, would you go first?

Dr Henrietta Bowden-Jones: I am a consultant psychiatrist. I am the founder and director of the National Problem Gambling Clinic, the only NHS service for pathological gamblers in this country, and I am the spokesperson on behavioural addictions for the Royal College of Psychiatrists.

The Chairman: Thank you very much. Dr Bevington?

Dr Dickon Bevington: I am Dr Dickon Bevington. I am a consultant child and adolescent psychiatrist. I work in the NHS in a substance use service for adolescents and I am medical director of the Anna Freud National Centre for Children and Families, which is a charity developing the next generation of psychosocial treatments and running a lot of training, mainly for statutory services around the country.

The Chairman: Thank you. Dr Rudkin?

Dr Angharad Rudkin: My name is Dr Angharad Rudkin. I am a clinical psychologist and I work with children and families who experience mental health

issues, behavioural difficulties and emotional difficulties, and I teach clinical psychology at the University of Southampton.

The Chairman: I thank all three of you for joining us. We will not be requiring my colleagues to declare their interests. You may have heard them already because we have done that in our first session. Lord Sheikh is going to start us off.

Lord Sheikh: All three of you have backgrounds in psychiatry and psychology. I want to ask about mental health issues relating to children. When they look at violent video games and the sharing of information, there are many instances where there has been self-harm. Are there any particular elements of children's online access that you have seen that are having a detrimental impact on their mental health and well-being? Do they differ according to the age group? Perhaps, Dr Bevington, you would start.

Dr Dickon Bevington: The simple answer is yes, there is evidence of harm. This is a very broad field. One of the main findings that is worth bearing in mind is that, although there is evidence of harm from pornographic sites, bullying and some of the other social media interactions, many children are exposed to material that they describe as upsetting and distressing at the time but are not harmed. One of the features of exposure to extreme internet-mediated experience is that it is a particularly good filter for children with pre-existing vulnerabilities. Those may be pre-existing genetic vulnerabilities—children with neurodevelopmental disorders, who are rather impulsive, who rush into things, who may already have a history of vulnerability and bullying, and be traumatised through their upbringing. They certainly may be children with a vulnerability in relation to low parental responsibility for knowing where they are and what they are doing. In one sense, the internet is extremely different in the threats that it offers, but, in another sense, it is extremely similar. It simply filters children who have high levels of vulnerability for genetic or environmental and upbringing reasons.

Lord Sheikh: Does it differ according to the age group?

Dr Dickon Bevington: Yes. There is growing evidence that those children who develop significant problems with internet-related behaviours are classically engaging in the internet in unhelpful or harmful ways at younger ages, which is incredibly similar to the history of young people who develop, say, substance use problems. The earlier you start your use of substances, the more the risk of you developing lifetime, chronic and severe problems. It is very similar to exposure to extreme content on the internet or exposure to bullying influences, which I agree from the previous evidence is often the highest preoccupation of young people. It may be that that is what they bring to people like myself rather than the pornography.

Lord Sheikh: Could it have a long-term effect where the child would be affected for a longer period or would it go away with counselling?

Dr Dickon Bevington: It is difficult to answer that in very general terms. A single traumatic incident could be very successfully treated if the child has good parental support, is able to access help and has parents who can bring them to treatment, and a pre-existing psychology that they have some trust in their

helpers. For most of the children who get into real problems around the internet, going back to my previous point, you have already filtered the ones who have low levels of family support or psychological attunement to help. They tend to be children who are less able to make use of help, certainly in ways that it is offered conventionally as a treatment. There was a recent study in 2014 in one area looking at compulsive sexual behaviour. There were very clear connections looking at young adults. It was quite a small sample of about 20 non-problematic young adults and 20 with compulsive sexual behaviour and a quite significant misuse or harmful use of the internet. Those very much fulfilled the criteria that I was talking about, and that, potentially, is quite a long-term problem, not just for them with a great deal of suffering but for the people they interactive with through life, and can be very difficult to treat.

The Chairman: I am not going to ask all of you to answer all the questions because we will run out of time, but do please come in whenever you feel like it.

Dr Henrietta Bowden-Jones: That is a very good explanation, and I share a lot of those thoughts. Going back to this suicide risk, it is important to focus on the idea of the internet as a place that may exacerbate pre-existing thoughts that were present, potentially, in a subclinical way. As Dickon has mentioned, you may have a child who is socially withdrawn because of environmental circumstances or, indeed, potentially psychiatric ones, but let us think about someone who is in a situation in which they cannot access help immediately. We know that children with low mood are more susceptible to becoming vulnerable to internet addiction, for example, and those children can distance themselves from their support networks and enter into another reality, because they are nowadays able to choose specific chat groups that may be particularly focused on low-mood depression, self-harm or, potentially, suicide. I have had patients in my clinic who have learned about suicide and self-harm from peers on the internet. These are people who, in the past, might have instead shared their troubles with schoolfriends and might have been pulled out of it. Instead, you see a real fragmentation of the tapestry that held them afloat, and you see them sinking at a time when people around them are less aware of what they are thinking because they are withdrawing. Actually, the withdrawal and the turning to the internet to lift one's mood at a time when things are very difficult are part of the criteria we look at through the diagnostic questions we ask.

Dr Angharad Rudkin: I agree very much with what has been said, but, thinking about the developmental trajectories during childhood and adolescence being a particularly tricky time, as we all know, and that need to explore, that curiosity and that increase in risk-taking, when that is happening on the internet, this is part of the issue that we have to deal with. The very normal developmental trajectory is taking place in a different arena.

I work with young people. I have four distinct categories of the internet with which or around which I work. The first is social media, the second is gambling and gaming, the third is pornography and the fourth is the internet as being an incredibly rich resource and incredibly wonderful database for young people to access, be creative with and explore. When I am working with young people, certainly of a younger age, part of those four would be more important than when I am working with adolescents.

Bishop of Chelmsford: I wanted to come in at a slightly different angle, which I am not sure we are covering in any of our questions elsewhere. We are inevitably focusing on some of the damaging effects from particular issues and people, but I am wondering about the very fact, for instance, of a very small child, under two, having a tablet and interacting with that with completely appropriate or age-appropriate material, not damaging material as such, but perhaps spending excessive amounts of time on it. What are the issues for child development in those very early, critical years? I gather some research has been done into these areas. I do not know much about it. I wonder whether you do.

Dr Angharad Rudkin: Yes, there is emerging research on it, and the use of devices with toddlers upwards is certainly increasing. Some research has shown that it increased by about 15% even between 2014 and 2015. It is becoming very much the norm for toddlers to spend time on their mother's or father's iPhones or tablets. Parents do this in an educational role. They believe that somehow these apps, games or videos are enhancing the child's educational capabilities, but I guess we cannot ignore the fact that there is a babysitting aspect to the internet and these devices with young children as well. We need to very much build on the information and advice there for parents on how much and what should happen. Certainly, in America, for example, there is advice that they should have absolutely no access up to the age of two, and thereafter two hours a day, but it is not based on any evidence. It is very much based on opinion. It is very much based on fear of change for all of us. This is not anything that we had to deal with when we were younger. We need to help build up a very good, robust evidence base, which helps us—professionals and parents—to make some informed decisions about whether if my two year-old watches a video for 15 minutes it is going to cause harm or is going to help them. What is it going to do? Certain research has shown video deficit theory, for example, where young people do not learn from videos in the same way that they do when they are interacting face-to-face with people. The concern is that these are not interactional activities. The young person—the child—will not be chatting; they will not be communicating or interacting. They are purely passively watching. It has been found that there is a slightly different effect in terms of learning from that as opposed to watching and chatting to your mum, your sister or a nursery worker.

Q12 Baroness Benjamin: Moving on from that, we all know that you can become addicted to certain behaviour patterns, such as smoking, drinking and shopping. There has been some research done that found that four out of 10 children are becoming addicted to the internet. Some children like taking their tablets to bed with them, and they would rather speak to their friends online or view sites online, and are not engaging with human beings. Is this an exaggeration or should we be worried about the issue of children being addicted to the internet? Have you seen an increase in the cases reported to you recently about this behaviour pattern?

Dr Angharad Rudkin: Before handing over, all I would say is that, for children, the immediate gratification is how they live, basically. Their sense of being able to delay gratification for a longer-term benefit is not quite within their cognitive capacities when they are young. So, for children having an immediate thrill from eating sweets and cakes, and similarly from consuming videos, games and TV programmes, it is very hard for them to understand that that is causing or may cause some long-term issues. Parents have to deal with young people who love

the immediate gratification that they get from getting through a different level on a game or from watching a "Peppa Pig" film or whatever, and being able to realise that, if you do this all day long, this may impair your development. We are not quite sure yet, but it may have an impact on it. It is very hard for young people to appreciate that. When I am working with young people, they say, "I just cannot turn my phone off. I just cannot stop playing these games". It is because they do not yet have the capacity to think, "If I do this now, then in five years' time I am not going to be very pleased that I did it". That is where parents as police, mediators and regulators all come in, and that is what causes a lot of family issues.

Dr Henrietta Bowden-Jones: Again, I would like to emphasise everything that you say. Taking it a step further, there is very good work from a Professor Jeff Derevensky at McGill University, who has looked at the potential priming of children's brains in relation to the games they are playing online now from an early age and how that might feed into the impulsivity that they already experience because of the late maturation of the frontal lobes, but it might also make them into human beings who are much more sensitive to a dysregulation of the reward pathways and more vulnerable to things such as pathological gambling, for example. Although no money is exchanged, there are continuous dopaminergic rushes in the brain as these children are constantly moved from one activity to the other with small rewards that are not monetary but are still relevant within the game. I just wanted to add that, because that is a body of work that is extremely well-respected around the world.

Going back to the addiction, we need to be a bit careful when we read about relatively small studies talking about an epidemic of internet addiction. I pick up on the European conversation we had. We need to measure excessive internet use, which is necessary but not available as yet, and I would like to stay away from addiction, because with children it is far more complex. They may be focusing on one of the criteria but to such an extent that they are suffering academically, et cetera. We need to identify the best possible screening tool and try to collaborate with our fellow European colleagues to find out exactly what the prevalence is at the moment. There are studies showing anything from 1.5% in Holland to 8% in Asia. I leave out the Asian countries, because I think they genuinely have higher prevalences. I have travelled and have spoken at various meetings there. They do see a higher prevalence, and there are clinics set up by the Government in various places to treat these issues. Again, they are issues that arise because of several other things, potentially, that are not quite right in these children's lives, but it is a fact that they are scoring highly when they are screened.

In England and in Europe, for example, with gambling, there is four times the prevalence in children as in adults because of the higher levels of impulsivity, as we talked earlier, and then there is a spontaneous remission for three-quarters of them, and you end up with a very vulnerable lot who continue to be pathological in adulthood, or you might end up with different adults who were not pathological as children. This gaming and this internet addiction as a whole is an issue that we not know enough about. We are not investing enough focus in terms of research and we are certainly not treating them in an evidence-based way, which therefore does not give us the understanding that we could have.

If I think of the National Problem Gambling Clinic, now that we are publishing data on 1,000 to 1,500 people, we know—we understand—the illness in England as it is now in our patients. We cannot do that with this particular presentation because we do not have the evidence base.

Dr Dickon Bevington: The only thing I would add would be to underscore this idea that it is a little premature for us to draw conclusions about the harm of spending time on the internet. However, we are absolutely clear, and have been for a long time, that it is what you are missing out by spending time on the internet that might be the more important bit. In particular, in the very early years, how do we develop a sense of ourselves? How do we develop these communicative capacities? All the evidence is absolutely robust that it is about what we call the intersubjectivity. It is me making a gesture of distress to my mother, my father or a carer, and seeing my mother or father imitate that distress back to show me that they have understood my state of mind, and then come up with something that might address that state of mind. That teaches me a couple of things. No. 1, it starts bit by bit every five minutes, every 10 minutes, every hour, and gives me a sense that I have a mind, which can be a happy mind, an excited mind, a frightened mind or an angry mind, and my parents are showing me this through this reciprocity. I show them something; they show it back to me in a slightly modified way that I can see, "You have understood me", and I begin to get this sense that I am an agent in the world and I have a mind that has different states. That is what you do not get if you are on a screen all the time.

Baroness Benjamin: One of the problems a lot of children have is that they count how many friends they have following them on Facebook as important and they go crazy if their phone or tablet dies on them. That is something that I feel, in a way, is almost becoming an addictive-type behaviour or fear of not being liked or wanted or feeling important.

Dr Dickon Bevington: I do agree with Henrietta. We have to be very careful with words like "addiction".

Baroness Benjamin: What would you call it then if it is not addiction?

Dr Dickon Bevington: I just think we have to be careful before we collapse it all into something that may or may not be exactly the same. The qualities of an addiction are: do you need more of the same to get the same effect? In other words, do you become tolerant to that thing? Do you have withdrawal effects? There are whole categories of things that we would use to judge addiction, which generally have not been used in the age groups of two, three, four and five years old. I treat children with substance use addictions, and, with regard to some of the ways in which those play out, my threshold for concern may be rather low compared with an adult treater, because, clearly, the young person is having their addiction in the middle of a developmental trajectory that is like an aeroplane taking off at the end of the runway. At the end of the runway there are things such as getting GCSEs, being able to fall in and out of love with a bit of grace, and having the social competence to go and do a job interview. If those years when you are trying to get that flightpath right are interrupted by formal addiction or excessive use of the internet without all the other things that you need to get those skills in place, then you are in trouble.

Dr Henrietta Bowden-Jones: It is a continuum, and harmful use is a very helpful term. It is harming the individual. They have lost their friendships; they have fallen behind at school; sometimes I see people who have opted out of school altogether because of sitting in their room playing video games. They may be extremely distressed and depressed, and now on anti-depressants because, as you say, they are overly concerned with people's opinions about them on social media. All these things are very real and can absolutely destroy an individual, a child, in their attempts to be who they want to be during a particular school year or within a family. But, when we look at addiction itself, there are a certain number of criteria according to diagnostic guidelines that need to be reached in order for the addiction itself. If you look at it as a continuum, by the time things are very severe, the children I have seen are in their room day and night; they are having their meals at home in their bedroom, not with the family any longer. They have now fragmented away from the nuclear family. They have lost weight. They are not exercising. Their mood is very low. They spend time being excited online and often then jump from gaming to porn to other types of sites that are very dark, and they have lost sight of who they are. They have no resilience, essentially. By that point, I would agree with you that addiction is there.

Interestingly, even with these young people, often dealing with the environmental issues gets them better much faster than just focusing in a cognitive behavioural way on the activity of being online. When they have enough trust in you, they themselves will say, "I am so unhappy with everything. I would not be gaming if my life was better" or "if my parents treated me in a different way"—often, bullying comes into this—or "if I was not bullied". Bullying is the worst thing for this, because people literally hide away physically from any companionship, any schoolground, whatever, and they have gaming as an excuse.

The Chairman: We are on question 2.

Dr Henrietta Bowden-Jones: We are passionate about what we do.

The Chairman: My colleagues are passionate about asking you questions. We do not want to draw to a close at the end of question 3. I say to my colleagues that we will not do supplementary questions to you, and I say to the three of you please be as precise as you can, if you would. Let us go to question 3.

Q13 Lord Sherbourne of Didsbury: To change the subject a little, Dr Rudkin, you talked about the great advantages of the internet being the access to a database and information in a way that, before, the internet was not available to us. It is a fantastic benefit. My question is this. I know that there has been some research done by Ofcom, but in your experience—I am not sure which of you to address this too—is there anxiety about what trust is placed in the sites that they visit, and what implications does that have for their future development, their critical thinking and critical faculties?

Dr Angharad Rudkin: Yes, and I think it is trust that the young people put into the sites as well as the trust that the parents put into the sites. For example, when you think about WhatsApp, a vast majority of parents do not know that there is an age limit on it. They were not aware that you had to be 13 to be on WhatsApp. There is that sense that we are trusting as parents and young

people. Because it is there, it must be good. There is an awful lot of work to be done around regulation and education there. When we think of children as consumers, they are naive. Adults can be incredibly naive around consumerism as well. But there is something about having to give them the information and for them to be clever consumers around different sites.

When it comes to a media character, for example, that young people really enjoy and trust, suddenly they do not have any critical faculties when they are consuming something to do with that character.

Lord Sherbourne of Didsbury: Can I make my question a little more pointed, perhaps, so that I am clear? A lot of people in this country read one tabloid newspaper, which they trust hugely. They think it is accurate; they think its opinions are objective. A lot of us perhaps do not have that view of that particular tabloid. Their critical faculties, because they have trust in that particular tabloid, are not very great. Is there a difference between young people accessing the internet and sites and the example I have just given about a tabloid newspaper?

Dr Dickon Bevington: There are some similarities. There is some very elegant, rather new research that is looking at this idea about how we develop trust in another person or, rather, trust in the value of the social knowledge that they might have in their head that we might try out with other people in our life. How do I learn from you and apply things next door? Going back to what I was talking about, about this intersubjective experience, it is the extent to which when I look at you I have an experience that you have got me; you have understood my predicament here, now. The extent to which I get that experience from you opens probably an evolved mechanism that is quite unique to humans that says, "If you are that good at doing that and understanding me, then the other knowledge that is in your head is worth me trying out in the rest of my life". Why is this significant? As the children that we are talking about move on in life and might start to look for some site that recognises their dilemma, that is what biologists would call assortative mating. You tend to connect with people who are similar, more like-minded with you. The young people who have very significant drug and alcohol problems, when I ask them, "How serious do you think your problems are?", often say, "Kind of in the middle". You think, "Really". Of course, they are in the middle because they are doing it more socially, but their whole social world revolves around drugs and alcohol.

If you go on to one of the pro-anorexia sites, people share their desire for thinness and promote thinness as a way of life. Self-injury sites robustly argue that it is their form of self-expression and robustly resist people's attempts to say that this is a bad way of doing it. They will speak of their distress and their suffering in such a way that another young person who may be slightly earlier in the journey will think, "You are the first people I have met who actually get me", and they will trust them.

It is a technique not unknown to politicians, but tabloid newspapers use it very well too. You tell people what they are really distressed about, and then the message that you need them to take away and deliver elsewhere follows soon after. I do not think the people in these sites are necessarily doing this with such malicious intent, but it has this pernicious effect of collapsing people's worlds in the way that Henrietta has been talking about earlier. It is very seductive.

Dr Henrietta Bowden-Jones: Maybe you pointed to something that is a positive of the internet. There are plenty of teenagers nowadays who shop around and who are able to give you a much more balanced view than some people of our generation, and I think we need to accept that it is not all bad in any way.

Q14 Baroness Kidron: I would like to move the conversation on a little and talk about the design of the internet itself. Obviously, none of you is designing apps and websites—or maybe you are. But you talk very eloquently about opportunity costs, what you are not doing while you are on, or excessive use, which I would like to suggest is a norm for us all now. It is not very excessive and extreme use but a culture in which general use is excessive, possibly. In that regard, what would you like to see designed in? Even if you cannot do it yourselves, what are the elements? You have talked about reward loops, but what are the other elements? What would you like to see?

Dr Henrietta Bowden-Jones: Can I reply to that because I feel very strongly about this? Having spent the last seven years on the Responsible Gambling Strategy Board looking at prevention, looking at things that can help the vulnerable populations, there are things we can learn. Timeout is essential. I think timeout allows people a moment to get out of that tunnel and say, "Hang on a minute. I have just spent all my birthday money on eBay. Was that a good thing? Do I want to carry on?"

Particularly if the sphere of the internet is porn, when I see patients who turn up in terrible shame and guilt about the endless hours they spend—14 or 15 hours at a go; I am not talking about an hour or two—timeout would have absolutely helped them. I do not do the technical side, so I cannot say exactly how this can be done other than by forcing the provider of the material to offer timeout. "If you have been on this site for over two hours or an hour, please opt in to take 10-minute breaks, and opt in when you are not hot from the activity but cold before you start". It is the same in gambling. When your mind is so completely wrapped up with winning or losing and you are chasing losses, you have lost your critical faculties to decide how much money you have apportioned towards gambling as a recreational activity and you are way down into taking money from the mortgage to repay your debts. I do believe that is important.

There is a problem with this, particularly with more unregulated spheres, because people jump from site to site. They sometimes have various tabs open at the same time so that they look at different types of porn within the same hour or two. It becomes very hard to get timeout on everything.

If you establish it on your own device, then in the heat of the moment you are only going to move to a different tablet or a different mobile phone. I do not have the answer, but, neurobiologically, I know that we could save a lot of people a lot of problems if we asked them to take a moment of rest before they question whether they really do want to continue with an activity.

Dr Dickon Bevington: I know there has been an enormous amount of talk about this over the years and it has proved impossible, but it still strikes me as sad. This is the idea of a universal button—a sort of, "I am in too deep", or, "I am uncomfortable with this" button. CEOP has talked about it. I know various other organisations have. I think it has proved incredibly difficult. That would be at the level of the browser, and browser developers do not like other people

telling them where they should put their buttons. But a button that was universally recognisable would be a massive help that connected you to a fairly simple algorithm for finding the right kind of help. It is not beyond the wit of these organisations, I think, to go back to that and have another bit of a think about it. I know it has been talked about for years and has not happened.

Baroness Kidron: Did you have a quick wish?

Dr Angharad Rudkin: I suppose, thinking about subclinical populations where it is not particularly problematic, that people who are creating these apps, websites and forums should be aware of child development informational research so that they know exactly what kinds of things are going on for kids who are going to be accessing this information, whether they are adolescents, three year-olds or seven year-olds, and to have some very clear classification for parents who are introducing their children to these different sites.

Baroness Kidron: Do you mean age appropriateness? Do you mean age rating?

Dr Angharad Rudkin: Absolutely; information for parents.

Baroness McIntosh of Hudnall: I think you have answered one part of what I want to ask you already, but, listening to you, I am hearing that you are describing the internet and its many manifestations as an extremely effective tool for amplifying or exacerbating—which was the word you used earlier—vulnerability. Out of that, there is the question of what is cause and what is effect. The question of what should be done about it is quite problematic if we are not entirely sure what is cause and what is effect. However, that said, there is a general sense that something must be done, which affects all of us around these issues. Do you have a sense beyond what you have already said about who is or should be responsible for tackling—let us not call it addiction, because we are not sure whether that is what we mean—the harmful overuse of the internet? Whose responsibility is it or should it be to try to put some controls in place of the sort that you are describing that would begin to tackle some of the effects on mental health and well-being that you have described?

Dr Dickon Bevington: Everyone's. The internet is clearly a somewhat larger invasion of newness into the world than the invention of literacy. Socrates was dead against literacy. He thought it was a really bad idea; he thought it would rot people's memories. Humans have a long history of inventing stuff that they do not know what to do with and then taking a century or two to work out how to do it. We can accelerate our learning, but we do have to have a view to the fact that this is a massive change in the way that we are thinking and communicating. There are parental responsibilities, absolutely clearly. There is education. In terms of health, we definitely need some very robust research—really well-conducted research. There is somebody in the room who is doing quite a lot of it sitting over there, and that is Professor Livingstone, who has led the way with the EU Kids Online research.

We have moved the goalposts with our alcohol limits and how many units are safe, but, broadly speaking, they have helped to work people's minds around the fact that a little might be fine but a lot is probably a bad idea. So, if I had one idea about how we go forward, there may be differences for different age groups and different kinds of quality of activity, but some kind of alcohol units-type parallel would be a helpful way forward.

The Chairman: What about time online?

Dr Dickon Bevington: Time online and the nature and the activity.

Dr Henrietta Bowden-Jones: I have a suggestion on a rather large scale but I imagine that several people in the room might find this a good idea. It would be to bring together people who may have experienced problems, people who have treated problems, people from the government side and, indeed, from the industry side, to do a much longer piece of work. In a way, what you are doing here is so fantastic. You have opened this big can of worms, and we have identified several issues that need to be addressed in depth. Why not have a conversation with a trusted body of people who have shown that they are completers and achievers, and they can give results for the well-being and protection of the vulnerable in a specific area, and bring them together to carry on the work that you have started today?

Dr Angharad Rudkin: Could I add to that and agree that it is everyone's responsibility, but it is getting the information to parents right from the very start? We should get midwives involved. When a parent first becomes a parent, they should start thinking that their child is being born into the internet area. What are you going to be doing with this? What kind of information is there out there? What kind of research evidence is there that will help you as parents to understand the internet and any impact it has on child development, and what are appropriate sites and what is appropriate information? We need a multi-sectoral, single place to which parents, professionals and anyone working with young people can go, and the information is there as it grows through these conversations from different sectors.

Bishop of Chelmsford: It is my question next, which anticipates that.

The Chairman: Lord Caithness, do you want to come in very quickly with a supplementary?

Earl of Caithness: It relates to both the Bishop's and Baroness McIntosh's question. Do you have an agreed guideline of what is addictive, what is excessive, and what is little? You have used these terms, but what does that mean in real life?

Dr Henrietta Bowden-Jones: It is slightly different with children than with adults. With adults, you can say, "If you have compulsive online gaming and you are doing it for more than 30 hours a week, we can define you as a person who has an addiction to gaming". As I mentioned earlier, any one of the nine criteria one could use in assessing the negative impact of gaming on an individual, and in a child that one particular criterion could devastate their life and their ability to progress. Therefore, I would say no, not really; it is much harder to be systematic about that in that way. However, it is all about tolerance in a way. How much are you increasing the activity to a level that is unbearable to others around you, to you and to your sense of direction in life?

Dr Dickon Bevington: I suppose, "What does healthy internet use look like?" would be an equally important question to ask, because the counter to all this sense that it is a disaster is to say, "Let us just not show our children the internet at all". That would be massively disadvantaging them these days, so somewhere there is an idea—it is a bit fluffy—of what is healthy internet use.

This idea of building a sustained conversation with young people, parents, mental health professionals, legislators and industry, getting into the meat of what healthy or harmful internet use looks like at different ages or developmental stages, seems critical.

Dr Henrietta Bowden-Jones: Which games are the most addictive, for example? Get the feedback from the population and then tackle the industry. "Why are you creating games that are so harmful? These are the criteria. Please stop".

Q15 Bishop of Chelmsford: We have gone on to this subject a little, but you have spoken a lot about the need for there to be research, good advice and guidance for parents. Does that mean there is not any at the moment? What help is available for parents in terms of mental health issues with the internet and—we must not call it addictive—harmful use? Also, does the NHS have any resource or expertise to deal with these things? Does it get talked about in a doctor's surgery?

Dr Dickon Bevington: Children's mental health services are in a major funding crisis at the moment. Everyone says that all the time, but come and look at child and adolescent mental health services. Is there a bespoke specialist network of practitioners who have the training and experience? Answer: no. Are there a lot of mental health professionals who do this sort of work or work with young people where part of their problems either have come to light through the internet or are manifested through their harmful use of it? Yes; lots of people are doing that work, but the kind of specialist treatment that Henrietta's service has is unique. I work in an addiction service—a substance use service—but we are commissioned to work with substances and not with the internet. I happen to think that, if you do not ask a young person about their online life, you are not taking a proper mental state history, and it would be one of my shouts for the psychiatric and mental health profession that we should be asking about this.

The Chairman: Angharad, do you have anything to add?

Dr Angharad Rudkin: Yes. It is so much easier to intervene early before things get difficult, and we need to help parents, teachers and everyone else working with young people to realise what is a healthy norm. We need to establish that ourselves as adults. I know you talked about PSHE earlier on and that kind of sense of helping young people critically to be aware of their internet use and what the risks and benefits are. Risks do not equal harm, but what are the potential harms?

Bishop of Chelmsford: I am sorry to interrupt you, but is that information available but we are just not communicating it?

Dr Angharad Rudkin: Yes. There are loads of people doing amazing things. There is MindEd, for example; there are various websites that have loads of information on this. There is Baroness Kidron's information on 5Rights. Until people think it is a problem, I do not think they are going to access the information. What is happening is that parents of our generation just do not know when it is a problem or not until something really bad goes wrong or the child gets very impaired. It will be interesting to see in 10 or 20 years' time, when people are becoming parents themselves who have grown up with the

internet, what kinds of issues they will be dealing with when they are thinking about their families.

Dr Henrietta Bowden-Jones: One of the things that is very hard to deal with at the clinic is the number of phone calls from parents of children who have internet issues. Because they are not gambling, we have to turn them away. We are not commissioned to treat this disease. When they ask us where they can go, if they can go to a centre that is designated for internet problems, we do not know where to send them. We have done a lot of research to try to find a national centre or something similar to what we do in gambling. This led us to do a pilot to see whether we could start treating the illness, and we had about 100 people coming through. Some of them were young, but none of them were children. There is an 85% success rate, so it is a treatable disorder. It is just understanding the illness and using the right treatment. My big wish would be to see a replica of what we have for gambling but for gaming and the internet in general, because in a specialist centre you can then embark on all the background research that you need to do with a newly discovered or newly understood illness. You can provide the back-up in order for legislation and policy changes to take place if needed when products are deemed to be unhealthy or certain people are deemed to be very vulnerable. Things can happen at a countrywide level if the illness is understood.

The Chairman: Baroness Quin, you have a very big question. Please ask it.

Q16 Baroness Quin: Given what has just been said, I would love to pursue that, but I know we do not have much time. As if current challenges were not bad enough, we are looking ahead also to future technologies such as artificial intelligence and the internet of things. I am sure it is quite difficult to assess risks related to these things at this stage, but is thought being given to risks in these kinds of new developments?

The Chairman: I have a feeling this one might be a big, new departure for all of you. Possibly it is one from which we would do well to get some written evidence from you, unless anybody feels there is a one-minute answer.

Dr Henrietta Bowden-Jones: Thirty seconds: virtual reality and post-traumatic stress disorder. That is one of the big things that people are talking about.

Baroness Benjamin: Could you elaborate on that? I find that really interesting. I would love to hear more.

Dr Henrietta Bowden-Jones: I am going to get told off.

Baroness Benjamin: We might start suffering.

Dr Henrietta Bowden-Jones: I would be very happy at any time to talk to any of you in a different setting and not take up too much time today, but I would be very happy to do that.

Baroness Benjamin: No; I would really like to hear about that. Even for people listening, this is something that I had not thought about that needs to be said rather than having it written down.

The Chairman: Try to be brief.

Dr Henrietta Bowden-Jones: I will be extremely brief, partly because I do not know very much about it myself. I hear from talking to industry that people are developing games, using virtual reality, that are putting human beings in situations that are causing them to experience fear, and then to experience positions of being unable to escape the setting they are in, still in VR. It is being noticed that there is a residual psychological state when the game ends that is similar to post-traumatic stress disorder symptoms, with hypervigilance, nightmares and whatever it may be. There will be plenty of online information about this. It all started with a conversation about a game and people shared the fact that even people in the industry are experiencing symptoms, even though they are used to these games.

Dr Dickon Bevington: Just to throw you one other googly, there is artificial intelligence and adolescent development in the sense of self. If your sense of self is reciprocity, we will be involving worlds where people are defining themselves as not just uncomfortable about being one or other gender but uncomfortable to the extent to which they are or are not part AI. People are going to fall in love with AI.

Q17 Lord Sheikh: I found your presentation here most informative. We have covered a number of issues, including mental health issues, the well-being of children, this question of addiction, trust, design of website controls, help for parents and artificial intelligence. Now, we are parliamentarians. What role should Parliament have? I have enumerated the issues that you would like us to pursue. What more would you like us to do?

The Chairman: Each of you in turn, please.

Dr Dickon Bevington: In one sense, we have talked about the specificity of the challenges that the internet brings up, and I would not want to lose that or diminish the importance to develop the research. Some of the research that is going on is great but I think it needs more funding. In one sense, there are also generalities. We were talking about the fact that the internet is just a new environment that filters or amplifies or exacerbates children and young people who already have major vulnerabilities. In reality, the overwhelming stress on mental health services, in general, for me is a greater threat than the lack of very specific internet-based services, which is not to discount their value. It is just that on the larger thing children's mental health is crumbling at the moment. I train teams around the country, so I am not just talking about specific areas. There is a massive stress. If we are to mount some kind of concerted effort, I am afraid it comes down to money.

Dr Angharad Rudkin: I would say very much so and add that regulation, information and research should start early, getting information to parents, and making sure that our discourse is based on evidence and not opinion and fear, and harnessing all the great work that is being done all round the country and all round the world, being able to bring it together so that we can make the most of it.

Dr Henrietta Bowden-Jones: For me, it goes back to what I mentioned earlier. I think you, in this room, have the power to make something big happen in relation to future generations and the internet, and I think a group with all the

responsible stakeholders would start changing the way we experience internet at the moment.

The Chairman: Well done; you did that one tremendously well. Although we are way over time, we are not so badly behind. If you would, we would welcome more from you, particularly on the question we could not get into too deeply, which was artificial intelligence and the internet of things. If there is anything you can offer us on that, that would be enormously helpful, but if there is anything else that you can bring before us we would be extremely grateful, and we are extremely grateful for all that you have said and done this afternoon, although I have had to restrain you and restrain my colleagues. It has been extremely worth while; thank you all very much indeed.

Dr Henrietta Bowden-Jones, Dr Dickon Bevington, and Dr Angharad Rudkin – oral evidence (QQ 11-17)

Transcript to be found under Dr Dickon Bevington

Brass Horn Communications – written evidence (CHI0041)

This submission is written on behalf of Brass Horn Communications, a small, membership orientated, volunteer operated, non profit Internet Service Provider based in the United Kingdom.

1. We are greatly concerned by the proposal that the web browsing of those under 18 will be filtered and actively monitored at school and possibly at home too under the guise of "preventing cyber bullying, [access to] pornography and the risk of radicalisation." as indicated by the "New measures to keep children safe online at school and at home" press release on the 22nd of December 2015 by the Department for Education.

Overblocking

2. Evidence collected[22] by the Open Rights Group has shown that the "Parental Filters" deployed by residential and mobile ISPs have caused numerous cases of overblocking, including at least a block of the NSPCC and Childline websites[23].

3. Without the checks and balances provided by projects such as blocked.org.uk the risk of overblocking is greatly increased, students who find themselves censored are unlikely to report that they can't reach a website regarding a sensitive matter.

4. Many of the filters are provided by 3rd parties that have differing opinions on what is considered offensive. Many examples can be found where ISPs such as TalkTalk and BT have blocked LGBT websites with unacceptable categorisations such as pornography.

Chilling Effect / Normalisation of Mass Surveillance

5. As children become teenagers and become aware that everything they search for can result in disciplinary or even Police involvement[24] they will become less likely to search or question information they need or want.

6. Instilling this fear/acceptance of total surveillance has concerning implications regarding the acceptance of mass surveillance by an entire generation.

7. Someone growing up in the future envisaged by Claire Perry MP, Nicky Morgan MP, Theresa May PM and John Carr will find that whether they are at home, at school, in the library or using their mobile phone they are unable to reach the information they require and know that anything they say or search for will be recorded and possibly used against them.

---

22 https://www.blocked.org.uk/isp-results

23 http://www.independent.co.uk/life-style/gadgets-and-tech/news/o2-changes-porn-filter-after-charity-sites-blocked-9023209.html

24 http://www.express.co.uk/news/uk/647539/Ukip-UK-Independence-Party-school-police-called-website

Data Access and Data Breaches

8. As with the Investigatory Powers Bill's Internet Connection Records there is a concern that by gathering the web browsing / communications data of students *(and possibly linking it back to them)* there is a very real danger that this data will leak and have considerable impact on those affected.[25]

9. The only way to truly prevent such leaks is to not collect the data in the first place.

Evasion

10. It should be recognised that filtering and surveillance are not a panacea, there are many entities around the world who educate, advocate and provide tools for circumnavigating censorship and defeating surveillance. *(Brass Horn Communications being one such entity).*

11. Whilst such tools and advice are not designed for children there is nothing to stop the older and more curious from using them. Teenagers *will* endeavour to bypass the controls that limit their freedom to explore and learn. As John Gilmore famously stated; The Net interprets censorship as damage and routes around it.

12. We would strongly recommend that the committee concentrate on exploring educational and pastoral avenues to limit the perceived dangers of the Internet as the tools created to assist Human Rights activists in bypassing censorship and evading surveillance will work just as well in an educational establishments and homes in the UK as they do in hostile locations abroad.

26 August 2016

[25] http://www.zdnet.com/article/vtechs-data-breach-debacle-6368509-kid-profiles-hit/

BT – written evidence (CHI0020)

Children and the Internet

1. What risks and benefits does increased internet usage present to children, with particular regard to:
i. Social development and wellbeing
ii. Neurological, cognitive and emotional development
iii. Data security.

1.0 The internet is increasingly woven into the lives of children. It has been overwhelmingly positive for them, connecting them to others, being an educational tool whilst offering a vast array of entertainment, much of it free. The internet helps children communicate, interact, find a voice, be creative and realise their potential.

1.1 There are risks for children that come with increased and unsupervised use of the internet. Some children, particularly those who are unsupervised for long periods of time, can spend too much time online potentially denying them real world experiences, physical activity and social interaction. Other risks are exposure to inappropriate and harmful content, eg, pornography, extremism, harmful contact such as grooming, cyber bullying, and identity theft and breach of privacy by unwittingly giving out too much personal information.

1.2 We refer you to the following reports for more insights:

- Ofcom's 2014 *"Internet safety measures - Strategies of parental protection for children online"* "Section 2 - Opportunities, risks and challenges" http://stakeholders.ofcom.org.uk/internet/internet-safety-measures/
- YOUNGMINDS and ECORYS - *Resilience for the Digital World - Research into children and young people's social and emotional wellbeing online*.

1.3 There is a need for ongoing research to understand how children of different age groups, eg, five-year olds as opposed to fifteen-year olds, are using the internet in order to develop evidence-based policy.

1.4 Multi-stakeholder collaboration is not only advisable, but necessary in order to maximise the benefits and minimise the risks of children's online activity. The Government would be an appropriate convener of academia, civil society and business, and to ensure that children's voices are a part of these conversations.

1.5 BT has long taken the issue of protecting children online very seriously. We have invested millions in providing and promoting increasingly advanced technology and tools to parents to help them manage the online experience of their children. We have also promoted education and awareness of online safety among parents, teachers and children through initiatives such as Internet Matters (a free online portal providing practical information on

online safety). We also work with partners such as NSPCC, UNICEF, Marie Collins Foundation, WeProtect, The Safer Internet Centre, Internet Watch Foundation (IWF), amongst others, to further promote online safety.

1.6 It is important that children grow up as knowledgeable, practical and empowered digital citizens so that they understand social norms in a digital world and can manage risks for themselves. It is vital that internet safety education is part of a wider approach around tech literacy. Young people are surrounded by technology from a very early age, yet as they grow up very few are curious about how technology works, nor appreciate how it will shape their futures. This is the tech literacy paradox with today's young people seeming digital natives yet being passive consumers. For young people to be empowered, they need to understand how technology impacts their lives. With digital technology developing at such a fast rate and many adults not keeping pace or being tech literate, children need to learn about the realities of the digital world and be confident in managing the new social norms and their reputation online.

1.7 BT has made a long-term commitment to build a culture of tech literacy and is calling for it to be the cornerstone of modern education. We have a target to reach five million children in UK by 2020, focusing on helping primary teachers become more confident with technology concepts. In partnership with the British Computing Society (BCS) we are upskilling primary teachers to deliver the computing curriculum through the Barefoot Computing programme[26], providing free resources and volunteer-led workshops. Over 700,000 children have been reached and over 90% of teachers who participate in a workshop feel more confident. More information can be found at http://www.btplc.com/Purposefulbusiness/Education/index.htm

1.8 BT research has identified five behavioural barriers preventing children from developing tech literacy skills and considering tech careers. Children have mixed feelings about technology and are getting conflicting and confusing messages about its use. At school they are told they need strong computational thinking skills but at home told to spend less time on their devices. The slicker the technology gets, the more it erodes children's curiosity and, unlike analogue devices, it is not designed to be tinkered with. And the language used and emphasis on coding makes it appear dull and 'nerdy' instead of dynamic. Young people do get excited when they see its application in the real world and how it can be used to make life easier and solve problems, with girls responding well to the potential for its 'real-world' impact.

2. Which platforms and sites are most popular among children and how do young people use them? Many of the online services used by children are not specifically designed for children. What problems does this present?

26 http://barefootcas.org.uk/

2.0 The Childwise Monitor Report 2016 www.childwise.co.uk/reports.html identifies favourite sites as Instagram, Snapchat and YouTube. We refer you to Ofcom's Report 2015 *"Children and Parents Media Use & Attitudes"* http://stakeholders.ofcom.org.uk/market-data-research/other/research-publications/childrens/children-parents-nov-15/ for information on popular platforms and sites and how they are used.

2.1. We also refer you to the UKCCIS's guide for "*providers of social media and interactive services*" https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/517335/UKCCIS_Child_Safety_Online-Mar2016.pdf, which has examples of good practice from leading technology companies, and advice from NGOs and other online child safety experts. Its purpose is to encourage businesses to think about *"safety by design"* to help make their platforms safer for children and young people under 18.

3. What are the technical challenges for introducing greater controls on internet usage by children?

3.0 The greatest technical challenge is identifying when the user of the internet is actually a child.

3.1 There is no practical method to identify a user on every connection and every device. The onus is on parents to install parental controls either on any device that their child has access to or on their home internet connection. Parental education and supervision of children is equally critical and should be ongoing as technology changes.

4. What are the potential future harms and benefits to children from emerging technology, such as Artificial Intelligence, Machine Learning and the Internet of Things (IoT)?

4.0 The benefits to children from emerging digital technology are most likely in areas of improved health, education and welfare. For example, IoT and associated big data analytics are highlighted by the UN Global Pulse initiative[27] as being critical in helping achieve UN Sustainable Development Goals. Another example is in the area of education, where virtual reality could offer immersive educational experiences that could accelerate learning, or create new ways to increase civic engagement and participation.

4.1 However, safeguards are still very much needed to protect children in this new world of emerging technologies, standards or best practice guidelines should be set as technology develops, especially with respect to children. Lack of reference to clear guidance and the fact that human rights impact assessments are not yet commonplace for new products and propositions are risks for businesses to mitigate. The civil society organisations Unicef[28]

---

27 http://www.unglobalpulse.org/

28 http://www.unicef.org/csr/css/COP_Guidelines_English.pdf
http://www.unicef.org/csr/files/Training_Module_3_Carrying_out_Child_Rights_Due_diligence_for_the_ICT_Sector.pdf
http://www.unicef.org/csr/toolsforcompanies.htm

and 5Rights are attempting to address this in the identification of online rights of children and young people. As well as foreseeing potential harm at the design stage, it is increasingly important to equip young people, and educate parents, with the skills to use, create and critique digital technologies and have the tools to negotiate changing social norms when technology is moving so fast and rules and controls can be bypassed.

4.2 The potential harms children face may be categorised into three areas:

- inappropriate content, eg, virtual reality, which is perhaps most implicated. But also IoT and Big Data with inadvertent sharing of private personal information without sufficient anonymisation or consent.
- inappropriate conduct, e.g. cyberbullying or 'sexting' might take on more harmful forms through virtual reality. Emerging technology might also contribute to and exacerbate the 'addictive' behaviour some children display when interacting with technology.
- inappropriate contact, e.g. artificial intelligence and virtual reality may create new challenges for children in how they develop relationships with people as the lines blur between what is real and what is fabricated. A key risk area is online grooming.

5. What roles can schools play in educating and supporting children in relation to the internet? What guidance is provided about the internet to schools and teachers? Is guidance consistently adopted and are there any gaps?

5.0 Schools play a leading role in educating and supporting children in relation to the internet. We would refer you to Ofcom's Report 2015 *Children and Parents Media Use & Attitudes* http://stakeholders.ofcom.org.uk/market-data-research/other/research-publications/childrens/children-parents-nov-15/

5.1 BT, in partnership with Unicef UK, launched *The Right Click: Internet Safety Matters* in March 2014 to deliver a programme of 600 'e-safety' workshops across the UK; we have now held over 320. This initiative is aimed at empowering primary school children to use the internet positively while staying safe, and equipping parents with the tools to help keep children protected. The workshop covers what children do online and provides practical ideas and tools, such as parental controls and privacy settings. This is being rolled out to schools that have attained Unicef UK's Rights Respecting Schools Award (RRSA), which supports schools in improving children's well-being and reaching their full potential. The workshops are delivered by BT volunteers and part of the programme trains teachers to deliver e-safety workshops in their schools. 840 teachers have attended the training. Over 3,000 parents and nearly 5,000 children have attended The Right Click Workshops. Parents are also given a handout with useful websites and pointers on setting parental controls and privacy settings. 78% of parents said that after attending the workshop they knew more about child internet safety than before. More information can be found at http://www.unicef.org.uk/rights-respecting-schools/training-and-support/internet-

safety/?utm_source=media&utm_medium=print&utm_campaign=cp&utm_content=100316_bt_rightclick_invite

5.2 BT also founded Internet Matters with three other ISPs to raise awareness and offer expert advice and guidance to help parents keep children safe online. www.internetmatters.org has a schools section, split into primary and secondary, which helps teachers teach e-safety. Free materials are also available for schools to send home and also gives access to a range of tools for use at parents' events.

5.3 It is important that education is wider than e-safety; children must be able to manage risks for themselves. With IoT and ubiquitous connectivity, it is vital internet safety education is part of a wider approach around tech literacy. The Welsh Government is developing a digital competence framework to place digital literacy as a cross curriculum responsibility alongside numeracy and literacy, the framework will be available in September 2016. The Tech Partnership is developing standards for basic digital skills needed to live and enter employment in a digital world and has safety and security at its centre including understanding concepts of e-safety and protecting information online as well as secure practices.

6. Who currently informs parents of risks? What is the role for commercial organisations to teach e-safety to parents? How could parents be better informed about risks?

6.0 We refer you to Ofcom's Report 2015 *"Children and Parents Media Use & Attitudes"* http://stakeholders.ofcom.org.uk/market-data-research/other/research-publications/childrens/children-parents-nov-15/

6.1 BT has been teaching e-safety to parents (see our response to Q5 and Q8). We have promoted parental controls requiring new fixed broadband customers to make an unavoidable choice during the broadband set-up process as to whether they want parental controls. For existing customers we ran email and direct mail campaigns describing parental controls along with pop-up messages for customers accessing online BT services who had not made a decision asking if they would like parental controls.

6.2 Whilst parental controls are important, they are not a complete safeguard for children and no substitute for education and awareness. Parents need to be actively involved in talking to their children about staying safe online and agreeing how they use the internet and social media; applying parental control filters by default does not encourage that approach.

7. What are the challenges for media companies in providing services that take account of children? How do content providers differentiate their services for children, for example in respect of design?

7.0 Again, the greatest challenge is identifying when the user is actually a child.

7.1 There is a need for accessible, child-friendly terms and conditions when it comes to online agreements like consent for data collection.

8. What voluntary measures have already been put in place by providers of content to protect children? Are these sufficient? If not, what more could be done? Are company guidelines about child safety and rights accessible to parents and other users?

8.0 We refer you to Ofcom's three reports *Internet safety measures - Strategies of parental protection for children online* and the work done by UKCCIS of which BT is a member https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis for information on voluntary measures.

8.1 We have long taken the issue of protecting children online very seriously. In addition to aforementioned education and awareness initiatives (see our response to Q5) we aim to protect children online by:

- providing free parental controls for broadband and mobile customers
- providing free software to our broadband customers to help to protect from viruses, scams and phishing
- allowing BTTV customers to hide or lock TV channels and block access to recordings including those after the 9pm watershed which contain post watershed "guidance" information. All our on-demand films and some TV shows also have a BBFC rating, which provides indication of content
- helping customers understand how to protect themselves and their data online. Our help pages[29] on BT.com have lots of information about staying safe. We have a website on scams that publicises what fraudsters are up to and offers advice
- founding the IWF (and now its largest financial contributor) and developed the world's first online system for blocking child abuse images (Cleanfeed)
- becoming members of the UK Council for Child Internet Safety (UKCCIS), Family Online Safety Institute (FOSI) and a member of the EU CEO Coalition on child internet safety
- signing up to the code of practice for self-regulation of content on mobiles and to the "Public Wi-Fi Statement" committing main Wi-Fi providers to provide filtering of pornographic and illegal materials where children may be present
- being involved with the Duke of Cambridge's initiative on tackling cyberbullying. More information can be found at http://www.btplc.com/Purposefulbusiness/Safetyandsecurity/Childinternetsafety/index.htm and http://www.btplc.com/Purposefulbusiness/Safetyandsecurity/Privacyandsecurity/index.htm

8.2 We believe that our voluntary measures and education and awareness initiatives are helping to protect children online. However, we would welcome increased support from the Government and other stakeholders in raising the profile of Internet Matters.

29 http://www.bt.com/help/home/security.html?s_intcid=con_sanda:HelpHome:L1:security:L2:securityhub

8.3 Our report *Privacy and free expression in UK communications* http://www.btplc.com/Thegroup/Ourcompany/Ourvalues/Privacycandfreeexpression/index.htm is available on BTplc.com which explains our approach on rights to privacy and free expression, and protecting our customers (including children).

9. What are the regulatory frameworks in different media? Is current legislation adequate in the area of child protection online? Is the law routinely enforced across different media? What, if any, are the gaps? What impact does the legislation and regulation have on the way children and young people experience and use the internet? Should there be a more consistent approach?

9.0 UK telecoms and broadcasting are regulated primarily by Ofcom within the framework set by the various European Directives, eg, Audiovisual Media Services Directive, the Communications Act 2003 and other UK and EU regulations and recommendations. The Communications Act 2003 gives Ofcom media literacy duties to monitor internet content and advise the public on online safety. Ofcom also regulates video-on-demand programme services which include internet on-demand services. The regulatory framework for online child protection is one of a multi-stakeholder self- and co-regulatory approach involving the Government, law enforcement, charities and industry who regularly come together under UKCCIS. We would refer you to the House of Commons Library brief "Internet regulation" December 2011 for further information http://researchbriefings.parliament.uk/ResearchBriefing/Summary/SN06145

9.1 We believe that the multi-stakeholder self- and co-regulatory approach has made the UK a world leader in online child protection. It has allowed children to experience and reap the benefits of the internet whilst improving online safety via technical tools and providing the education, awareness and skills to allow children, parents and teachers to manage and avoid risks. We would refer you to Ofcom's 2015 report *Children and Parents Media Use & Attitudes Report* http://stakeholders.ofcom.org.uk/market-data-research/other/research-publications/childrens/children-parents-nov-15/ for further information on children's experience of internet use.

10. What challenges face the development and application of effective legislation? In particular in relation to the use of national laws in an international/cross-national context and the constantly changing nature and availability of internet sites and digital technologies? To what extent can legislation anticipate and manage future risks?

10.0 Much online content viewed by children in the UK comes from outside the UK, falling outside UK regulations. Differences in law and cultural norms provide challenges for making effective and applying national legislation, eg, agreeing the definition of a child, what constitutes pornography and what is regarded as harmful.

10.1 There is also a challenge in ensuring legislation does not inadvertently or deliberately restrict freedom of expression and open communications, limiting the rights of individuals. Legislation can also have unintended consequences, eg, network level filtering not being compatible under EU Net Neutrality regulation.

10.2 It is very challenging for legislation to anticipate and manage future risks given rapid technology developments. Where possible, existing laws should be reviewed and amended to remain relevant to digital technology developments before considering new legislation, which takes longer to enact. Self and co-regulatory initiatives can also deliver the same outcomes faster than legislation. If legislation is necessary, eg, technology developments have made the enforcement of existing laws more difficult, the legislation should be fit for purpose, flexible and technology neutral. Not only can legislation quickly date, people are increasingly mobile world citizens so potential harm is not restricted to the boundaries of a particular jurisdiction. We all need to understand the implications of our interactions online.

10.3 The UK and stakeholders like BT work closely with EU Member States and other international networks and partners, eg, WePROTECT. We would encourage this continued involvement with the EU post Brexit and the strengthening of the UK's engagement in other international networks to promote best practice and encourage better coordination of effort to improve policy and measures to protect children online.

11. Does the upcoming General Data Protection Regulation take sufficient account of the needs of children? As the UK leaves the EU, what provisions of the Regulation or other Directives should it seek to retain, or continue to implement, with specific regard to children? Should any other legislation should be introduced?

11.0 We believe that the upcoming General Data Protection Regulation (GDPR) does take sufficient account of the needs of children and we would support the implementation of the provisions relating to parental consent and the flexibility around the age under which this is required.

11.1 We would also support retaining provisions for protecting minors from inappropriate on-demand media services under the Audiovisual Media Services Directive. In relation to EU Net Neutrality Regulation, whilst ISPs are working with Ofcom and DCMS to ensure the continued availability of content filtering, were the legitimacy of such filters to be successfully challenged under the EU Net Neutrality Regulation, the UK should amend that regulation to explicitly permit such filtering.

11.2 Save for the age verification measures in the Digital Economy Bill to protect children from online pornography, we do not believe there is a need for other legislation to be introduced.

12. What more could be done by the Government? Could there be a more joined-up approach involving the collaboration of the Government with research, civil society and commerce?

12.0 We believe the UK's multi-stakeholder self- and co-regulatory approach involving the Government, law enforcement, charities and industry has made the UK a world leader in online child protection. We would encourage the Government to develop evidence-based policies for online child protection consulting with children and to strengthen the UK's engagement in international networks for the online protection of children to promote best practice and encourage better coordination of efforts to improve policy and measures to protect children online.

12.1 The Government can play a role in challenging past orthodoxies and really consider what young people need in today's digital economy. There is a need to rethink the role the education system plays in preparing children for the world they live in and engage with civil society organisations to develop a new framework that will empower young people and keep pace with advances in digital technology.

August 2016

Alex Burchill – written evidence (CHI0065)

1. As a researcher at the University of Sheffield and a former social strategist at FleishmanHillard Brussels, I would like to make a submission of evidence which explores the implications of the growth of social media as a news source. I am delighted that the committee has taken the time to investigate what I believe to be a highly important issue and I hope to be able to contribute useful insights. This submission will highlight the potential problems caused by phenomena such as 'fake news' and 'filter bubbles'. Although making concrete recommendations is beyond the remit of this submission**, I do believe that by educating our children about the potential dangers of using social media as a news source, we can give them the level of critical understanding which they will need to effectively harness the internet's power**. The contents of this submission will hopefully provide insights which not only help to answer question one, but also questions five and six as outlined in the 'Call for Evidence' for this inquiry.

Social Media as a source of News

2. The recent Reuters Institute's Digital News Report highlighted how people are increasingly turning to social media to access news, with 51% of participants admitting to using it as a news source and 12% of them using it as their main news source. This trend is especially pronounced amongst young people, with 28% of 18-24 year olds saying that social media is their main source of news. This means that for this age group, social media is a more popular news source than television. Although the report does not provide specific data on the habits of children, **I believe that these figures are relevant because they demonstrate a clear correlation between youth and the use of social media as a news source**. As Ofcom's annual report on the media habits of Children and Parents demonstrates, social media is central to children's lives, with 23% of 8-11s and 72% of 12-15s having a profile and usage occurring throughout the entire day. Taking this into consideration, **I believe it would be naïve to suggest that children don't use social media as a news source**, despite there being a lack of research on the matter.

3. This is an important development because the news shared on social media is not subject to the same editorial rigour as more traditional news sources. 'Fake News', where websites or blogs upload stories based on misinformation is common. Analysis carried out by Buzzfeed after the recent Presidential election in the United States showed how in the three months before polling day, fake news stories generated more engagement on Facebook than the top stories from major news outlets; with the former receiving 8,711,000 engagements to the latter's 7,367,000. **This shows that 'fake news' is becoming more widespread on social media.**

4. This is a problem for children especially because they have less developed critical understanding capacities than adults. As the aforementioned Ofcom report states, critical understanding is crucial if children are to *"get the*

benefits the internet has to offer, and avoid potential risks." **Worryingly, both the Ofcom report and a recent study by Stanford University suggests that critical understanding amongst children is lacking.** The former shows us that compared to 2015, Children between the ages of 12 and 15 are more likely to believe that most of the information on the sites they visit to get news is true. The Stanford study reaches similar conclusions, showing that in America, 82% of middle-schoolers couldn't distinguish between an ad labelled "sponsored content" and a real news story on a website.

5. Companies including Facebook and most notably Buzzfeed have pledged to take steps to tackle the problem of 'Fake News' and this is a welcome step. **However, the burden should not lie solely with industry.** Parents, schools, and legislators should look at methods which they can adopt to help improve critical understanding amongst children.

6. Equally as worrying as the rise in 'fake news' is the effect of the concept of 'personalised content'. As with many search engines and news sites, social media platforms use a series of algorithms to personalise users' news feeds, essentially deciding for them what they can and can't see. To use Facebook as an example, each story is given a personalised 'relevancy score' which is based on- amongst other things- a specific user's likes, dislikes and online behaviour. The more 'relevant' Facebook's algorithm deems a story to be, the more likely it will appear on a user's feed. Before the internet, broadcasters decided what the public needed to know and they made these decisions based on considerations of ethics and importance aswell as relevance. On the internet, users are not shown what they *need* to see but what they *want* to see. **This creates what Digital expert Eli Karias calls a 'filter bubble' which is invisible, involuntary, and unique to every individual.**

7. Users are limited by the confines of their own bubble, being exposed to a selective range of information. Resnick et al have outlined the potential problems caused by filter bubbles, arguing that selective exposure correlates with higher levels of attitudinal polarization and greater fragmentation in issue priorities. **If children are routinely exposed to the same opinions from the same sources, then it is likely that their perspective on the world will be incomplete and skewed.**

8. Due to the sheer level of information on the internet, a level of filtering and personalisation is obviously necessary. However, that does not mean that filter bubbles are not problematic nor does it mean that we can't take action. **If we can educate our children about the potential problems which filter bubbles both online and offline can cause and encourage them to regularly work to 'escape their bubble', then we can aid their development.**

Concluding statements

9. The rise of social media as a news source creates potential problems for children. To combat these problems, **we need to educate children to improve their levels of critical understanding and help them learn about the origins of the information they are consuming.**

10. In some circles, this is already happening. In industry, MediaSmart works with children and parents to 'open eyes', whilst in the media, the Guardian Newspaper has recently started sharing articles from Conservative sources, encouraging people to "escape their bubble". Some schools have started teaching these issues in PHSE, but evidence is anecdotal. I am sure that there are other schemes that I have not mentioned which are doing important work. **The challenge is to bring all this work happening on the periphery into the mainstream so that as many children as possible can reap the benefits- this is the inquiry's main challenge.**

    Word count: 1116

Bibliography

Ingham, M., "BuzzFeed Names Fake-News Expert Craig Silverman Its First Media Editor", http://fortune.com/2016/12/02/buzzfeed-media-editor/, (accessed 29/11/2016)

Karias, E., The Filter Bubble: What The Internet Is Hiding From You, (London, Penguin, 2011), pp 1-304

Newman, N., Fletcher, R., Levy, D. and Nielsen, R., "Reuters Institute Digital News Report", https://reutersinstitute.politics.ox.ac.uk/sites/default/files/Digital-News-Report-2016.pdf, (accessed 29/11/2016)

Ofcom, "Children and parents: media use and attitudes report", https://www.ofcom.org.uk/__data/assets/pdf_file/0034/93976/Children-Parents-Media-Use-Attitudes-Report-2016.pdf, (accessed 29/11/2016)
Rensick, P., Munson, S., Stoud, N., Kriplean, T., Garrett, R., "Bursting Your (Filter) Bubble: Strategies for Promoting Diverse Exposure", in CSCW 2013 Computer Supported Cooperative Work San Antonio, TX, USA — February 23 - 27, 2013, (New York, ACM, 2013), pp 95-100

Select Committee on Communications, "Call for Evidence, Children and the Internet", https://www.parliament.uk/documents/lords-committees/communications/children-internet/CfEChildren-internet.pdf, (accessed 29/11/2016)

Silverman, C., "This Analysis Shows How Fake Election News Stories Outperformed Real News On Facebook", https://www.buzzfeed.com/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook?utm_term=.twN0gAA9l#.gmddY11N2, (accessed 29/11/2016)

Stanford History Education Group, "EVALUATING INFORMATION: THE CORNERSTONE OF CIVIC ONLINE REASONING", https://sheg.stanford.edu/upload/V3LessonPlans/Executive%20Summary%2011.21.16.pdf, (accessed 29/11/2016)

Wilson, J., "Burst your bubble: five conservative articles to read this week", https://www.theguardian.com/us-news/2016/dec/01/conservative-news-articles-this-week-media-bubble?CMP=fb_us, (accessed 29/11/2016)

December 2016

Dr Marc Bush and Dr Nihara Krause – oral evidence (QQ 98-107)

Tuesday 15 November 2016

Watch the meeting

Members present: Lord Best (The Chairman); Baroness Benjamin; Baroness Bonham-Carter of Yarnbury; Earl of Caithness; Bishop of Chelmsford; Lord Gilbert of Panteg; Baroness McIntosh of Hudnall; Lord Sheikh; Lord Sherbourne of Didsbury.

Evidence Session No. 7 Heard in Public Questions 87 – 107

Examination of witnesses

Dr Nihara Krause, Consultant Clinical Psychologist, Founder and CEO, stem4; Dr Marc Bush, Chief Policy Adviser, Young Minds.

Q98 **The Chairman:** We are sorry we kept you waiting for a bit. We were having a very good session before, and we know we will have a very good one now. Dr Nihara Krause and Dr Marc Bush, you are both very welcome. Thank you for joining us. Can I ask both of you to introduce yourselves briefly and explain where you are coming from in relation to our inquiry?

Dr Nihara Krause: I am Nihara Krause. I am a consultant clinical psychologist and the founder and CEO of stem4, a charity that offers workshops in secondary schools in four areas of mental health and resilience. We also educate school nurses and GPs.

Dr Marc Bush: I am Marc Bush. I am the chief policy adviser at YoungMinds. We focus on mental health from nought to 25. Last year, we did a lot of work on digital resilience, which covers the online world.

The Chairman: I am going to ask a very big question, so perhaps you could get the answer into three or four sentences. How would you assess briefly the current state of children's and young people's mental health and well-being in the UK? Where are we now?

Dr Nihara Krause: Our data are still a little old, but one in 10 five to 16 year-olds present with some form of diagnosable mental ill-health condition. That statistic increases to one in four in young adults. About half of the children with mental ill-health conditions present with conduct disorder, and just under a quarter with anxiety or depression. It is probably true that the rates of disorder rise steeply in middle adolescence and again between the ages of 18 and 20.

The Chairman: Not good.

Dr Marc Bush: Child and adolescent mental health is in a period of big change at the moment. The Government have invested £1.4 billion in a transformation programme, but we are not at the end of that journey. We know that a quarter of all young people who are referred by GPs or teachers are turned away from CAMH services because the services are just not there, or the young people do not meet the thresholds of eligibility for those services. Double the number of children and young people turn up at A&E as a result of not having their needs meet elsewhere. While there are some wonderful services and professionals within the NHS and schools, we know that people are waiting too long to access services, and in the period before accessing a service their needs escalate and they end up in crisis.

The Chairman: Would you say a brief word about child development stages? How do the emotional, cognitive and social needs of children change as they grow older?

Dr Nihara Krause: There are a number of different ideas, but briefly there are expected developmental stages. When children are very little, you would be working on issues around attachment and trust. As they get a little older, you would expect issues around emotional regulation, learning about give and take in relationships, learning about boundaries and, through that, how they might place boundaries on their own behaviour. That is up to about the age of five.

From the age of six until about 12, there is a very rapid change in children's understanding of themselves and the world. They start to think more about morals: for example, what is good and bad; they start to separate what is real and unreal; and they start to think more about cause and effect, so the consequences of their behaviour start to become more apparent to them. Of course, there will be the beginnings of very strong identity formation, and that will happen through testing out a variety of different types of identity.

That continues into adolescence when there is the most rapid growth in becoming independent, autonomous, starting to think very clearly about what roles they might like to take, what sort of person they might be and how they connect socially, and their responses to other people and how other people in turn affect them. That enables them to think clearly about how they relate to peers and adults. As they get older, there is the formation of intimate relationships.

The Chairman: Dr Bush, do you have anything to add to that very comprehensive answer?

Dr Marc Bush: Not much. I would pick out a couple of key words. The first is about children and young people being active in all the things that were mentioned. When we talk about the internet, sometimes we assume that children and young people can be protected from everything, yet frequently they are the people creating as well as using that content. That is a really important thing in those developmental stages. The second point is the recognition, which has already been mentioned, of the impulsive nature of later childhood and early adulthood. The final point to flag is that identity and relationship

formation is happening, and that is a really important part of where we start to see the well-being impact of their online world.

Q99 **Bishop of Chelmsford:** This question gets to the nub of many of the things we are trying to explore in this piece of work. The House of Commons Committee on Health reported that the sharing of indecent images on mobile phones and other types of communication was harming young people's mental health and led to big increases in self-harm, et cetera. The Committee concluded that "in our view sufficient concern has been raised to warrant a more detailed consideration of the impact of the internet on children's and young people's mental health, and in particular the use of social media and the impact of pro-anorexia, self-harm and other inappropriate websites".

I have two questions. First, to what extent are the cognitive, social and developmental needs of children catered for or undermined by internet use? In your experience, which particular elements of children's internet use have an impact on children's mental health and well-being? Perhaps you could deal with that one; there is another question to follow.

Dr Nihara Krause: Thinking about children's developmental stages, on the positive side the internet provides an arena. It is almost an anonymous identity playground for children to play out the different roles they might feel they want to undertake. In a way, it helps them with creativity and helps them to direct where they want to be. As mentioned, they are active users of what is there outside them. The negatives are that, in a way, there is pressure to put forward your best self, and that is very difficult for children, particularly developmentally, as they are thinking about themselves. If they put forward their best self and that is criticised, or not liked, it leaves children very vulnerable and susceptible to how they might deal with things. The internet has also at some level become an escape to avoid the pressures children feel in their daily life, so it is thinking about how they might use that escape, and whether they use it positively or negatively, based on what they interact with.

Bishop of Chelmsford: Before Marc comes in, perhaps I could add my second question, which is something we have touched on at various points. Thinking probably of very young children, Public Health England's report, *How Healthy Behaviour Supports Children's Wellbeing*, identified a large body of research that showed a negative association between screen time and mental well-being. Is there clear evidence for linking internet use? I am thinking particularly of excessive screen time and the detrimental impact on development, mental health and well-being. What further research, in your view, is needed?

Dr Nihara Krause: From what I have read, it would seem that three-and- a-half hours per day of screen time had a negative effect on children's self-esteem and body image. That is what the report mentioned. In this type of research, it is very difficult to look at the individual factors for the children who use the internet for three and a half hours. Are they the one in 10 children who might drift into using it, or might it be any child who uses it? We need to know a little more about the groups of children who might use the internet in that particular way.

Bishop of Chelmsford: What research should be done in your view?

Dr Nihara Krause: The research should be more comprehensive and use better definition of subject groups and how things are evaluated. It should use more robust methodologies, and should compare potentially vulnerable children and those who might be more susceptible to misuse of the internet with children who are not.

Bishop of Chelmsford: Although I do not have it in front of me—I should have brought it with me; I apologise—I seem to remember reading at the beginning of this inquiry some evidence related to very young children, perhaps as young as 18 months, where excessive use of, say, a tablet affected the way the brain was wiring itself. I do not know whether you want to make any comment on that. I am sorry for explaining it in such lay man's terms.

Dr Nihara Krause: Not at all. There is some research to indicate that there is neural activity, particularly if you use a tablet before you go to sleep, for example; the amount of blue light can affect sleep cycles and can aggravate overactivity in some children.

Dr Marc Bush: About a third of internet users in the world are below the age of 18. That gives us a sense of the growing population of young people who will always have been web-enabled. Two in three nine to 16 year-olds have at least one social media or networking account, and for 15 to 16-year-olds it rises to nine in 10. By their early to mid-teens, the majority of people are already frequently using online or social media accounts.

I shall skip over the impacts on behaviour, well-being and mental health because I know that is coming up later. I want to talk about some of the features that might aggravate people's mental health. The first is that the online world creates an environment where people can be cyberbullied and where offline bullying can follow people to their online activity. We have talked to young people who describe the distress they face in the playground because people are calling them names. That distress follows them on to their Facebook page, and it follows them on to their WhatsApp group among all their friends. Suddenly, it is as if they are always being seen; they cannot hide from that abuse. It is important to recognise that, because the constant surveillance means they feel that they are constantly under threat.

In your question, you mentioned self-harm. We are worried about self-harming websites on the dark web, be that pro-ana or pro-cutting websites, which effectively promote and encourage people to self-harm. Somewhat paradoxically, some of the information on them is important for children who self-harm, because it tells them how to do so safely, but overall they promote self-harming and in some situations encourage suicidal behaviour. That is the deep web.

If we go to the light dark web, as it were, I could get my phone out right now, go to Instagram, for instance, put in a hashtag which does not include the words "suicide", "self-harm", "cutting" or "anorexia", and find a whole range of pictures and instructions about how to cut, how to ingest dangerous materials or how to restrict my diet. We feel that this is all happening in very deep spaces on the web, but I and all our children are only one hashtag away from accessing that information. Then there

are the closed groups, where we will probably never be able to intervene. If I am an eight or nine year-old and I have a smartphone and my friends have a smartphone and we go off to school, we might all be in a WhatsApp group. There is no way of looking at that encrypted messaging. Therefore, promotion of those behaviours, or bullying or intimidation, can happen within that closed network. There is no way of penetrating it.

Finally on the negative side, before a couple of positives, it is important to remember that every single day on social media screens children and young people are encountering normative and unrealistic representations of their bodies, of identities and of what it means to be a particular gender. We know this is having a disproportionate impact particularly on girls but also on young men's mental health and well-being.

On the positives, when you ask young people about the risks of the online world, they rank them extremely low. That is because they are active contributors; it is where they go to get information and advice, for example from our HeadMeds site, which gives them advice on psychiatric medicines. It is also where they reach out online either to offline friends or to people they will never meet on the other side of the world to try to ask their advice. There have been recent studies that suggest there are positive benefits from going online. To give a very contemporary example, a Positive Outcomes study suggested that using Pokémon Go not only got children and young people out and about searching for Pikachu and Pokémon but engaging with their offline environment as well as their online one.

Q100 **Baroness Bonham-Carter of Yarnbury:** I am so glad you ended with that. We are looking at the influence of the internet on the mental health of children and young people, and of course it is important to concentrate on the bad, but I worry that that is all we are doing. I am pleased you said what you said, because there are isolated young people who can find that information. I should be asking you a question rather than making a statement. Your description of the internet sounds a little like what we read about boarding schools of the 19th and 20th centuries—you could not get away from bullying and so on. I think you have answered the point, but I would like to press you a little more on the positives, because I do not think we should be concentrating on just the negatives of the internet for the mental health of young people.

The Chairman: Are there any more positive thoughts?

Dr Nihara Krause: It encourages children to be creative and to be innovators. It offers huge scope from that angle. From an academic and learning perspective, it is an immense source of information, if it is used positively. For children who lack social skills or who are very shy, it is a very important place to meet, connect and learn how to be part of a peer group. Certainly, a lot of young people feel that the emotional benefits that online offers are very big. They like the group support they can get from their peers.

Baroness Bonham-Carter of Yarnbury: It is a positive thing, but we have to find a way of navigating away from the potential harm.

Dr Nihara Krause: Yes. It is about enabling children and young people to know how to navigate it and be able to use it.

Q101 **Lord Sheikh:** I want to ask about emotional and behavioural problems relating to boys and girls, and how different they are. Do you find that the mental health and well-being of girls and boys is affected in the same way and to the same extent? How are they affected? Is it possible to measure and assess the effects? What remedial action can we take to deal with the different effects on boys and girls?

Dr Nihara Krause: In a general context, at a younger age there are not many differences between girls and boys. As they get older, there are more gender differences, but in general more boys than girls present with conduct disorders and behavioural problems. At a younger age, more girls—but only slightly more—present with anxiety and mood disorders. There is a lot more reporting of girls presenting with self-harm, but I think that is based on the definition of self-harm, and even with anxiety and depression it is about how boys present their anxiety and self-harm. A lot of boys who present with conduct disorders or behavioural conditions are anxious; they just show it in a different way.

Lord Sheikh: It is not easily manifested when it comes to boys. They do not tell us what they feel, although they may be feeling it inside.

Dr Nihara Krause: Yes. They might be more likely to show it through their behaviour than verbally. More boys are reported to present with addiction-based issues than girls, but again it depends on the type of addiction. If it is a shopping addiction, it may be biased more towards girls than boys. Definitely more girls than boys have eating disorders, but if you look at body image issues, a lot more boys present with concerns about their bodies.

Lord Sheikh: Do eating disorders such as anorexia apply to boys as well? Do boys have the same problems?

Dr Nihara Krause: Yes.

Lord Sheikh: I thought there would be more girls than boys.

Dr Nihara Krause: Boys present with the same types of eating disorders as girls: anorexia nervosa, bulimia nervosa and binge-eating. Boys also sometimes present with body dysmorphic disorder, which might lead them to talk about bodybuilding. They might have a slightly different concept, but the issues are the same: control, dissatisfaction with themselves and their bodies and low self-esteem.

Dr Marc Bush: As to how those behaviours manifest themselves, self-harm is more commonly reported or identified among girls, less so in boys, but in recent years the number of girls, although it is much higher, has been declining and the number of boys has been increasing. The reverse is true for suicide and suicidal behaviour. It is much higher in boys but declining; in girls, it is much lower but increasing.

It is important to mention, given the nature of the inquiry, that most gaming at the moment is web-enabled, and there is a significant difference in the gender consumption of gaming. Most of the gaming world is female: 52%. Boys tend to use massively multiplayer online

games—MMOs—or first-person shooter games, which are very much about participating in questing, adventures or military operations. Girls tend to be involved in role-playing games, which are more about fantasy and sci-fi, and are more likely to use games on their mobile phones. The reason I mention that is that all those routes have the possibility of dialogue with whoever you are playing with, so there is a communication point, both positive and negative, for mental health.

Lord Sheikh: Do you find that sometimes it is temporary and they grow out of these phases? Is that the general position?

Dr Marc Bush: Yes, although there has been a huge increase in the number of adult women who play online games. The nature of some games is that people grow out of them, but actually we have games—

Lord Sheikh: But generally, is the problem you are referring to a temporary phase, or do you find that after a while it withers away in most cases?

Dr Marc Bush: No. The gender divide seems to be there within that different type of gaming world, and that is probably because of what we were saying about boys being encouraged to express anger and emotion through questing, military expertise or aggression, and girls through fantasy, creativity and showing emotion.

Dr Nihara Krause: On the question about whether it continues into adult life, it depends on each individual and why they use it. One of the difficulties with multiplayer online games, for example, is that there is no ending. Your score gets higher and higher. For some children, for example if they have attention deficit disorder, boundary setting and impulse regulation is very difficult, so those children can become adults who continue to use those games in a different way. Similarly, if girls who are quite isolated use role-playing and do not have significant role models in their life, they may carry on using those sorts of games for much longer in adult life, because they might have an attachment to a character or an identity the games provide them with. It depends on individuals.

Q102 **Baroness McIntosh of Hudnall:** I was going to ask you about body image, but you have talked about that, so I am not sure how much more you want to add. Instead, I want to go back to something that occurred to me as a result of everything you have said up to now. How much of what you are describing is, as far as you can assess it, genuinely new behaviour, and how much of it is behaviour consistent with what we know has always been part of child development and adolescent behaviour, including things such as eating disorders, which we regard somehow as modern afflictions but are not? If you look at Victorian novels, you can find plenty of evidence; it is just not described in that way.

Picking up the point Baroness Bonham-Carter made about the highly inward-looking worlds of certain kinds of education, you see the same tropes manifesting themselves. How much of what you observe is genuinely new behaviour, and what order of problem do you believe the

internet is creating through its ability to amplify what are standard behaviours that we have always known about?

Dr Marc Bush: I will comment on both. To answer your second question first, you are totally right. There are existing behaviour sets—responses to emotional distress and poor mental health—being played out in a new world either online or on social media. For me the big difference, and this is what children and young people tell us, is that they have the opportunity now to enhance or augment their bodies and worlds in a way that was not there before. The digital world allows you to do that in the most creative and beautiful ways, but also in ways that create a lot of distress. Most of the surveys, to summarise them, say that most children and young people have augmented their face or body on social media to make themselves look more like the images they see on their Facebook feed, for instance.

Baroness McIntosh of Hudnall: It is new because the tools are new.

Dr Marc Bush: Exactly. Behaviours that perhaps were there before are becoming more prominent. A lot of the work that has been done on early teenage sexuality has shown that a disproportionate number of early teenagers are shaving body parts to reflect the kind of bodies they are exposed to online. There are different forms of augmentation. Linked to your first point, we know that the promotion of different kinds of augmented and enhanced bodies online is affecting young men. Lots of men are starting to become obsessed with exercise; they are exercising on injury or to injury; they are ingesting things that damage their physical as well as mental health. It reinforces that spiral in a way that is not recognised. For girls and young women, there is a lot more sensible conversation about what girls' bodies should look like. For boys, the majority of things they are consuming say that it is realistic to ingest all that, to go every single day to the gym and have a huge six pack and a huge body; but it is effectively a form of eating disorder—self-harm through ingestion and body dysmorphia. For me, that is the stuff that children and young people are saying is different about this kind of platform.

Baroness McIntosh of Hudnall: Given that what we are trying to do is see whether anything can be done to moderate that, or in some way influence people not to be so vulnerable to such pressures, from your perspective what could be done and is not being done that we should know about?

Dr Marc Bush: There are two practical things. One is an international movement to recognise iRights—you may have seen the iRights statement—which would enable children and young people to delete their digital footprint after a period. Not only should children and young people have that right; we should all have it. Secondly, there are a lot of measures that we think are really important about prevention or protection, but not everything from government and industry. They are saying, "Let us stop people using these platforms", which obviously you cannot do, and then, "Let us wrap these platforms in cotton wool", which you cannot do either, because many young people create the content themselves. We believe that digital resilience should be embedded in all

curricula, so that we teach people about the consequences of what they are doing online—what it means to form an identity and seek advice online—so they can navigate the online world for themselves. The risk is that, if we do not do it for that generation, we are allowing ourselves and other generations to define a different kind of protection that possibly does not exist for children and young people. When we ask them, "What do you want us to do about it?" they say, "We are the people creating the future of these platforms. Give us the tools to navigate them and support others, and, importantly, if things go wrong we know where to refer our peers to".

Dr Nihara Krause: To add to what Marc has very comprehensively said, you are right. A lot of what is being shown is usual growing-up behaviour. Where a lot has changed is in the expectation of immediacy. It is very difficult for children to know how to deal with that. Learning to wait is no longer a concept for a lot of young people, and that creates difficulty: how do you learn things, acquire things and have patience? We need to think about that in educating children in school and home.

Secondly, because of the public nature of what they might be expressing and finding out, children are not always aware of how to protect themselves and how to know the difference between what might be real friendships and virtual friendships. There needs to be much more cohesive input into understanding relationships. There should be some sort of social relationship education throughout. If you know how to make friends in real life and how to protect yourself against untrue friends, it becomes easier to translate those skills into your virtual life and interaction.

The third point is about more choices. Two generations ago, if you admired a pop star, you might have stuck posters on the wall and joined a fan club. Now you can follow them. You can post something benign about them. It makes children and young people feel there is a huge number of choices. How do you limit choice? How do you curb temptation, in a sense? Those are all fundamental lessons that can be brought into schools and homes. Greater education of parents needs to be encouraged. Parents are becoming a lot more digitally aware. There are courses and training, but the scene is always changing, so there needs to be some input. Adults or parents who have mental health issues themselves find it incredibly difficult to set boundaries and manage children, and those children are potentially the ones who will present with more mental health issues, so we also need to think about supporting parents.

Q103 **Lord Gilbert of Panteg:** We are very conscious of the danger of just listening to a whole range of problems and negatives about the internet. In the vein of Baroness McIntosh's question, can we have a look at addiction and habit-forming behaviour? Children use the internet and internet-connected devices in every aspect of their life, so it is not surprising that they use them a lot; yet children say that they feel concerned that they may be addicted, or that they are displaying some sort of habit-forming behaviour. I think you said, Dr Bush, it was more prevalent among boys than girls. Is it really habit-forming behaviour, or is it just overuse of the internet, which could be addressed through

education?

Dr Nihara Krause: Research is a little divided at the moment and is developing. If you look at the traditional ways of diagnosing an addiction, both DSM-5 and ICD-10, which are the diagnostic manuals to classify internet gaming disorder, are still unclear. They are waiting, pending further research, to see whether this is primarily a disorder. However, a number of young people present with a range of symptoms that are very typical of something that is more than overuse and is more similar to addiction or misuse. They include increased tolerance, so people need to play for longer and longer to get the same hit; they show withdrawal, in the same way as you might if you were decreasing some sort of compulsive behaviour; and a few brain studies show increases in dopamine in the brain, which is our pleasure-seeking neurotransmitter. That might indicate higher levels, but the research is at its beginnings.

Lord Gilbert of Panteg: Is it possible to identify whether the children who are beginning to have those issues would otherwise have had an inclination to such behaviour in any event and this is just the way it is displayed to you, or whether it is brought about by those devices and the internet?

Dr Nihara Krause: With any condition, there is an interaction between the person and their vulnerabilities and issues, together with what is outside. That is true of anything. We are all subjected to, say, social media or body images, but not all of us will go on to develop an eating disorder. You need a combination. In that sense, a lot of young people who are vulnerable to compulsive misuse will use whatever the substance might be. In this case, it might be the internet or gaming.

Dr Marc Bush: It is important not to pathologise that use. It is just a normal response to things that children and young people are experiencing. Children and young people tell us they are using the online world both to mitigate and enhance anxiety, in effect. It is predominantly anxiety. There is a range of other things, such as looking for information or seeking help. A lot of it is about anxiety mitigation. People might go back on the same kind of apps to self-soothe. It does not matter what the content is; it is about having something they can pull out of their pocket and look at in a situation that they find triggering or anxiety-ridden.

Some positive practical solutions could be built into all those platforms. Building on a positive one that has already been done, the majority of social media platforms now have some form of message that comes up if you search for a difficult term like "suicide" or "self-harm". You could get them to prompt other things. For instance, other areas of the world are playing with this idea: what if someone who is registered in a domain is searching at three in the morning and they are known to be under 16? Could you get a message that flashes up that says, "Is everything okay? If not, this is who to ring"? A US and Australian-based company is looking at peer-based support mechanisms to enable young people to talk to other young people on the other side of the globe. If you need to talk about your anxiety, depression or social phobia, you can discuss it with people who are experiencing exactly the same thing; they are just

in a different time zone. The moderation issues are quite difficult, but it is a really good idea.

Building on that, a lot of people use gaming platforms. They are designed to be addictive because they create a virtual reward. It would not be a big step to create your own rewards, or to have your own time limit built into a game. Could an app go on top of gaming apps that said, "The half-hour is up. Why not reward yourself by walking round the garden or ringing a friend you have been putting off?" Young people could put their own rewards into those things. Young people have told us that they would really welcome that.

Finally, we know that loads of behavioural prompts ping out of everywhere—they literally ping. The first thing we hear in the morning is the alarm; the second thing we hear is a ping from our email, Facebook or Twitter. A couple of people in the tech world are thinking about whether there could be user-generated behavioural prompts. Could the first ping be, "Why not do a wake-up meditation?" or, "This is the time of day when you usually feel most stressed at school. Why not spend five minutes in the toilets cooling down?" Is there a different way to use health-based informatics to prompt positive things, as opposed to, "Keep engaging, keep engaging"?

One in three adults have enduring mental health conditions because of childhood adversity or trauma. A great way to deal with the effects of childhood trauma or adversity is to use a fantasy—an online or different kind of world—so there are positive effects for many children and young people. However, they are also the group at great risk of becoming addicted. It starts off being really positive and then it might become an addiction, so intervening in childhood adversity and trauma more broadly through social interventions would help reduce addiction.

Lord Gilbert of Panteg: Thank you very much for highlighting those positive aspects. It is clearly an area you are both working on currently. The Committee would be interested to hear from you as your thinking develops as you conduct your research.

Q104 **Lord Sherbourne of Didsbury:** Can I follow up on compulsive and addictive behaviour that might be partly a result of the features of the app or website, or simply the response to it? Let me give you a precise analogy in the form of motor cars. Of course, we can always encourage everybody to drive safely, but what the motor manufacturers have done is build into their cars, year after year, safety mechanisms to make them easier and safer to drive. Do you have a view about whether the people who develop and create websites and apps should take a leaf out of the motor manufacturers' book?

Dr Nihara Krause: Absolutely. A number of the suggestions Marc made are part of those safety features. In addition, a lot of apps and websites have embedded marketing, for example. One of the things they could have instead are embedded safety features, such as, "Is this getting you stressed? How do you recognise whether this is working positively or negatively for you? Can you go down a gear or two?" Things like that will enable people, in a similar way, to reduce their stress.

Lord Sherbourne of Didsbury: Are there any examples at present where producers and designers of apps do precisely that?

Dr Nihara Krause: Marc? I am not sure about that one.

Dr Marc Bush: Are you referring particularly to health promotion?

Lord Sherbourne of Didsbury: No. Are there designers who have been sufficiently responsible to say, "We are going to build into our app or website something that prevents what we regard as detrimental, compulsive or addictive behaviour"?

Dr Marc Bush: As a group, social media providers have responded well, but they are at phase two, as it were. There are reporting, flagging or signposting features. I talked about Instagram earlier. If I search for terms like "self-harm", it will say, "Is everything okay? This is a distressing image. Do you really want to view it?" The problem is that I can say, "Yes, thanks", push it to one side and keep going. The prevention side works only so far. We need to start thinking about what industry can do, along with government, to intervene when people choose to ignore safety or health promotion.

Lord Sherbourne of Didsbury: You are saying that there are examples of, if not best practice, at least better practice.

Dr Marc Bush: Better and getting there.

Lord Sherbourne of Didsbury: People could look at that as leaders of good behaviour.

Dr Marc Bush: Yes, definitely. There are also apps that go on top of apps, as it were, which effectively help parents to control the features, or limit the amount of time they use, or support mental health, such as peer-to-peer apps you can talk to or get advice from, or things like mindfulness apps. Lots of positive things are being built as well. You have set a very important challenge for government, the charity sector and industry: what is the next wave of interventions that are not just the first line of defence, but educate people to think about how they interact with the online world more effectively, and get the benefits from it?

Dr Nihara Krause: It is a great point that, at the moment, there are safety apps and potentially impulsive behaviour-inducing apps. The two being merged together is definitely the way forward. I cannot think of anything that does that, but that is the way app manufacturers are moving.

Q105 **Baroness Benjamin:** I visited several schools recently. When I asked how many children had phones, computers and mobile devices in their bedrooms, the majority put up their hands. A recent survey has shown that almost half of children admitted that they check their mobile devices when they go to bed. They play games, and sometimes they feel a bit anxious if they are not looking at their mobiles. Do you see any evidence that the always-on nature of some devices and platforms is having an adverse effect on children and young people's mental health and well-being?

Dr Nihara Krause: Yes, there are definitely some reports to indicate that children are finding it much harder in relation to their attention

span; for example, there is greater distractibility. It is a different type of compulsive behaviour; it is almost like an obsessive behaviour, because often it is fear of being left out. If there is a social invite going on, they do not want to be the one who does not get it in time. If there is an image shown for a very short time, they want to be up to see it; otherwise, they will miss it and they will be the one person who does not see it. There are some reports that that sort of constantly switched-on nature reduces intimacy and creates an increase in anxiety and checking.

Dr Marc Bush: Research at Cardiff University found that three-quarters of children sleep with some kind of portable media or online device in their sleeping environment, so it is really immediate. If they wake up during the night, they can grab it and look at it. Glasgow University found that children as young as 11 were on social media sites way into the early hours both as a way of keeping themselves engaged in what was happening in that world, which is insatiable, and as a way of avoiding sleep.

Rather than repeating what has just been said, perhaps I could end with where to take this. For us, the next part of education is thinking about self-care. In previous generations, we would have taught people to think about downtime. We would have thought about self-soothing, having a good meal, going to bed and getting the right amount of sleep. We just need to re-educate parents and young people to think about self-care, including the online world. Sleep is a really important part of self-care, and neglecting it through the online world is yet another addition to a whole range of ways of not caring for yourself.

Baroness Benjamin: You are right. I was chatting to a young girl who told me that she had a terrible life during the day and her only comfort was looking at television and people late at night and forming a relationship with them. That is another type of mental issue we are dealing with. When any of us plays a physical game, we get timeout; we get an interval and time to relax, breathe and stop playing the game and so on. Do you think that, if the providers could build a timeout limitation into whatever young people are watching on their devices, it would be a helpful feature to deal with some of the issues you are talking about?

Dr Nihara Krause: It would be a very helpful feature. Ultimately, we want young people to learn how to implement that control themselves and regulate their behaviour, but if there was a general rule that all that stuff went off at the same time for everyone and no one was communicating, there would not be so much anxiety about being left out.

Dr Marc Bush: My answer is yes, but probably only to the extent that all the preventive or protection measures work. Coding is in the curriculum; every young person is exposed to ways of navigating round all those safety features. That is where we need to make a big leap beyond just safety as the intervention. Young people are resourceful. If they want to be up all night because World of Warcraft is the only place where they have meaningful relationships, they will be up all night having meaningful relationships on World of Warcraft.

Baroness Benjamin: I tell them to empower themselves by making the decision. Perhaps that is something we need to look at as far as mental

awareness and well-being is concerned—for them to be empowered to do it for themselves.

Dr Marc Bush: You are totally right.

Q106 **Earl of Caithness:** I want to follow up Lord Sherbourne's question in a bit more detail. Both of you have now been transposed into Secretaries of State in government. You have told us about lots of good ideas. How are you going to implement them? What is the role for government in this, if there is one?

Dr Nihara Krause: It is to continue to keep the issue as an ongoing discussion and raise awareness in that way, and think about how and where the education of children and parents might take place. An obvious direction is for that type of education to be placed in schools, but it needs to be wider than schools. It needs to be in a number of different community and other settings; that needs to be part of the way we start to think. There needs to be some sort of regulation for the type of research that is carried out, who is involved in that research and how its results are promoted and advocated. It is exceptionally good that there has been so much prominence of the importance of looking after our mental health, for example. That has been incredibly important in a Cinderella of a Cinderella service at some level. However, a number of surveys are not necessarily carried out by researchers or by using some sort of psychological framework. They are publicised in a variety of ways, and they become the tools that inform and are carried into education.

Earl of Caithness: That is great. It is lovely, but is it a government job? Is it a directive from government to say, "This is what you have to do", or is it for the sectors doing it to work closer together?

Dr Marc Bush: It is about collaboration. The role for government is to work out the parameters and framework to make it work within what is knowable about the online world. Regulation is important, but it is a matter of them setting out the kind of prevention and promotion measures they want. If I was the Secretary of State, that is where I would be going.

There is also a very important collaborative role with industry, which creates most of the solutions, and the charity and public service sectors, both of which innovate in this space. Government can promote innovation; it can create funds. The DfE was thinking about that and the DH has huge innovation grants in the space, but if we want good practice models, we know that Australia is far ahead on this. The Australian Government spend a huge amount of money collaborating with both charities and industry to create online-based mental health provision. I can provide further detail offline. The Canadian Government also do that. There are working models from around the globe to show that government, through its vision in upholding children's rights but also in creating and market-shaping a new environment, can get other players to innovate in that space.

I said earlier that children and young people are active. The DfE was thinking about—I do not know where it has got to—whether some of the innovations needed to be done on a peer-to-peer basis. It was barking up the right tree, in that case, because young people probably know

where other young people will go to get advice or navigate around those interventions.

Earl of Caithness: Do you agree with the evidence we have been given that children in the UK are as well protected on the internet as any children in the world?

Dr Marc Bush: We are not a web-based organisation; we are about mental health. From what we understand, they are probably some of the best protected among web-enabled youth. It is just that where we have got to is slightly dated, and we need to update some of those protections and move to a promotion agenda.

Q107 **Baroness Bonham-Carter of Yarnbury:** This question is about social media platforms. A topical story at the moment is about the disappearance of a young man, Arthur Heeler-Frood. His parents are requesting that Facebook supply information. Facebook is not supplying information. What is your take on the responsibility of social media platforms? It is a big question.

Dr Marc Bush: It is a huge question. I would have to take it from a children's safeguarding perspective. For me, if it tips into a protection or child safeguarding perspective, there should be a requirement on those platforms to share necessary data, because it could lead to a child being found earlier than otherwise.

Dr Nihara Krause: I agree.

Baroness Bonham-Carter of Yarnbury: You said something interesting earlier, which I wrote down but have now lost. You said it was the responsibility of ISPs to allow people to get rid of things, if they want to do that. I think you are saying it is also up to them to give information if it is of use in situations that involve children's safety.

Dr Marc Bush: Yes, particularly because information on the internet is not accredited; it is not checked factually. There are fewer spaces such as HeadMeds, which we run, that give young people practical advice on psychiatric medication and the consequences of taking it. That is an important place to signpost, because a peer telling a peer about their experiences of a medicine can say, "I had a good experience, but here are the things that might happen", or, "I had a terrible experience, but here are the things that might be good for you". It is enabling peers to be informed. Sometimes in peer-to-peer education we forget that it should be an informed peer to an informed peer, and a confident peer to a confident peer. If you lack confidence, you should be signposting on.

Baroness Bonham-Carter of Yarnbury: What if it is misinformation?

Dr Marc Bush: A lot of it is misinformation, and that is where the Government's role comes in, because they can say, "Here are places that we trust". For instance, Facebook could say, "Here are the 10 places we trust if you are in distress and you want to know more about mental health". That is being piloted in other countries in the world; it would not be a huge thing to pilot here.

The Chairman: You mentioned informed peers. That is what you have helped all of us to be. I thank you both very much. We have got to the

heart of some of the stuff the inquiry has been most concerned about. It is incredibly helpful. Thank you both very much for joining us today.

CAP and BBFC – oral evidence (QQ 87-97)

Transcript to be found under BBFC

CARE – written evidence (CHI0022)

About CARE

1. CARE (Christian Action Research and Education) is a well-established mainstream Christian charity providing resources and helping to bring Christian insight and experience to matters of public policy and practical caring initiatives across the UK.

Executive Summary

2. CARE warmly welcomes the Inquiry which seeks to assess both the opportunities and risks that are presented to children through the internet; and how policies can be developed to enhance the value of the internet for children. While CARE fully supports the very positive benefits that the internet can provide, our priorities are to ensure that parents are supported to manage their children's internet use, regardless of platform, and that children are protected from harmful material. Those principles inform this submission.

3. CARE makes seven key recommendations:

3.1 The Government should ensure that parents of children under the age of eighteen are informed about the risks associated with the internet and given information to keep their children safe (see questions 1, 2, and 6).

3.2 The Government must require ISPs to put 'default-on' family-friendly filters on the services they provide (see question 8).

3.3 The Government must require ISPs to ensure age verification occurs before any changes to filtering levels (see question 8).

3.4 The Government should ensure that smaller ISPs put in place family-friendly filters and controls on the internet services they provide to the same standards as the big four ISPs (see question 8).

3.5 The Government should enact legislation by the end of 2016 to make its current arrangement with the big four ISPs[30] legal, following the recent EU Net Neutrality vote (see question 8) and use the opportunity to extend family friendly filtering to all ISPs.

3.6 The Government should ensure a level playing field offline and online regarding the regulation of different types of media and ensure consistency of approach for video-like material so that '18' rated pornographic material consumed via video on demand is subject to age verification (see question 9).

3.7 The Government must strengthen the enforcement mechanism in Part 3 of the Digital Economy Bill (age verification of pornographic websites) by introducing mandatory financial transaction blocking and giving the

30 The big four ISPs are: BT, Virgin Media, TalkTalk and Sky

regulator a power to block particular websites, as needed (see question 10).

4. Our submission answers questions 1 to 3 and 6 to 10.

Inquiry Questions

Risks and benefits

Question 1: What risks and benefits does increased internet usage present to children, with particular regard to: i. Social development and wellbeing ii. Neurological, cognitive and emotional development, iii. Data security

5. CARE believes that although the internet can provide an array of benefits and opportunities for children – such as giving children the ability to inform themselves of the world around them and the ability to socialise with peers – it can also pose some very serious risks. CARE's focus is on children's access (whether deliberately or unintentionally[31]) to inappropriate, sexualised/pornographic material and the impact this has on them.

6. Studies examining children's access to pornography have shown the affect pornography use can have on young people's **social development and wellbeing** in the development of their attitudes towards sex, relationships and themselves.

7. Research suggests that:
   - At 11 years old most of the children surveyed *had not* seen pornography – only 28% of 11-12 year olds had seen pornography. [32]
   - By 15, children were more likely than not to have seen online pornography (65% of 15-16 year olds report seeing pornography). [33]
   - There is easy access to hard core pornographic material[34] that can be violent and degrading to women.[35] [36]

---

31 "I wasn't sure if it was normal to watch it…" Elena Martellozzo, Andy Monaghan, Joanna R. Adler, Julia Davidson, Rodolfo Leyva and Miranda A.H. Horvath, (June 2016), page 23 Study covers 1,001 children between the ages of 11 and 16 year old. Commissioned by the Children's Commissioner for England and the NSPCC https://www.nspcc.org.uk/globalassets/documents/research-reports/mdx-nspcc-occ-pornography-report-final.pdf

32 *Ibid,* page 8

33 *Ibid,* page 8

34 In March 2014, the regulator for on-demand TV reported that the vast majority of pornography sites visited were not UK-based and that 23 of the top 25 adult websites provided "instant, free and unrestricted access to hard core pornographic videos", accessible to under-18s. *For Adults Only? Underage access to online porn*, The Authority for Television on Demand, March 2014, pages 4 & 19 (no longer online)

35 The Deputy Children's Commissioner for England said *"Explicit sex and violent still and moving images depicting rape, bestiality, the use of pain and humiliation are potentially just a few clicks away."*
Basically…porn is everywhere – A Rapid Evidence Assessment of the effects that access and exposure to pornography have on children and young people, Horvath, Miranda and Alys, Llian and Massey, Kristina and Pina, Afroditi and Scally, Maria and Adler, Joanna R. (2013), page 4, Produced for the Children's Commissioner for England

8. Early exposure to pornographic material can be extremely harmful to children. *The Economist* reported that given the view that sexual tastes are formed around puberty *"ill-timed exposure to unpleasant or bizarre material could cause a lifelong problem."*[37] CARE is concerned that viewing pornography can lead to:

8.1 ***Unrealistic attitudes to sex**:*

- A 2016 study found that 53% of boys believed that pornography was realistic as opposed to 39% of girls[38] and a significant minority wanted to copy what they saw - 21% of 11 -12 year olds; 39% of 13-14 year olds and 42% of 15-16 year olds.[39]
- 72% of participants in a small 2014 study believed that *"pornography leads to unrealistic attitudes to sex."*[40]

8.2 ***Damaging impact on young people's views of sex or relationships.***

- The 2016 study found that children in the sample reported feeling curious (41%); shocked (27%); confused (24%) when they first watched pornography. However, what is most noteworthy about the findings is that these negative emotions *"subsided through repeated viewing of online pornography."*[41] This raises concerns over the normalisation of pornography among young people. The research commissioners said *"we need to ensure that we are not creating a narrative for young people that viewing and emulating online pornography is normal, acceptable or indeed expected."*[42]
- A 2015 literature review reported both boys and girls indicated that they had encountered *"shock," "surprise," "guilt," "shame"* and *"unwanted thoughts" in* relation to their pornography experience.[43]
- 70% of participants in 2014 said that *"pornography can have a damaging impact on young people's views of sex or relationships."*[44]
- A 2013 Rapid Evidence Assessment concluded that *"access and exposure to pornography affect children and young people's sexual*

---

https://kar.kent.ac.uk/44763/

36 See also Bridges AJ et al, Aggression and sexual behaviour in best-selling pornography videos: a content analysis update, Violence Against Women. 2010 Oct;16(10):1065-85. Suggested that 88% of scenes in popular pornographic videos contained physical aggression and 49% verbal aggression. http://www.ncbi.nlm.nih.gov/pubmed/20980228/

37 'A User's Manual', *The Economist,* 26 September 2015, http://www.economist.com/news/international/21666113-hardcore-abundant-and-free-what-online-pornography-doing-sexual-tastesand

38 "I wasn't sure if it was normal to watch it…", *Op Cit* page 9

39 *Ibid*, page 10

40 Young People, Sex and Relationships: The New Norms,' *Institute for Public Policy Research*, August 2014, page 4. Study involved 500 18 year olds http://www.ippr.org/files/publications/pdf/young-people-sex-relationships_Aug2014.pdf?noredirect=1

41 "I wasn't sure if it was normal to watch it…", *Op Cit,* page 9

42 *Ibid*, page 1

43 Sexual rights and sexual risks among youth online, A review of existing knowledge regarding children and young people's developing sexuality in relation to new media environments, Sonia Livingstone and Jessica Mason, Sept 2015, page 35 https://www.cois.org/uploaded/Documentation/For_Consultants_and_Supporting_Organisations/Affiliated_Consultants/Spotlight/Susie_March_-_Review_on_Sexual_rights_and_sexual_risks_among_online_youth.PDF

44 Young People, Sex and Relationships: The New Norms,' *Op Cit*, page 4

beliefs… Maladaptive attitudes about relationships; more sexually permissive attitudes; greater acceptance of casual sex; beliefs that women are sex objects; more frequent thoughts about sex… Pornography has been linked to sexually coercive behaviour among young people and, for young women, viewing pornography is linked with higher rates of sexual harassment and forced sex."[45]

- A similar conclusion was reached by a 2015 literature review, which noted research indicating exposure to pornography can lead to more permissive sexual attitudes; acceptance of casual sex and heavily influence the way that young people – both young men and women – believe they should either look or act during 'real world' sex, alluding to boys feeling 'performance anxiety' from pornography and other media.[46]

8.3 ***Pressure for young girls/women to act or look a certain way***

- The 2014 study reported 77% of young girls stated that *"pornography has led to pressure on girls or young women to look a certain way."* And 75% of young girls said that *"pornography has led to pressure on girls and young women to act a certain way."*[47]
- The 2015 literature review noted that some, but not all young people believed that pornography creates double standards in relation to boys' and girls' behaviour and that much of the research also revealed the pressures that girls face to have the ideal body type and operate "*in an environment where hyper-sexual femininity is normative*".[48]

8.4 ***Risky Behaviours***

- The 2013 Rapid Evidence Assessment concluded that *"access and exposure to pornography are linked to children and young people's engagement in "risky behaviours",* which are likely to include having sex at an earlier age; having unprotected sex or using drugs and alcohol whilst having sex.[49] [50]
- Two reports published in 2016 reported that children were aware of the pressures on girls to send nude or revealing pictures of themselves through social media. [51] [52]

8.4 ***Criminal Activity***

- Many judges have identified pornography as a significant factor in criminal cases brought before the courts - many of these cases involve

---

45 Basically…porn is everywhere, *Op Cit*, pages 7 and 8

46 Sexual rights and sexual risks among youth online, *Op Cit*, pages 10, 23, 36 and37

47 Young People, Sex and Relationships: The New Norms,' *Op Cit*, page 4

48 Sexual rights and sexual risks among youth online, *Op Cit*, pages 23 and 24

49 Basically…porn is everywhere, *Op Cit,* pages 7 and 35, Note that that definitions of risky behaviour vary across cultures.

50 Similar concerns have been found in research studies cited in Sexual rights and sexual risks among youth online, *Op Cit*, pages 37 and 38

51 Ofcom: Children's Media Lives – Year 2 findings, 27 January 2016, page 9 - Study of 18 children aged 8-15 http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/childrens-media-lives-year-2/children_media_lives_year2.pdf

52 A minority of young people had generated naked or semi-naked images of themselves; some of them had shared the images further, "I wasn't sure if it was normal to watch it…", *Op Cit,* page 10, 11 and section 5.3

children both as perpetrators of heinous sexual acts and as victims of such acts; [53] such stories reveal the disastrous consequences that occur when children access pornography.

9. In summary, "*children viewing highly sexualised pornographic material are at risk of negatively affecting their psychological development and mental health by potentially skewing their views of normality and acceptable behaviour at a critical time of development in their life"*[54] and "*it cannot be right that so many children may be stumbling across and learning about sex from degrading and violent depictions of it".*[55]

Question 2: Which platforms and sites are most popular among children and how do young people use them? Many of the online services used by children are not specifically designed for children. What problems does this present?

10. **CARE's particular concern is children's access to pornographic material on the internet. Children can and do access (whether purposefully or accidentally[56]) these sites which are not specifically designed for them, and which inherently pose risks for younger audiences, as acknowledged in response to question 1. With 24% of 8-11 year olds and 69% of 12-15 year olds now owning a smartphone[57] allowing them to access the internet away from home and far from parental supervision there are challenges for parents to ensure their children utilise the internet safely. This fact has led to a number of initiatives set out in this submission by industry and Government to protect children and encourage parents to support their children's safe online use. This submission critiques those initiatives.**

Question 3: What are the technical challenges for introducing greater controls on internet usage by children?

11. CARE's response deals with the verification processes on the internet that determine whether a person is under or over the age of 18 years since *"Electronic age verification plays an important part in assisting parents and caregivers by enabling businesses to enact the same protection*

---

53 *Boy aged 10 'raped male classmate in the school toilets, as he acted out online* porn', court told, Mail Online, 22 April 2014 http://www.dailymail.co.uk/news/article-2610371/Schoolboy-10-raped-boy-school-toilets-seeing-internet-pornography-deciding-act-out.html#ixzz3K5J4B2S1; *Blackburn boy, 13 rapes his sister, after watching porn on Xbox*, Lancashire Telegraph, 7 February 2014

54 Submissions, Inquiry into the Harm Being Done to Australian Children Through Access to Pornography on the Internet, Parliament of Australia, Submission 11 http://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Environment_and_Communications/Online_access_to_porn/Submissions

55 "I wasn't sure if it was normal to watch it…", *Op Cit,* page 2

56 "*Ibid*, page 23

57 Ofcom Children and Parents: Media Use and Attitudes Report, November 2015, page 6 http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/children-parents-nov-15/childrens_parents_nov2015.pdf

standards online that have been recognised and enforced in our bricks and mortar world."[58]

12. CARE fully supports the principle of requiring commercial pornographic websites to institute age verification through the Digital Economy Bill (see questions 9 and 10 below). However CARE recognises for age verification to be successfully implemented for the public and industry, the technical process needs to be:[59] [60]
    - affordable – both for the investment in the systems and the cost per check;
    - easily used by consumers;
    - not over intrusive into privacy otherwise consumers will migrate to uncompliant websites;
    - reliable – providing excellent match rates so that eligible consumers are allowed access and children correctly protected. Without this there will be no trust from the public and liability issues for websites.

    We recommend that the Government considers all these points in developing the age verification framework keeping in mind the importance of a robust age verification process (both in structure and enforcement) for protecting children (see also question 10).

Question 6: Who currently informs parents of risks? What is the role for commercial organisations to teach e-safety to parents? How could parents be better informed about risks?

13. Our answers to questions 1 and 2, show that there are risks for children amidst the vast opportunities of the internet. CARE believes that parents have the primary responsibility to raise their children as good and safe digital citizens. We advocate for parents to be provided with both the information and the tools they need to help them do this. There also needs to be a partnership between parents, industry and government to minimise the potential harm to children from exposure to pornography.

14. Despite the fact that UK parents intervene more than their European counterparts, with regards to what their children are accessing online,[61] there is still more that could be done to better inform parents about e-safety. Last year's Ofcom report on Parents and Children's Media Use showed that parental views are mixed when it comes to whether they believe that their children know more about the internet than they do –

---

58 Doing the Right Thing: How Electronic Age Verification Protects Kids Online, An IDology Whitepaper, 2006, page 4. Available from http://ww2.idology.com/lp/age_verification_whitepaper.html

59 Adult Providers Network Seminar on Age Verification, 15 May 2014 http://www.adultprovidernetwork.co.uk/age-verification-in-practice-seminar-minutes/

60 Nash V et al, University of Oxford, Effective age verification techniques: Lessons to be learnt from the online gambling industry, Final Report, December 2012-December 2013, pages 4 and 40 https://www.oii.ox.ac.uk/archive/downloads/publications/Effective-Age-Verification-Techniques.pdf

61 Livingstone et al, *Net Children Go Mobile. The UK Report. A Comparative Report with Findings from the UK 2010 Survey by EU Kids Online,* July 2014, page 53 http://eprints.lse.ac.uk/57598/

with 43% of parents with children aged 5-15 agreeing with the statement *"my child knows more about the internet than I do"* and 42% disagreeing.[62]

15. A report published at the beginning of 2015 on children under 8 and their use of digital technology, cited "*evidence of gaps in parental knowledge relating to online risks*" and recommended: "*Development and promotion of parental and carer education materials [..to] encompass safety settings, passwords, privacy protection and content filters, and they should assist with the mediation of unsupervised internet access by young children*" as well as "*Development and promotion of communication strategies outlining how parents can talk to young children about managing online risk*."[63]

16. CARE firmly believes that parents must be equipped so that they can help their children use the internet as safely as they can. We support principles in Lady Howe's most recent Online Safety Bill which requires **that online providers give information about online safety when a service is purchased** (clause 4) and that there **should be a requirement on the Secretary of State to educate parents with children (under eighteen years of age) about tools that can help keep children safe online** such as filters and about safety risks associated with the internet (clause 6).[64]

Governance

Question 7: What are the challenges for media companies in providing services that take account of children? How do content providers differentiate their services for children, for example in respect of design?

17. CARE supports the view that the onus must be on media companies to consider the safety aspects of products and services that they design. In particular, CARE very much welcomed the Government's manifesto commitment to *"stop children's exposure to harmful sexualised content online, by requiring age-verification for access to all sites containing pornographic material and age-rating for all music videos"*[65] – which has now been incorporated into the Digital Economy Bill (but see our comments about regulation below).

---

62 Ofcom: Children and Parents: November 2015, *Op Cit* page 133

63 Livingstone et al (2014) Young children (0-8) and digital technology: a qualitative exploratory study - national report - UK. Joint Research Centre, European Commission, Luxembourg. - information taken from Executive Summary, pages 3-4 http://eprints.lse.ac.uk/60799/1/__lse.ac.uk_storage_LIBRARY_Secondary_libfile_shared_repository_Content_Livingstone%2C%20S_Young%20children%200-8_Livingstone_Young%20children%200-8_2015.pdf

64 Online Safety Bill 2016, http://www.publications.parliament.uk/pa/bills/lbill/2016-2017/0027/17027.pdf

65 Strong Leadership, A Clear Economic Plan, A Brighter, More Secure Future, *The Conservative Party Manifesto 2015,* https://s3-eu-west-1.amazonaws.com/manifesto2015/ConservativeManifesto2015.pdf

18. Pornographic website providers should be aware from all current data that children can and do access this material both through accidental and deliberate exposure.[66] The challenge is to manage the sites so that only those aged 18 and over are able to access them. A similar challenge is faced by gambling websites which are required to have age verification policies in place,[67] as well as sites selling alcohol, which are required to meet the mandatory licensing condition for age verification, whether the sale is online or offline.[68] Given that these online age restrictions already operate, the extension of age verification to pornography websites should be manageable and can build on the experience from other industries. CARE makes further recommendations about the proposals on age verification in the Digital Economy Bill under Question 10.

Question 8: What voluntary measures have already been put in place by providers of content to protect children? Are these sufficient? If not, what more could be done? Are company guidelines about child safety and rights accessible to parents and other users?

19. A voluntary agreement was established between the major mobile phone operators in 2004 to regulate adult content on mobile phones. The most recent Code of Practice was published in 2013.[69] In September 2013, British Board of Film Classification (BBFC) took over the Independent Mobile Classification Body and set out a new framework for classification of commercial content sold by mobile operators and for use of filtering other internet content with the aim of protecting *"children by restricting adult content to adults only".* CARE very much welcomes this initiative and notes that in the BBFC framework adult content goes beyond pornography to violence and drugs.[70]

20. In addition to the mobile phone operator agreement, the Government also made arrangements with the four largest internet service providers in 2013 (BT, Virgin Media, TalkTalk and Sky) to present customers with an "unavoidable choice" to make as to whether they wanted family-friendly filters. The agreement was not incorporated into statute and is conducted on a self-regulatory basis.[71] The agreement that was reached with the big four is a welcome step forward; however we are still of the view that the arrangements must go further in four areas.

---

66 *"I wasn't sure if it was normal to watch it…", Op Cit,* page 23

67 Social responsibility code provision 3.2.11, 3.2.13 Gambling Commission, License Conditions and Codes of Practice, February 2015

68 Sections 19 and 19A of the Licensing Act 2003 stipulate there are mandatory licensing conditions. Detailed requirements to meet the licensing conditions are set out in, Revised Guidance Issued under Section 182 of the Licensing Act 2003, March 2015. The age verification requirements are set out at paras 10.48-10.52, page 71

69 Applies to EE, O2, Vodafone and Three, http://www.mobilebroadbandgroup.com/documents/UKCodeofpractice_mobile_010713.pdf

70 Mobile Content, *British Board of Film Classification* http://www.bbfc.co.uk/what-classification/mobile-content

71 Ofcom Report on Internet Safety Measures, Strategies of parental protection for children online, 16 December 2015, Executive Summary, pages 3-5 http://stakeholders.ofcom.org.uk/internet/internet-safety-dec-2015

21. Firstly, Ofcom's most recent report on ISP filtering showed a very variable take up amongst users.[72] It was found that whilst awareness of ISP content filters among parents of 5-15 year olds had increased from 50% in 2014 to 57% in 2015, actual use of the filters remained relatively low in 2015 at 26% (although this was an increase of 5% on the previous year).[73] A first step in helping equip parents would be for commercial organisations to provide "opt-in or default-on" internet services to *all* households – in this scenario, internet service providers would automatically place family-friendly filters and controls on their services unless an internet user who is over the age of 18 chooses to opt-in to receiving internet services with adult content. Sky has already taken the initiative to adopt this 'opt-in/default–on' approach to their services[74] and has seen an increase in the number of households using their filtering options from 62% of existing customers,[75] so we recommend that other ISPs should also follow suit. When considering the fact that parents' trust in their children to use the internet safely has decreased from 83% in 2014 to 78% in 2015,[76] tools that can help minimise exposure to inappropriate material would go a long way in protecting children, giving parents' greater confidence that their child is able to use the internet in a safer way. **CARE recommends that ISPs provide 'default on' family-friendly filters on their services to help minimise children's exposure to inappropriate online content.**

22. Secondly, the family-friendly filter arrangement with the big four ISPs does not provide sufficient age verification before allowing filters to be changed. Currently, all of the big four ISPs' voluntary family-friendly filter schemes have similar mechanisms which allow for family-friendly filtering settings to be changed as and when requested: a verification email will then be sent to the account holder confirming that such action had been taken.[77] This so-called 'closed-loop' approach does not consider the fact that a verification email sent to the account holder would require monitoring and would potentially mean that any child who had changed the settings would be able to view inappropriate content until the account holder viewed the email and changed the settings, which maybe hours after or even days, or maybe not at all. **CARE recommends that ISPs must be required to ensure robust age verification takes place prior to filters beings lifted.**

23. Thirdly, the family-friendly filter arrangement currently excludes smaller ISPs which means that potentially 12% of the market do not benefit from family filters.[78] All children – no matter which ISP provides services to

---

72 *Ibid,* paras 1.16-1.19, page 6

73 *Ibid,* paras 1.22-1.23, page 7

74 Sky to block pornography by default to protect children, *BBC News*, 20 January 2015 http://www.bbc.co.uk/news/technology-30896813

75 Ofcom Report on Internet Safety Measures, Strategies, *Op Cit,* para 3.20, page 22, para 3.38, page 26

76 *Ibid,* para 9.4, page 66 – this is based on parents of children aged 5-15

77 Ofcom, Report on Internet Safety Measures. Internet Service Providers: Network Level Filtering Measures, 22 July 2014, page 3, http://stakeholders.ofcom.org.uk/binaries/internet/internet_safety_measures_2.pdf

78 Smaller ISPs and EE currently hold 12% of the market (end of 2015), See Ofcom, Facts and figures http://media.ofcom.org.uk/facts/

their home – should be able to browse the internet as safely as possible. The current arrangement provides the unsatisfactory scenario whereby some children are afforded greater protection through the option of family-friendly filters than others – this anomaly must be rectified. **CARE recommends that smaller ISPs should be in scope of the family–friendly filtering arrangements and have to meet the same standards as the big four ISPs.**

24. Fourthly, in October 2015 the European Parliament voted in favour of net neutrality principles to be implemented at the end of 2016, which would prohibit internet services being treated in a discriminatory way. This EU vote raises questions over the legality of the voluntary family-friendly filter arrangement with the big four ISPs. During Prime Minister's Questions on 28 October 2015, David Cameron stated that the Government would legislate to ensure the legality of the family-filter arrangements with the big four.[79] [80] **CARE believes that enshrining the Government's arrangement with the big four ISPs in legislation by the end of 2016 should remain a priority for the Government so that parents have the tools they need to manage their child's internet access.** The Government should use the legislative opportunity to extend family friendly filtering to all ISPs, to improve age verification procedures before filters are lifted, and to ensure there is a transparent, consistent approach between all ISPs in the level of filtering provided (which would be achieved by clause 2 of Baroness Howe's Bill[81]) since the big fours ISPs do not currently operate within any agreed transparent classification framework similar to the framework operated by the BBFC nor is there any appeals process for sites that are either over blocked or allowed through filters. [82]

Legislation and Regulation

Question 9: What are the regulatory frameworks in different media? Is current legislation adequate in the area of child protection online? Is the law routinely enforced across different media? What, if any, are the

---

79 *"We secured an opt-out yesterday so that we can keep our family-friendly filters to protect children. I can tell the House that **we will legislate** to put our agreement with internet companies on this issue into the law of the land so that our children will be protected" (emphasis added)* Question 9, Prime Minister's Questions, 28 Oct 2015 Column 344 http://www.publications.parliament.uk/pa/cm201516/cmhansrd/cm151028/debtext/151028-0001.htm#15102833000668

80 During Committee Stage of Baroness Howe's Online Safety Bill 2015, the Minster for Internet Safety and Security, Baroness Shields made a similar comment *"we must legislate to make our filters regime legal according to the new net neutrality regulations. The date for that is by December 2016."* 11 December 2015, Column 1803 http://www.publications.parliament.uk/pa/ld201516/ldhansrd/text/151211-0001.htm#15121154000396

81 Online Safety Bill 2016, http://www.publications.parliament.uk/pa/bills/lbill/2016-2017/0027/17027.pdf

82 For instance see Ofcom Report on Internet Safety Measures, 22 July 2014, para 2.6 for how different ISPs put content in different categories; paras 2.32 and 2.33 report that "*ISPs outcomes and decision making process are therefore not centralised through one final arbiter or otherwise shared*" and there is no open information for individual websites about how they are classified, para 2.37. http://media.ofcom.org.uk/news/2014/internet-safety-measures/

gaps? What impact does the legislation and regulation have on the way children and young people experience and use the internet? Should there be a more consistent approach?

25. CARE is particularly concerned about children either accidently or intentionally accessing: pornographic content, 18 rated and R18 material through a variety of media. Our response will therefore focus on regulation as it pertains to these issues.

DVDs and Blu-Rays Available Offline

26. Offline physical media is classified under the Video Recordings Act 1984 by the British Board of Film Classification (BBFC). Supply of an '18' classified DVD/Blu-Ray to someone under 18 is a criminal offence under the Act. Supply of DVDs/Blu-Rays that are classified 'R18' outside of a licensed sex shop is also an offence. Both offences are subject to a fine or imprisonment for up to six months (sections 11 and 12 of the Act, respectively).

On- Demand Programme services

27. The Audiovisual Media Services Regulations amended the Communications Act 2003 (section 368E(4)) to require companies providing on-demand services to ensure "harmful material" is only "*made available in a manner which secures that persons under the age of 18 will not normally see or hear it",* with the expectation that this will be through age verification procedures, although this is not set out in statute only in guidance.[83] However, this "safeguard" only applies to R18 and not 18 rated material which is unsatisfactory. Given that society has decided that it is not appropriate for children to watch 18 rated films like *Fifty Shades of Grey* offline *and* the technology exists for protecting children from watching adult video on demand material online, it is not defensible to say children should only be protected from watching R18 material online. Logically they should be protected from watching both 18 and R18 material offline *and* online. Furthermore, recent Ofcom data shows that for young adults aged 16-24 viewing paid-for on-demand content accounted for 20% of this age group's total viewing time in 2016.[84] As on-demand material becomes an increasingly important part of the viewing habits of younger people, the need for consistent policies on accessing age restricted material becomes more important since some of this age group would not be able to watch the same material "offline" were it classified "18". CARE welcomes clause 8 of Baroness Howe's Bill that would ensure age verification for video on demand would include 18 material.

Pornography websites

---

83 Ofcom Rules and Guidance, Statutory Rules and Non-binding Guidance for Providers of On-Demand Programme Services (ODPS), pages 10-12 http://stakeholders.ofcom.org.uk/binaries/broadcast/on-demand/rules-guidance/rules_and_guidance.pdf

84 Ofcom: The Communications Market Report, August 2016, page 57 http://stakeholders.ofcom.org.uk/binaries/research/cmr/cmr16/uk/CMR_UK_2016.pdf

28. The Government has recently sought to uphold its manifesto commitment to "*stop children's exposure to harmful sexualised content online, by requiring age-verification for access to all sites containing pornographic material and age-rating for all music videos."*[85] It has followed through on this promise in Part 3 of the Digital Economy Bill which proposes that all overseas and UK commercial websites and apps[86] that are making pornography available in the UK should have an age verification procedure that prevents children and young people from accessing this material (clause 15) – CARE welcomes Part 3 of the Bill in principle (see also our answer to question 10).

29. CARE believes there should be a level playing field across all media. For this reason, prior to the Bill's publication we argued for a criminal offence rather a civil offence for the new proposals in the Digital Economy Bill. We are also concerned that the measures in the Bill exclude on-demand programme services from the scope of Part 3 (see clause 15(6)) as they are already regulated by Ofcom under the Communications Act 2003, which means that there would still be no level playing field across video-like material. **CARE recommends that age verification which already applies to R18 for on-demand programming regulated by Ofcom should extend to '18' pornographic material as well so there is consistency of treatment of video-like material.**

Question 10: What challenges face the development and application of effective legislation? In particular in relation to the use of national laws in an international/cross-national context and the constantly changing nature and availability of internet sites and digital technologies? To what extent can legislation anticipate and manage future risks?

30. Our response deals with the current issues raised by the Digital Economy Bill. Our concerns about consistency of treatment are set out in question 9. The central challenge to the Government's proposals **is enforcement**. This challenge is critical given so many popular pornography sites are based in other jurisdictions. In March 2014, the then regulator for on-demand TV reported that the vast majority of pornography sites visited were not UK-based and that 23 of the top 25 adult websites provided *"instant, free and unrestricted access to hard core pornographic videos,"* accessible to under-18s.[87] CARE's concern is that foreign websites will have no strong commercial incentives to comply with the proposed age verification rules. A similar point was made in a review of age verification systems by the University of Oxford which noted that for gambling websites where there are "*strict audit and enforcement requirements*", there is incentive to invest in "*high-assurance identity and age-verification processes" but "where enforcement is patchy and uncertain, the incentives to invest in expensive authentication systems are less clear"*[88]

---

85 *Conservative Party Manifesto 2015, Op Cit*

86 Child Safety Online: Age Verification Consultation Response, July 2016 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/534965/20160705_AVConsultationResponseFINAL__2_.pdf, page 7 – but excluding services regulated under on-demand programme services

87 For Adults Only? Underage access to online porn, *Op Cit*, pages 4 & 19

88 University of Oxford, Effective age verification techniques*, Op Cit,* page 27

and that is "*especially true for smaller or less well-known companies who are also less likely to receive reputational damage if any illegal selling is revealed*."[89] Part 3 of the Bill as currently defined, however, fails to address the concern about enforcement

31. Firstly, while there is an ability to impose large fines (clause 21(2)) these are likely to be only for "*persistent non-compliance*".[90] It is, therefore, not clear what would happen if there was no compliance or the fines were not paid, nor how fines would be collected from websites based outside of the UK.

32. Secondly, the Government also stated that its *"preference is for the regulator to have discretion as to which sites and providers it takes enforcement action against."*[91] CARE is particularly concerned with this approach – if the regulator decides that it will only take enforcement action against certain sites, children could simply switch to watching pornographic material on sites which the regulator is not pursuing, and which potentially have no age verification. The University of Oxford reported on gambling websites that "*one of the biggest sources of irritation for the responsible operators that we interviewed, is the ease with which customers can turn to unlicensed competitors whose operation may be illegal, but very difficult to prevent*."[92]

33. Thirdly, CARE believes that that pornography providers would be strongly incentivised to comply with the age verification proposals through financial transaction blocking. Mandatory financial transaction blocking would ensure that payments made by UK customers to defaulting pornography sites – that is, sites that do not place robust age verification mechanisms on their services – would be blocked until age verification requirements are followed. This proposal was put forward by Baroness Howe in her Online Safety Bill[93] and was also considered by the Authority for Television on Demand (ATVOD) in relation to foreign websites.[94] The Government has stated that payment providers will be able to *"withdraw services"* from sites that do not comply with the new regulatory system that mandates age verification and that this would *"nudge porn providers to comply and put age verification in place."*[95] The notion of *"nudging"* porn operators gives marginal reassurance that companies will be ***required to*** comply. While the Digital Economy Bill allows for the regulator to inform payment providers or ancillary services of non-compliance (clause 22), there is ***no requirement*** for them to act to block payments or withdraw services. The Government says that because the law would be clear about the non-compliance, "*we do not think it would be appropriate or*

89 *Ibid,* page 39
90 Child Safety Online: Age Verification Consultation Response, *Op Cit*, page 10
91 *Ibid,* page 11
92 University of Oxford, Effective age verification techniques*, Op Cit,* page 39
93 Clause 12, Online Safety Bill http://www.publications.parliament.uk/pa/bills/lbill/2016-2017/0027/17027.pdf
94 For Adults Only? Underage access to online porn, *Op Cit*, page 5
95 Age Verification for pornographic material online, Impact Assessment, Department for Culture, Media and Sport, 25 May 2016, page 9 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/538426/2016-06-06_Age_verification_impact_assessment__1_.pdf

necessary to place a specific legal requirement on these payment providers to remove services."[96] The Government is relying on these financial services companies acting to remove services on the basis that their terms and conditions require merchants to be operating legally in the country they serve. **This is not sufficient.**

34. Fourthly, should fines, financial transaction blocking or removal of ancillary services like advertising not be sufficient incentives for websites to comply, CARE believes that there should be a power in the Bill to allow IP blocking (blocking non-compliant websites). The Government has said this would be disproportionate and not in line with other policy areas (e.g. terrorism)[97] but IP blocking can already be used for copyright infringement so there is a logical argument to extend it to child protection.[98] Internet Service Providers say it would not be effective but the NSPCC, the BBFC, some pornography companies and the Digital Policy Alliance are in support of such a proposal.[99] CARE believes that the Digital Economy Bill should be amended to include the option of IP blocking as a means of strengthening the enforcement mechanism for age verification.

35. In order to meet its commitment to protect children, **CARE recommends that the Government must strengthen the enforcement mechanism in Part 3 of the Digital Economy Bill, particularly with regard to foreign websites. Part 3 must be amended to require Financial Transaction Blocking and give a power for IP Blocking.**

26 August 2016

96 Child Safety Online: Age Verification Consultation Response, *Op Cit,* page 12
97 *Ibid,* page 6
98 Section 97A, Copyright Designs and Patents Act 1988 http://www.legislation.gov.uk/ukpga/1988/48/section/97A
99 Child Safety Online: Age Verification Consultation Response, *Op Cit,* pages 22, 24, 26 and 28

Childnet International and UK Children's Charities' Coalition on Internet Safety – oral evidence (QQ 1-10)

Evidence Session No. 1 *Heard in Public* *Questions 1 - 17*

TUESDAY 19 JULY 2016

Members present

Lord Best (Chairman)
Lord Allen of Kensington
Baroness Benjamin
Baroness Bonham-Carter of Yarnbury
Earl of Caithness
Bishop of Chelmsford
Baroness Kidron
Baroness McIntosh of Hudnall
Baroness Quin
Lord Sheikh
Lord Sherbourne of Didsbury

_____

Examination of Witnesses

Will Gardner, CEO, Childnet International, and **John Carr OBE**, Secretary, UK Children's Charities' Coalition on Internet Safety

Q18 The Chairman: I welcome you both; thank you very much for joining us. Before we get into questions, perhaps you could introduce yourselves to us and tell us a little about your background so that it goes on the record formally. John, would you go first?

John Carr: I am John Carr. I am secretary of something called the Children's Charities' Coalition on Internet Safety, which is an alliance of all the big, professional children's charities, such as the NSPCC, Barnardo's, the Children's Society and so on. Essentially, we monitor policies impacting on children's use of digital technologies with a view to seeking their improvement or betterment, which means we talk a lot to the industry as well as to several different parts of government, Parliament of course, and the media.

The Chairman: Thank you very much.

Will Gardner: I am Will Gardner. I am the CEO of Childnet International, which is a children's charity. It is 20 years old, and its mission is to help make the internet a great and safe place for children. We work in schools; we have a team that goes out to schools across the country, talking to children and young people, parents and carers, and staff. We speak to young people from the age range of three up to 18, with the goal of giving young people the skills to use this amazing technology safely and responsibly. We develop educational

materials, which we put online for free for schools and others to access so they can also help support young people in this space.

We work on the policy side too, and with John and Sonia we are members of the UKCCIS executive board. We work collaboratively with industry, charities and other sectors to pursue this mission. We also form part of the UK's Safer Internet Centre, which is a part-EU-funded project, which brings together the Internet Watch Foundation as a hotline, the South West Grid for Learning as a helpline for professionals working with children and ourselves as an awareness centre, and we organise Safer Internet Day in the UK.

The Chairman: Thank you very much. The first question is from Lord Sherbourne.

Q19 Lord Sherbourne of Didsbury: Drawing on your practical experience, which is a big advantage to the Committee, and from what you have seen and the work you have done, we know there are lots of advantages and benefits of the internet for children in the different age groups that you cover, and we know there are a lot of risks. Focusing on the risk at the moment, what do you think are the greatest risks that young people face with the internet?

Will Gardner: There are different ways of answering that question. First, what is the one that young people are most worried about and are perhaps most likely to come across? If you were talking to young people, they would pick up cyberbullying. Their peer group is the one that they would be most worried about. They are worried about mean comments online and content that they see online that is upsetting. These are things that they would highlight. Clearly, the risks are broader than that, and the ones that are perhaps not as common, just as the very common ones, can be just as harmful in certain circumstances, such as grooming, sexual exploitation, online reputational damage and so on. There is a wide range of potential risks, and the challenge for us, without going too far away from the question, is that we have to recognise that there are risks and, as Tanya Byron did in a review a few years ago, recognise that we cannot always remove those risks. We have to give young people the skills to manage the risks as best they can.

Lord Sherbourne of Didsbury: As a follow-up to that, what is your assessment of their sense of awareness of these risks?

Will Gardner: It varies from age to age, but in the work that we have done in primary schools and in secondary schools I think young people are aware of risks. It does not always mean they act responsibly and safely while they are using technology, but there is a general awareness of internet safety. There has been a lot of work done in schools over a large number of years, and it is a question of trying to drive that awareness into behaviour change, which is the challenge that we face.

Lord Sherbourne of Didsbury: Is there anything, Mr Carr, you would like to add to that?

John Carr: Empirically, there is no doubt that bullying and online harassment of various kinds is, without question, the issue that most children and young people would mention at the top of their list in terms of behavioural issues. In relation to content, Professor Livingstone is sitting up there, so I am sure she

will correct me if I have got this wrong, but, in the study that she did on EU Kids Online, the class of content that most people mention most frequently that they found upsetting was pornographic material, broadly agreeing with what Will has just said.

The Chairman: To get the balance right, could you also say what you see as the greatest benefits of the internet for children?

John Carr: The benefits are immense. It has completely transformed the way in which children can access cultural, educational and sporting information. Every type of information is there at their fingertips. Sadly, in my day, we had to go to libraries and get out books and stuff like that. I am not saying that was a bad thing to do, but it is just so much easier and there is a richness of material available to young people.

The Chairman: Is that what young people identify as the great advantage—not going to the library?

John Carr: My guess would be that most young people would rate the interactive components No. 1—the way in which they can stay in touch with their friends, keep up to date with what is happening in their crowd at school, their sports team and their favourite band. In terms of the broader picture, there is no doubt at all that all those other factors are there.

Will Gardner: I would agree with that. Educationally, it is a very important element for young people. New technology brings huge benefits for discovering, exploring and so on. It has become part of the social lives of young people. It is very integrated into that, and there is pressure on young people as they get older to be interacting within these environments. It can be a great advantage to communicate in groups in that way. It is also a great source of support and advice even for young people for a range of different topics with information that they might not want to ask trusted adults about; it can be a source of information and help in certain circumstances too. There is a nice cartoon from about 10 years ago that summed it up saying, "What is the greatest risk about the internet?" It is that we forget about the benefits and we focus on the negatives, and it is really important that this part of the conversation has its weight in here.

The Chairman: Absolutely. Can I remind colleagues, before they ask a question, to declare any interests that they may have?

Q20 Baroness Quin: Obviously, children can experience bullying not online—offline—and may get access to pornographic material and so on. How would you describe the difference between the risks online and those offline for children?

Will Gardner: With different issues, it might have different impacts. With bullying, one of the messages we give out to schools is that cyberbullying is bullying; it is a behavioural thing, and the answer will very much lie in the relationships between the individuals involved. One of the things is not to get too drawn into the technical elements. It is not something for the ICT teacher to sort out. It is very much another type of issue. In relation to cyberbullying, for example, the issues are around the fact that it is 24/7. Even though it is bullying, there are some factors that add to that. If it is humiliating content, the audience can be much larger. There might be anonymity, which can be very

distressing for the person who is on the receiving end because they might not know who it is. On the other side, the internet is quite disinhibiting in relation to the cyberbullying topic, where you might say things online that you would not say face to face and you cannot necessarily see the impact of what you are doing on the person with whom you are communicating. That is the bullying angle.

If you go to pornography, if you look at the differences, accidental exposure to pornography online is probably what I would see as one of the biggest differences. The explicitness of the content and the fact that it can be moving, real time and all the rest of it is a big issue. The NSPCC study found very recently that accidental exposure was a big issue facing young people in relation to pornography, and I think that is significant.

Baroness Quin: Would you like to add something?

John Carr: I would. First, I think the word "pornography" is a problem, because for people of a certain age—including my own age, I might say—when you mention the word "pornography", a great many people still think that you are talking about *Playboy* centrefolds, pictures of ladies dancing without a bra on the beach or something of that kind. They have no idea about the nature of some of the material that is now instantly available on the internet to anybody of any age at the click of a mouse. It is not pornography as we would have understood it in the 1960s or 1970s. Overwhelmingly, it is anti-women violence, although there are other aspects to it, and the idea that any child or young person could ever learn anything of any value or use about sex, relationships or anything of the kind from some of the sites that I have had to look at from time to time is completely absurd. But the word itself has become an obstacle to understanding. I cannot think of a better word. I am trying. I will offer a prize to anybody who can think of a better phrase. You may know that in a related area we have stopped calling child pornography "child pornography"; we now call it "child abuse images", and that has become fairly well accepted. We have a similar challenge in relation to what historically has been called pornography, because the word no longer conveys in any meaningful way what it is we are discussing on the internet, which is why—I think we will come on to this later—the Government's Digital Economy Bill, which contains clauses on age verification, is exceptionally important, because we need to keep this kind of material away from young eyes.

Baroness McIntosh of Hudnall: I would like to go back to the distinction that you made, Mr Gardner, between what children or young people themselves say about what risks they fear or face, and what you would assess those risks as being or what the wider risks might be. We have some stats about how many children accidentally or otherwise encounter what we will continue to call pornography and various other things, but do you have any idea how many young people that you are aware of personally experience bullying behaviour, or whether they are aware of it and fear it because they know about it? What is the incidence, as it were, among young people of actual experience of cyberbullying?

Will Gardner: The numbers for cyberbullying are around 11% to 12%. I think that, last time, Sonia's research gave a figure of about 12% for young people who have experienced cyberbullying in the last year. The DfE did a big study that came out earlier this year, which gave a figure of about 11%. That is talking

about cyberbullying. There is a level below cyberbullying, which includes meanness online that might not have some of the hallmarks that you might apply to bullying, such as repetition or deliberate intent, but nevertheless was upsetting. Those are the kinds of numbers that we are talking about in relation to that.

Baroness McIntosh of Hudnall: If I can pursue this for a minute, beyond that, there are a lot of other young people who are perhaps not themselves experiencing this but are aware of it, presumably because they know people who are.

Will Gardner: Yes.

Baroness McIntosh of Hudnall: Does the fact that they know that they could become victims or that other people are victims have any effect on their behaviour—either how they use the internet or on their relationships?

Will Gardner: In a way, we are hoping that there will be that level of awareness about this to try to be a control on young people's behaviour in relation to others. On a slightly separate note, we looked at online hate for the last Safer Internet Day as a topic about young people's exposure to hateful messages online, not necessarily directed at them but more broadly. When I say "hateful", I mean targeting particular groups in our community, whether that is LGBT, young people and so on. Eighty per cent of young people had seen messages that were hateful online, which is very interesting, and that had had an impact on young people's confidence in engaging in the social media world. I cannot tell you the percentage off the top of my head, but there was a figure in there that was really interesting. Does that content influence how you interact with social media? You could see that that was a factor there.

Baroness McIntosh of Hudnall: That they felt more ready to engage.

Will Gardner: No. It was almost like a deterrent to engage with social media. They had seen that content out there and that was putting people off expressing themselves how they might want to, for fear of a retaliation not necessarily by people they know, but by the broader online community.

Q21 Baroness Kidron: Unfortunately, I have to do this technical thing of declaring my interests first, so forgive me. I am a founder of 5Rights, which is a campaign to make rights apply equally on and offline. Both in my capacity as an individual and through my company, I work with a broad range of companies and institutions to develop technical tools that improve young people's interaction with internet technologies, and I sit on a number of international and national task forces and commissions that have to do with young people and the internet.

My question is actually very short. Would you care to say something on the record about the gender aspect of what you have just said? If they fear to engage, is there a specific piece for young women and young girls?

Will Gardner: That is a very important point to add in. Something that came out of the research from *Net Children Go Mobile* is that girls, broadly speaking, have a worse time online in relation to this area, and that is really important to flag up. It is not exclusive; it is not just about girls; but I think that is very much worth taking into account. Therefore, we need to think about issues relating to

body image, peer pressure and other such things, and even think more broadly than that in relation to that particular topic.

Lord Sheikh: We have talked about the risks—bullying, grooming and sexual exploitation. There are some horror stories that we have heard where children who are being bullied have committed suicide. When a child is bullied, how likely are they to bottle it up inside, and how likely are they to talk to a teacher or a parent? If they do talk to a parent or somebody else, what help is available, because bullying can have very dire results?

Will Gardner: That is the big challenge for bullying as well as cyberbullying in relation to that. There are a number of different things we do know. If we ask children, "Who are you most likely to want to talk to about issues affecting you online?", we see that from the primary age through to the early secondary stage parents are No. 1; they would be the first port of call for young people. But when it gets to 13 and 14 year-olds, friends take over as the top people that a young person would want to go and talk to, and parents fall in at No. 2. They are still a significant second all the way through to 18 and remain there. We want to encourage young people to come forward. We have done some work asking young people about cyberbullying particularly and what the obstacles are to their coming forward and talking to their school about it. There is work that schools can do in relation to this, and schools are doing some work in this space, about encouraging even anonymous reporting. Cyberbullying can enable there to be witnesses in a way that perhaps would not necessarily be the case in offline bullying. There might be opportunities for children themselves or others to talk about something that is happening and for schools to be really clear about what they are going to do once they are told about something. Sometimes children are afraid of losing control and not knowing what is going to happen. Are they going to get into trouble? There is work to be done around this space.

In relation to this, as I said before, cyberbullying is bullying, and there is behaviour between individuals or groups. Schools have a long history of dealing with the issue of bullying from a pastoral perspective in trying to make the situation better. The systems are in place, and we want to encourage schools to recognise that they have knowledge in this, but there are some extra places to which they can turn. If it is on social media, there is reporting to social media to try to help get content taken down, if that is an appropriate way to go. There is a helpline supporting professionals in this space called the Professionals Online Safety Helpline, which we encourage our professionals to go to for advice on particular issues. There are things, absolutely, that schools can do, and there is guidance there. We have just developed some new guidance that we are about to bring out for schools in this space.

Lord Sheikh: Does the child feel that it is their fault? Do they feel like that sometimes?

Will Gardner: It can absolutely be that. You can imagine a situation where a humiliating picture of a child was taken and it is posted and shared. The child could feel embarrassed but also guilty that that is the case, and that could provide a barrier to their coming forward. There might be accusations of, "What were you doing that for?", or complicity in the picture and so on.

Q22 Baroness Bonham-Carter of Yarnbury: I want to ask you specifically about how governance and policy should be moulded and developed to address

the fact that we are talking about very different age groups. I also wanted to pick up on what Baroness Kidron said about the difference between what happens to boys and girls. My experience with children is this accidental access, which, as you get older, is presumably less of a problem; I do not know if that is the case. There are rather a lot of questions rolled into one major one, which is that you are talking about a very wide-ranging age group here.

John Carr: If I could say something on this question of governance, first, you are absolutely right that you need nuanced and different approaches for different age groups. Broadly speaking, in so far as we have laws around these things, people under the age of 13 are regarded as children, and there would be a whole raft of things that you would expect to apply in respect of them. But between the ages of 13 and 18 they are all lumped together in one chunk, and, again, similar policies would be applied to them. I am not sure that is a very good approach, because between the ages of, essentially, 12 and 18 children do a lot of growing up.

Baroness Bonham-Carter of Yarnbury: Is that based on just being teenagers?

John Carr: It is actually based on the American federal law. Most of the social media platforms, and that is essentially what we are talking about in these discussions, are American companies. Under US federal law, they are required to make a distinction between persons below the age of 13 and persons above the age of 13, and then up to 18. At 18, all bets are off. There are no special considerations or special rules that apply to them. Between the ages of 13 and 18—that is between 13 and 17, in other words—there are. Below the age of 13, you should not be on there in the first place.

On that point, as we know, recently the BBC published its research that corresponds very much with what Sonia and Will have done before, which was that 75% of 10, 11 and 12 year-olds in the United Kingdom were on social media platforms that legally were not supposed to have them there, because the legal minimum age for those platforms is 13. By the way, in the Czech Republic, I think the percentage is around 85%. In Cyprus, it is 80%. It is not that Britain's children are uniquely prone to misrepresenting their real age. It is happening pretty much universally, and it is all a product of this US federal law, which set 13 as the bottom limit but did not impose any obligation on the companies to verify the age of people when they applied to join or when they joined up. It is simply sufficient to tick a box to say, "Yes, I am 13", and that is it. The only legal obligation that the companies have after that point is, should they discover that somebody is in fact below the age of 13, they have to kick them off. The companies are allowed to take people under the age of 13 on to their sites, but if they choose to do that they must obtain parental consent. The companies have never wanted to get involved with the trouble, hassle and expense of seeking parental consent; so they simply say, "In that case, you have to be 13 to be a member". This has resulted in massive degrees of non-compliance in the UK and more widely.

On the question of governance, one in three of every internet user on the planet is below the age of 18. In parts of the developing world, it rises to one in two. This is the product of research published by UNICEF and Chatham House; Sonia Livingstone and I were joint authors of it, along with Jasmina Byrne. Young people are easily the biggest single distinguishable or definable constituent

group of internet users. You would not know that if you looked at the internet governance institutions. They are pretty much massively overlooked and disregarded, and it is a fault of governance institutions, fundamentally.

Baroness Kidron: John, can I ask you to unpick a little this point about 13 to 17, because I am not aware of so much work being done in separating out that group. In fact, I would say that "all bets are off" actually starts at the age of 14. You seemed to suggest that there was this group and they had special care, but I am not certain.

John Carr: I meant that, in relation to advertising, for example, of different types of products, below the age of 18, in theory and in principle, on Facebook, Google and all these other major social networking platforms, certain types of advertisements will never be presented to you. If you assume you have truthfully declared your age and it is below 18, certain classes of adverts will not be there. You will be able to disclose your physical location. A lot of these apps and these websites collect physical location data. If you are 18 or above, I think I am right that, by default, it is turned off. If you are below the age of 18, it is turned on. There are a number of things that do apply between the ages of 14 and 18.

My real point is this, though. We only have one rule. It is binary: 13 to 18 is too broad a spread. I remember that when I was 16 certain things were happening in my life that were not happening when I was 13 or 14. I think there is a case for saying that 13 to 18 is too broad a spread and it should be more closely examined and defined. I do not know what the answer is. It is very complicated and technically challenging, but that does not mean it should not be done.

Baroness Bonham-Carter of Yarnbury: Will might have wanted to answer.

Will Gardner: I was thinking when you were talking about policy more in relation to schools. There has been a lot of policy support in place for schools in relation to this particular area about developing acceptable use policies, training, education and awareness, and suchlike. There is a self-review tool available for schools called 360 Degree Safe, which is free; 10,000 schools are now using it and they are self-assessing what they are doing in relation to internet safety. It has given us an incredible picture, because that data is channelled back and we can see what is happening across the country in relation to e-safety, what are the areas of strength in schools and what are the areas of weakness. On the policy side and the filtering and connectivity angle, that is where the strengths are in schools. More in relation to staff and governance training is where the weaknesses currently are. That is what we know.

Baroness Bonham-Carter of Yarnbury: You think that is a good way forward.

Will Gardner: It is really important that we are looking to develop better training for school governors. The UK Council for Child Internet Safety is developing something for governors right now to try to support that level of knowledge. Staff training is an ongoing thing. There is work going on in this space, but it is a big challenge. As we know, children are as likely to come and talk to anybody in a school in relation to an incident of bullying, whether that be a teacher or a school staff member, and it is important that we make sure that there is that level of understanding and knowledge of what to do in order to respond to these issues.

Earl of Caithness: I just want to press you, Mr Carr, a little more because you ducked it right at the end when you said you did not like 13 to 18 as a group but you did not have an alternative. Come on—you have got to have an alternative.

John Carr: I can tell you what my gut feeling is, but this issue came up rather acutely when we were still full members of the European Union, because, there, they were considering a whole new set of data protection and privacy rules. The point of view that I expressed in my evidence to the European Union was that there ought to be proper, academic, independent research done into the different ages at which different types of capacity develop within children. There has been some done in relation to advertising and things of that kind, but it is rather old now. It was not specifically oriented towards the internet. So the view I expressed was, "Let us look again at the way children and young people are working in and around this new digital environment and see if there is a more nuanced view that we ought to be taking". Maybe 13 is the right age; maybe 17 is. All I am saying is that there is no evidence to support it.

Earl of Caithness: As a quick follow-up to that, even if we did that and decided it was right, would we have any influence if everything is being governed by America, who will not change their 13 year-old rule?

John Carr: Spain, specifically, said no to the American law, and they passed a law saying that they thought 14 was the right age. They did that about eight or nine years ago. The companies in Spain do honour that. By the way, they only honour it to the same extent that they honour it here—that is to say, they still do not check what your actual age is but you declare 14. In Holland, they have adopted 16, and, again, as far as I am aware, most of the internet companies at least nominally honour that age limit. We should be able to do better; we should be able to produce good research to show it, and, yes, I think within our own jurisdiction the companies would honour it.

Q23 Baroness Benjamin: I would like to declare my interests. I am the vice-president of Barnardo's. I often speak on behalf of the NSPCC and I am the vice-chair of the All-Party Parliamentary Group for Children's Media and the Arts. We have reported on children's online behaviour.

I have just come up with an idea. Instead of the blanket term of pornography, how about sexually abusive behaviour in imagery? It makes it quite different, because a lot of people enjoy watching it.

John Carr: That is certainly more accurate.

Baroness Benjamin: At least you know what you are dealing with. It is on the tin: you know what you are dealing with. In 2015, the NSPCC carried out a project in conjunction with Mumsnet to ask parents to view and rate the 60 most popular social media, games and apps that children use. They found that parents saw sexual content in 72% of the sites; bullying in 52% of the sites; and violence/hatred content in 52% of sites. Do you think there is enough guidance and advice available to parents, who often declare that they are ignorant about the internet, to enable them to educate and inform their children, or to protect their children from inappropriate content?

John Carr: There is no shortage of advice. I do not know how well it gets through to the intended audience. Will, you do more work in that space than me.

Will Gardner: There is a lot of information and advice. There is a challenge, absolutely, in keeping that up to date, and there is the work that you are talking about, which is the Net Aware work from the NSPCC, which is a really important piece of work. Ofcom found that 76% of parents of 5 to 15s said they know enough to help their children manage online risk. It is quite a big level of awareness, but that is still 24% who felt that they did not, and there is absolutely a need to do more there. We have learned over the years that we need to be working in this space. Schools are a really important avenue in this space. We know that parents' preferred source of information on this topic is schools, which is really important. We feel that being positive in relation to technology and not too scary, which can be quite disempowering for parents and can lead to an outcome that nobody is looking for, is another lesson that we have learned over the years. But we know this is going to be a continual thing that we need to focus on. Also, in the Ofcom study, 9% of parents of 3 and 4 year-olds said they felt their child knows more about technology and the internet than they do. There is going to be continual work to reassure and equip parents to take that parenting online as well as offline.

Baroness Benjamin: Do you think there should be some sort of public service broadcast that gives parents a message on this? There was the Green Cross Code advising them how to help their children cross the road. Do you think there should be some sort of pornography or sexually abusive behaviour imagery code to alert parents about the dangers?

Will Gardner: If you take it topic by topic, there is scope for doing that. If you want to focus on pornography or cyberbullying and address parents on that subject, there is scope, but online safety as a whole is too big to boil it down. We have had these conversations. We have wanted to try to develop these simple three things that you need to do, but it is more than three things. It will depend on the age of the child you are looking after as to what those things are. There is a real need for very simple messages. We do have big activities and campaigns that are current. We organise Safer Internet Day, which is in February every year, and we reach 20% of parents on the day, which we think is a good achievement for a one-day campaign. We also need to support schools to work in that space. There have been big public awareness campaigns before, and the UK Council for Child Internet Safety has those. "Zip it, Block it, Flag it" was the message that was put out on bus stops, and there have been other attempts to do that. My sense is that it has to be more sustained than that, and the budget is not there to provide that in a sustainable way. That is more likely to come through institutions that parents are continually relating to and interacting with.

Baroness Benjamin: Some parents put a block on certain computers at home, but I had a case where one parent did not do it on her work laptop and the child found it. There is that kind of ignorance with parents not realising the implications of doing it as broadly as possible. For children who do not have parents who care, that is the other problem we are dealing with.

John Carr: I remember "Clunk Click Every Trip". I will not mention the man who spearheaded it, now that I have brought that to mind, but never mind. I think a sustained public campaign, public health-type of approach, would benefit us greatly. The problem up to now is that the Government have not been willing to spend any money on this type of public education work. They have relied

entirely on the industry to do it. The industry has stepped up to a degree; there is no question about that. They have done very well; they have got something called Internet Matters, and Will and I are both on its board. But in relation to the total size of the problem and the challenge, it is nowhere near being enough, and it certainly does not match anything like you get in the public health field. So I would certainly welcome a shift in emphasis in that sort of way.

In respect of pornography, however, I think the answer is very simple. There should not be any in places where children go. We have never argued that pornography should not exist on the internet. That would be a stupid and illiberal thing to say, but we have said that pornography should not be accessible unless and until somebody has been able to prove that they are an adult—that is to say 18 or more. We have succeeded extremely well in doing that in the field of online gambling. We should and can do it in respect of pornography, and there is a Government Bill that will shortly be before your Lordships' House that will help in that regard, although it does have a fatal weakness, which perhaps we will come on to later.

Q24 Bishop of Chelmsford: It would be very good to hear more about that, but I want to take us on to something that has come up several times, which is the role of education and schools in all this. As you will be well aware, PSHE—personal, social, health and economic—education is a non-statutory subject on the school curriculum. What part do you think that could play in safeguarding children primarily in the digital environment and in teaching them and helping them to get the benefits from it, and should it be compulsory?

Will Gardner: We are part of the group that supported the move for PSHE to become statutory. We think that is a really important element. Sex and relationship education guidance has not been updated since the year 2000 formally, so there is a real need to do more in this area. The NSPCC study that just came out looking at the issue of pornography, where too many young people responded that they wanted to emulate some of the things they had seen in the online pornography they had come across, is a case in point. Young people need help to understand. If we are not able to protect them from seeing these messages, they need help in trying to interpret and understand what this actually is. I think that is a very compelling reason, but it is broader than issues around pornography and sex education. It is around peer pressure, body image and social media. Sexting and cyberbullying is all wrapped up in PSHE. At the moment we have the computing curriculum, which has e-safety education for key stages 1, 2, 3 and 4 that was introduced in September 2014. We would like to see statutory PSHE picking up on the behavioural elements of how we need to equip and support young people. PSHE is a brilliant way to do it, because, often, there is not a black and white answer or a right and wrong answer in relation to some of these discussions. There are shades within it. We need to try to help young people discuss and develop the correct norms of behaviour. I think the PSHE environment is a really good way of doing that.

Baroness Quin: I would like to follow up something you said before about some kind of public information or awareness push—some kind of campaign. In your view, who would lead this? There seem to be several government departments that have an interest, whether it is Education, Home Office, Culture, Media and Sport, or Health even. Has any thought been given to a government initiative

that matches the UK Council of Internet Safety that you were talking about before?

John Carr: If you speak to the police, which presumably you will be doing at some point, their view is that we have to start thinking about this whole area as we do public health-type issues. From the point of view of the police—obviously they will speak for themselves—they see this challenge as being on the same scale as and similar to other types of health-related issues that have occurred in the past. Was "Clunk Click" a public health issue or was it not? I guess it was and it was not. You said earlier that there is lots and lots of advice around for parents. It is reaching them that is the issue.

If we rely only on schools, we will fail. Why? Because for a great many parents, schools are not welcoming places that they feel comfortable going to or being part of. I did it for my own children at their school. I went and gave talks at parents' evenings and so on and so forth. In the room, there were lots of parents just like me. Lots of parents were not in the room, and it was probably their children who needed the help the most. Relying only on schools is doomed. That is why, again, I get back to the point about public health. Where do people go? They go to doctors' surgeries, supermarkets and hospitals; they go to a whole heap of places in which schools do not figure. Again, that is why I think a public health-type approach—a much bigger, broader-based thing—is required. It is beyond the resources of the industry to finance it. Industry, by the way, is too diffuse a term in any event. There are so many different individual players now in this space, which is why the obvious place would be for government to lead it, and health would be my first choice.

Baroness McIntosh of Hudnall: While absolutely taking the point that you cannot put all this onus on schools, and what we mean by schools is teachers, could I none the less ask this in relation to the possibilities that PSHE represents? First, what is your observation about the ability and the willingness of teachers to take on the responsibility for delivering an effective programme, and what is there out there to help them to get properly equipped? If we had PSHE as a standard part of the curriculum, they would be trained in it along with all the other millions of things they have to do, but they would be trained in it. For those who do not have that training, what is there to help them and encourage them to deliver that work effectively?

Will Gardner: The approach that we have taken from our organisation's perspective is to provide resources and to make them as easy as possible to use for teachers. Some of the topics that they would need to talk about in this context are very difficult things to talk about, such as sexting, involving sex and technology, which can be a daunting subject to bring up with a group of young people. We have to provide teachers with materials with which they feel confident and comfortable and hold their hands, if you like, to the point at which they can see exactly what they need to do. There has been a lot of work developing such material for teachers, which has been tested and is there. We have just developed a PSHE toolkit covering a number of these different issues and which we are waiting to launch and promote. There is a PSHE association that provides some accreditation for these resources, which can help them to do almost a quality control of some of the resources that are out there and to disseminate it to the teachers who need to have it. They have a great network of PSHE educators across the country.

Baroness McIntosh of Hudnall: Presumably, the take-up of that is effectively voluntary. The schools that do not choose to take it up do not have to. Is that the case?

Will Gardner: That is the case. By and large, if schools have a problem, our experience is that they will want to talk about it. If it is a sexting or cyberbullying issue, that has often been the driver for schools to want to talk about these things. The other big driver in the education system at the moment is Ofsted, which provides great leverage on school leadership to address e-safety from a policy and education perspective.

Q25 Baroness Kidron: It always seems that we go very quickly to parents and schools, looking for them to deal with the result of this rather than the cause. I want to go back to the technology itself. There is one part of this that is filtering and blocking. I have a very baseline question about how effective you think it is, but, perhaps more interestingly, what are your views on where industry is failing, where industry could flip the switch a bit and provide services? John, you have already mentioned that we could have age verification around sexually violent images. I would like you to talk a little about that.

John Carr: Facebook's pioneering slogan—the idea on which the company was founded—was "Move Fast and Break Things". It ties in with another idea, which is central to the whole idea of how the internet industry operates, which is permissionless innovation. The whole thing is about having a great idea, getting it out there and seeing how it goes. If we find out there is something wrong with it later, it is based on this idea that it is better to apologise than to ask permission in the first place. You get the product out there, see how it goes, and, if something goes wrong with it, you tweak it and change it if and when you have to.

I think that is wrong. I think we should try to establish, either through law or culturally, that any and every company has a duty of care to children if it brings out a new product or a new service, just as it does in the physical world. If you bring out a new iron, a new toaster, a new motor car or a new anything, there is a whole set of hoops that you have to go through to prove that it is fit and proper to be put in the marketplace in which you are about to put it. That does not apply in internet space. It should; there is no reason why it could not. By the way, Facebook has now abandoned, officially at any rate, that slogan of "Move Fast and Break Things", but the philosophy is still deeply embedded in the way internet businesses think. That idea of establishing a duty of care would be a very big step.

On filtering and blocking, the first key point to make about that is that within the United Kingdom, while it is true that all our big internet service providers provide free filtering tools on a voluntary basis, these only reach 90% of households; 10% of households are not covered by the big ISPs. What about the children in those households? There is a gap. Lady Howe has been bringing a Bill to your Lordships' House persistently for the last five or six years, which, had it been passed, would have closed that loop. It is a shame that it was not passed because it should be; 10% of the children of this country is too big a percentage to ignore. Filtering has a very important and valuable role to play. It is not sufficient, but it is certainly a very good start.

Will Gardner: I agree with John. We do not want to overpromise on what filtering can do. If we see it as a useful tool, probably its main benefits are in

relation to accidental exposure and for protecting younger children. You can see very clearly that that is something you would think parents would want to engage with and use. So it is a useful tool, but we must not overpromise and give people the idea that that is what they need to do.

We have the ISPs, and John spoke about the 90%. But there are the mobiles, which are all covered, and then there is the public wi-fi scheme, which was recently set up. From a UK perspective, we are leading in that area.

Over the years there has been an established good practice of what industry should be doing, covering a wide range of different industry providers. They cover some really very basic elements; for example, there must be clear safety information and advice on the service that people are using, and there must be clear, prominent and accessible safety tools that people know they can use to block and report and so on. This has been encapsulated originally in Home Office good practice guidance and now in UKCCIS good practice guidance. The challenge for is to try to make sure that that is spread out there right across industry. The bigger players are more engaged in this process, but often it is the smaller ones that are not. The process of technological development seems to be very rapid and very sudden. The people who seem most surprised by the success of the service seem to be the people developing it sometimes, and safety seems to be catching up in relation to the popularity of many services.

Baroness Kidron: Can I press you on this point? A great deal of what gets blocked is around the issue of content, and that is a large part of the concern. But you have expressed that what concerns kids is things such as bullying and so on, and some of the things that would make them safer are cultural things, such as not being on all the time, having time-outs or things not spreading along keywords that might be in the algorithm. I am pressing you again and asking you whether you think, in this fit and proper test, industry should have a little more pressure put on them about the cultural aspects. As they move fast and break things, they are breaking kids; it is not just things.

John Carr: Would I want Facebook to teach my children how to behave? I am not sure about that. Of course, to the extent that they can influence the way children behave, they should do it to the maximum degree, but I would not look to the industry for advice and guidance on a lot of these sorts of things. Many of them, particularly the smaller developers to which Will refers, will only act under pressure anyway.

The Chairman: Baroness Benjamin, I have a little queue here of people wanting to speak. Lord Sheikh wants to come in next and then Baroness Bonham-Carter, and then we will come to you.

Lord Sheikh: There is one issue that we have not talked about, which is racism. We have talked about bullying, grooming and sexual exploitation. Racism worries me. To what extent is racism a problem and, if so, how can we deal with this? The second point is regarding what happens at school. We have talked about cyberbullying. Could the child also be subject to verbal and physical bullying at school? Do they happen simultaneously? Does it occur like that?

John Carr: I am looking at Will's research on the very point, Lord Sheikh. I will defer to Will on that.

Will Gardner: We did a study on online hate and we found that young people's exposure to online hate included racist hate online. There is a significant percentage—24%—of young people who said that they had seen that.

Lord Sheikh: As high as that.

Will Gardner: They had seen that online. I am not saying it was directed at them, but they had seen it online. When we talk about cyberbullying, we are talking about a whole range of different bullying, including racist and homophobic bullying. That is all encompassed within that term. That has come to great prominence in our discussions among the UKCCIS community about the political discourse that we have just been through, the referendum result and the rise of racist and hateful incidents, and what we can do to support schools in relation to that, because there will be an online component to that.

Lord Sheikh: Do you think that has increased post-Brexit?

Will Gardner: For online I do not know; I do not know if there is data on that. I think the police are reporting a rise in reported incidents, and I think it is only natural to assume that that will take an online form as well.

Baroness Bonham-Carter of Yarnbury: We may possibly have moved on, but I was interested in what you said, John, about how the gambling industry had managed to hedge their world. I do not quite understand why that cannot be translated into—

John Carr: Well, there you are. The 2005 Gambling Act, as it became, went through with all-party support. It imposed an obligation on every online gambling website to institute an age-verification mechanism before you could place a bet or receive any winnings, and so on. It had to be compliant within the money laundering rules as well. We have never had the same in relation to pornography or, indeed, other adult content. The Metropolitan Police, for example, did an experiment on the sale of knives. They sent children under police supervision into shops to try to buy knives, and in something like 95% of the cases the child was unable to buy a knife because the shopkeeper saw the child, guessed that they were under 18 and would not sell it to them. Online, children succeeded in about 70% of cases in buying a knife. It is not just pornography where this has been an issue.

In the Digital Economy Bill, which had its First Reading in the other place last week, there are provisions that the Government have brought forward. I was a member of the working group that helped draft them, although they did not listen to every word of my advice, otherwise it would be better than it is. When the Bill reaches you, there is a proposal to introduce age verification specifically in relation to pornography sites, and it is an extremely good measure and very important, but it can be improved and I will happily explain why in a briefing note later.

Baroness Bonham-Carter of Yarnbury: What is the fatal flaw?

John Carr: The fatal flaw is that the new regulator will be required to notify banks and credit card companies where the non-compliant pornography sites are—that is to say the sites that are not introducing age verification—but there will be no obligation necessarily to block access to them. The assumption is that the banks and the credit card companies will withdraw their payments facilities,

and that will be a great incentive for the porn sites to introduce age verification, but there will be a category of pornography sites that will not do it. We are saying there needs to be a residual power in there to allow the regulator to say, as we do with child pornography and child abuse image websites, that that site must be blocked.

The Chairman: Are you talking only about where there is payment involved in those cases?

John Carr: Yes.

The Chairman: Is there not an awful lot of very unsuitable material that is entirely free that requires no interaction?

John Carr: All this material that we are talking about is free at the first point of access, and that is the point at which the age verification mechanism needs to kick in. But you have hit on a very good point. The Bill is not intended to catch every single publisher of pornography. It is only aimed at commercial pornography websites, but, by the way, they are massively the most important of the two. I know the NSPCC gave evidence to you in which they expressed a slightly different view. It would be wonderful if we could catch every single porn site. Some of them are absolutely tiny, little, insignificant things at one level. If we try to catch every tiddler in the pond, the big fish will swim away. I think we need to be more strategic and tactical. I agree with the Government's approach to that extent. We should go after the big commercial porn sites. If we can make that work, we can come back and revisit it, and find a way to deal with the other non-commercial, smaller ones and user-generated content, but if we try to do it all in one hit I am afraid we will fail.

Baroness Benjamin: I heard that the porn sites are making £2,000 per second. It is a big industry.

John Carr: There is a strong commercial incentive for some to comply, but some of them will not, so we need to have a residual power in the Bill—it is not there at the moment—to allow those sites to be blocked as if they involved child abuse or other forms of illegal content.

Baroness Benjamin: One of the criticisms often raised when you mention blocking, age verification and filtering is that people say that legitimate sites will be blocked, it is not fair and they do not want it for whatever reason. They want to watch porn and why should they not? If they did watch and they had to age-verify themselves or admit that they are watching, their bosses will know they are watching porn, and they do not want anybody to know that. That is one of the arguments. Do you think that filtering has become better developed so that not every single thing is blocked? Do you think it is better that we safeguard children and people switch on rather than having to switch off?

John Carr: The way filtering works at the moment with most of the ISPs—not all, by the way, and that might be something that you could look at, at some point—is that parents always have the option to turn off the filters or the filters might not work. The measure that the Government are bringing forward is nothing to do with how parents use filters in the home. This is about the responsibility of the people making money out of pornography; they have obligations as well. If a kid goes into a bar and asks for a pint of beer, you might

regret the fact that the parents were not around to stop them going into the bar in the first place, but it does not give the barkeeper a right to give the child a pint of beer. So it is with pornography. If parents for whatever reason turn off the filters, it still does not mean that the people making all this money out of pornography have a right to give it to five year-olds. We still need this separate and additional power in addition to the filters. They are not alternatives; they are complementary.

The Chairman: We are coming to the end of our time.

Baroness Benjamin: The point I wanted to make is that there are people who do not believe in filters.

John Carr: I once had to produce my passport not that long ago in a bar in America to prove I was over 21. It was mildly irritating and inconvenient.

The Chairman: You were flattered.

John Carr: Apparently they do it to everybody. It is mildly irritating and inconvenient, but I understand the social benefit and social gain behind it. It is true that some guys who are currently looking at porn without any restraints will probably have to go through a few hoops in future to do so. I am very sorry about that, but the greater benefit—the greater gain—is that we will be able to protect our children more effectively.

The Chairman: I am not going to come to you, Will, because we are running out of time, but you can pick up anything on that, if you would, in writing.

Earl of Caithness: You have answered most of what I was going to ask.

Baroness Benjamin: I asked his question. I am so sorry.

Q26 Earl of Caithness: Parliament produces legislation and regulation. Is the current regulation properly enforced, because there is no point in having it if it is not? Given the Digital Economy Bill, which is focused primarily on schools and age verification, have you any confidence that that will be enforced and make a difference? I have a third question, but I will wait to ask that so that you can answer those two first.

John Carr: As the Bill is currently drafted, no, I do not have confidence in it because, without a residual power to enforce the decisions of the regulator, I am afraid there will be sites that are able to get around it. If they are not subject to the jurisdiction of UK courts—and, overwhelmingly, these guys are in California, by the way, Uzbekistan and various places, and certainly not here—they can ignore a decision of the regulator because they cannot be brought to a British court. It is not an extraditable offence. We have to have a residual power to say, "Block access to the site". That is one thing. More generally, there is relatively little regulation in this space, as a matter of fact. Baroness Benjamin asked earlier about the filters. The fact is that we only know about the efficacy of the filtering regime that we have in this country because of voluntary declarations that the ISPs made to Ofcom. Ofcom simply asked them, "Are your filters working and how many of your customers are using them?" I am sure that each of the ISPs answered those questions truthfully, but Ofcom did not check; Ofcom did not verify the answers that it received because the Government did not ask

it to. The Government simply said, "Will you write and ask them what the current state of play is?" I think it would be much more in the public interest, and it would give lots more people confidence in that data, if there was some regulation or power to compel truthful answers, or for Ofcom to be able to inspect in some way what they were doing.

Will Gardner: Very briefly on a different note, it is over a year since we introduced revenge pornography legislation, which was intended for use in relation to adults, but one year on we have found that the legislation has been used in incidents in relation to children, and that is significant to find out because, from our understanding, that was not the intention of the legislation. When there are indecent images of children, there is a different piece of legislation—the Protection of Children Act—that should be used in relation to that. The first Act does not have the intent that is carried in the revenge pornography legislation. If this second revenge pornography legislation is being used in relation to cases with children, I would want to ensure that the subsequent other things that come along with sex offences, such as the sex offenders register and all that type of thing, are also included and are not seen as different things. I want to make sure that that is tied up. It was a surprise for us to see that cases involving children had used revenge pornography legislation.

On a different point around enforcement, on the issue of sexting, this is what we are discussing very much at a UKCCIS education group around the response of law enforcement to sexting incidents. What is the responsibility of schools to escalate to law enforcement, trying to make sure that that is done in a way that protects children? There is the development of a new code for law enforcement called Outcome 21. In order to prevent a case in which children had been sharing images with each other being passed on to law enforcement, it does not necessarily get tagged and recorded in a way that will reflect on DBS checks in the child's future life. Outcome 21 would help to protect children from that in the future.

Earl of Caithness: My follow-up question is: can a country act totally unilaterally in this area effectively? Given that these platforms are in America, Uzbekistan or wherever they have come from, can we as a country act effectively against those sites that you want stopped? Does it make any difference whether Britain is in or out of the EU as far as this whole subject is concerned?

John Carr: Before the European Union became energetically involved in this online child safety space, Britain was pretty much the only country within the European Union at the time that was doing anything at all. I used to meet with American companies and I would say, "This is what is happening to British children", and more or less routinely they would say things like, "How interesting. We are not hearing that from anywhere else. You cannot possibly expect us to change our policies or change our behaviour just because in one country—yours—you say things like this are happening". Of course, when the EU began to engage, we started meeting children's organisations and regulators from all over Europe, and found out that pretty much in every country the same sorts of things were happening to children. The American companies could not ignore the European Union because it has a gigantic amount of clout in the way that one single country simply does not. I voted to remain and it is very sad

from a number of points of view that we are not going to be there. That does not mean, though, that there is nothing that we will be able to do in future. That would be a counsel of despair. We are still a significant market; we are still a significant player. By the way, we are probably going to have to copy all the rules that the EU develops anyway. That is going to be true in many areas, not just this one.

The Chairman: We are wildly out of time. We will have to skip our final question, but would you like to wind up, Baroness Kidron?

Q27 Baroness Kidron: You both started saying that the biggest issue is bullying, but by the time we get to governance we always talk about sexting, pornography and so on. Do you not think that there is some space for regulation or legislation around reporting and response times, and upping the game for kids around the bullying piece, which is the bit that they are worried about?

John Carr: My short answer to that is that we should start thinking about the big online platforms in the same way as we think about public utilities. We should not simply take the word of Facebook or Google for it that they are behaving in exactly the right way in all circumstances at all times. There should be Ofnet or something that has some inspection powers and some ability to require them to open up their books. We have asked them time and time again, "How long does it take for you to deal with this type of complaint from a child?" "Oh, trust us. We are doing it", blah-blah-blah. It is not good enough and I think eventually we will get public accountability. Ofcom would be the obvious place otherwise, but maybe it needs a more specialised agency focusing solely on online space.

The Chairman: A final word, Will.

Will Gardner: It is a very important point, because with the social media environment we rely on users to make reports to remove content. That is currently the police in this environment, and we need to make sure we maintain users' trust in that system. We have argued for speedy response times. Tying people down to a response time is very tricky. The best we have obtained is some services saying, "We will do our best to respond in 48 or 24 hours". That is a big jump forward, because there have been instances in the past where people one month later say, "I am still waiting to hear", not knowing that their report has been reviewed and rejected, and they should be taking another course of action. It is much more empowering and we need to keep user confidence. Some of the issues of reporting are very different. If it is about IP, for example, legal teams will need to be involved and it is not really responsible to say, "We will get back to you within 48 hours", because that will not be the case. But there is a way of framing users' expectations that is a useful compromise with which industry can work. We have seen some do that. Also, I can single out Facebook because they have a dashboard for users making reports, where you can track your report and see what happens to it. Developing transparency around that reporting process is enormously empowering for young people to maintain confidence in that system. There is more we can do in that space, but I do not want to get so seduced by that as being the solution to the issue in its entirety, obviously. If we are relying on industry to solve cyberbullying, they have an important role to play, but clearly there is an offline element with which we need to be fully engaging.

The Chairman: Thank you very much. If there is anything else that you feel the Committee ought to know about, perhaps you would drop us an email later.

John Carr: I definitely will.

The Chairman: The fact that we have run way over time indicates, I think, our interest in what you had to say to us. Thank you both very much indeed. It was really helpful.

Children's Charities' Coalition on Internet Safety – written evidence (CHI0001)

1. The Digital Economy Bill is directed at larger commercial pornography sites, almost all of which are domiciled outside of the UK and therefore, for practical purposes, beyond the reach of UK courts and law enforcement. While nominally these sites are "free" in that they do not charge to look at the bulk of their wares they are nevertheless highly commercial in nature, collecting their income in other ways e.g. through direct sales and advertising.

   The Bill is most welcome but it has a fatal flaw. The Bill requires the sites to introduce age verification to prevent persons under the age of 18 from being able to look at their content. The assumption is that the credit card companies will threaten to withdraw payments facilities and the advertisers will threaten to withdraw advertising from non-compliant sites (which would be operating illegally) and this will be a sufficient incentive for most porn publishers either to comply or cease publishing into the UK. This is a reasonable assumption. The Bill will also create a Regulator with a power to compile a list of non-compliant sites. This list will be circulated to interested parties e.g. credit card companies and advertising agencies but neither are *obliged* to act although, as already noted, it is anticipated that most will. However, if a commercial pornography site uses no UK-based payments facilities and receives no advertising from UK sources, or it changes its business model to arrange things that way, it could continue to operate with impunity. Thus for persistently non-compliant sites the Bill should give the Regulator a residual power to require access to non-compliant sites to be blocked, in a manner similar to that which, de facto, already exists for child abuse images.

2. We need to start thinking about the major social media platforms in the same way as we do public utilities. Certainly in respect of children and young people the platforms' dominance in some areas means children and young people may feel they have little choice but to join and be part of the social milieu to which all or the great majority of their friends belong. It is unacceptable for there to be no way for the public to be reassured about the efficacy and appropriateness of these businesses' internal systems for dealing with complaints from or issues raised by children. An independent regulator (perhaps Ofcom) should have the legal power to compel at least the larger platforms to open their books and allow independent inspection and verification of their public-facing processes to ensure they are working satisfactorily.

3. The UK's system for providing filters to customers of the UK's "Big Four" domestic broadband providers is excellent but there appears to be significant variations in the levels of take up between the different ISPs. At first sight this seems strange because the demographics of their customer base do not look as if they are wildly different. In any event the claims the ISPs make about levels of take up have not been independently verified.

When the last (and so far only) checking exercise was carried out, Ofcom merely asked the ISPs to inform them of their take up levels. Ofcom sought neither to verify the claims the ISPs made nor to explain the reasons for any differences. This is not satisfactory. Moreover the current voluntary system for providing filters only extends to the customer base of the "Big Four". It seems they reach only 90% of households. Children in the other 10% deserve the same level of protection.

4. The system of filtering for mobile networks appears to be working satisfactorily but it has never been thoroughly inspected and verified by an independent agency.

5. Ditto in relation to "Friendly WiFi" i.e. the system where the providers of internet access via WiFi in public spaces take steps to limit access to adult content and illegal materials. A key question here would be to determine how extensively it is operating and perhaps also to identify any major enterprises or concerns that had not adopted "Friendly Wifi".

6. There has never been a proper, independent evaluation of the optimal age limits for using social media platforms. The single lower age limit of 13 is the product of a US Federal law which was passed in the 20th Century before social media platforms existed. With one or two exceptions e.g. Spain, the rest of the world acquiesced rather than sought to examine critically the appropriateness of that age standard. Perhaps we need more than one age level depending on the nature of the platform and the type of activity in question. In addition the absence of any obligation to verify the age of customers is leading to a huge level of non-compliance. This is not satisfactory.

7. A new law is required to allow victims of child sex abuse to claim compensation from persons found in possession of images of that abuse. The USA has a similar law specifically designed for this purpose. Aside from assisting with victim recovery it could also act as a major deterrent to a certain class of person who collects these images. The MoJ is currently considering this idea.

8. We ought to establish that the providers or suppliers of digital services have an unambiguous legal duty of care to consider the online child safety aspects of any and every service before it is released. One of Facebook's founding ideas was "Move fast and break things", otherwise expressed as, "it is easier to apologise after the event rather than seek permission before it". It is understood that this has now been formally renounced by Facebook yet it remains a dominant idea across the whole of the internet industry.

9. There are several notable weaknesses in internet governance institutions and processes: one is their failure to take proper account of the fact that children and young people are a very substantial constituency of users and that they have rights under international law which are routinely ignored. ICANN in particular has been woeful in several key regards. HMG has an important leadership role in this area.

10. Finding ways to help parents to help their children get the most out of the internet while remaining safe is a major and urgent societal challenge. We cannot blithely assume it is a problem which will solve itself with the passage of time. In this context schools have an important role to play but if we see them as the sole or principal route to parents we will fail because too many schools continue to be seen by too many parents as unwelcoming places. A public health sort of approach may therefore be worth considering as an additional or complementary strategy. What we are talking about, in essence, are the skills needed for 21st Century parenting. That repertoire of skills must now include a knowledge of how the internet fits into young people's lives and how best to support children and young people in the use of the technology.

19 July 2016

Children's Charities' Coalition on Internet Safety and Childnet International – oral evidence (QQ 1-10)

Transcript to be found under Childnet International

Children's Commissioner for England – written evidence (CHI0028)

1. Introduction

The Role of the Children's Commissioner:

- The Children's Commissioner has a statutory duty to promote and protect the rights of all children in England with special responsibility for the rights of children who are in or leaving care, living away from home or receiving social care services;

- Works with government and public bodies to improve policy and practice relating to the care system, and to ensure that children's voices are heard. This involves consistent and systematic consultation with young people in all aspects of the Children's Commissioner's work;

- Operates an advice, assistance and representation helpline for children who live away from home, including children in care.

2. Children online

For most children there is no longer a clear distinction between their online and offline lives. The amount of time children spend online has more than doubled, from 4.4 hours a week in 2005 to 11.1 hours in 2015 for 8-11 year olds and from 8 hours to 18.9 hours for 12-15 year olds.[100]

Whilst the online world has created incredible opportunities for young people to explore, experiment, socialise, create and educate themselves in ways which were previously undreamt of, it has also exposed children to the risk of harm, including from seeing extreme pornography and from sexting.

Protecting children from potential harm and educating them about both the physical and online worlds are shared responsibilities in which parents, carers and grandparents, governments, policy-makers and educators, and importantly, industry, all have vital roles to play.

3. Impact of pornography

This year, the Children's Commissioner, together with the NSPCC and Middlesex University examined how many children and young people are being exposed to online pornography and what impact it is having[101].

The findings of this research showed that where children were accessing pornography, it was just as likely to be viewed accidentally as deliberately and that children quickly become desensitised on subsequent viewing.

---

100 http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/children-parents-nov-15/childrens_parents_nov2015.pdf

101 https://www.childrenscommissioner.gov.uk/sites/default/files/publications/MDX%20NSPCC%20OCC%20pornography%20report%20June%202016.pdf

Who has seen online pornography?

- 28% of 11-12 year olds report having seen pornography which rises to 65% at age 15-16.
- Children were statistically as likely to stumble across pornography accidentally as to search for it deliberately.
- More boys view pornography by choice than girls.

Feelings and attitudes towards online pornography

- On first viewing pornography, young people report a mixture of emotions, including curiosity (41%), shock (27%), and confusion (24%).
- Shock and confusion quickly subsides on repeated viewing, whether it is deliberately sought out or accidentally viewed.
- 53% of boys reported pornography was realistic compared to 39% of girls.

Risks and harms

- 44% of boys compared to 29% of girls reported the pornography they viewed had given them ideas about emulating what they had seen.
- 21% of 11-12 year olds wanted to emulate what they had seen compared to 39% of 13-14 year olds and 42% of 15-16 year olds.
- 26% of those surveyed has been sent links to online pornography and 4% had sent others pornography.

'Sexting'

- None of the children in focus groups described sexting as taking and sharing self-generated photographs of naked bodies or body parts. Rather, they interpreted sexting as writing or sharing explicit or intimate words.
- Only 7% of the surveyed children reported sending naked or semi-naked photos of themselves onto others.
- Only some of those who were 15-16 knew how to remove intimate images of themselves from the internet via ChildLine and the IWF partnership.

Young people's views on intervention

- The participants called for the importance of more education about pornography delivered in a relevant and engaging way. Young people wanted to be able to find out about sex, relationships and pornography in ways that were safe and credible.

With smartphones overtaking laptops as the most popular device on which to access the internet[102], children and young people are almost always a few taps away from seeing potentially harmful and distressing material. It is clear, whether intentionally or not, that young people are viewing pornography and it is important that parents, carers, teachers, and government respond to that.

4. The Digital Taskforce

Last autumn, the Children's Commissioner set up a Digital Taskforce of policy, legal and technology experts, along with a group of young people, to explore children's experiences of growing up in an increasingly digital world.

102 http://media.ofcom.org.uk/news/2015/cmr-uk-2015/

Children are now offered unlimited opportunities to participate, create and socialise and it is important that every child has access to that potential. The Commissioner however intends to ensure that the same protections that apply to children online also apply to them offline and that digital platforms and service providers are doing all they can to protect these rights.

This Taskforce will have three major outputs and will be reporting in early 2017. First, we will write a General Comment to be submitted to the United Nations Committee on the Rights of the Child. The Convention on the Rights of the Child was ratified at a time when the internet was still in its infancy and consequently, there are currently no digital-age specific interpretations of each article despite this now being an integral part of a child's life. The Committee acknowledges this gap.

A General Comment therefore is an essential and timely contribution. It will provide a clear interpretation of the existing rights structure with regard to how it applies to the digital environment. This Comment is being drafted in collaboration with Dr Sonia Livingstone and in consultation with the UN Committee and international interested parties.

Secondly, the Commissioner's Taskforce is also exploring how children's rights are currently understood and incorporated by the providers and platforms they use. Through discussions with the major internet service providers, social media and telecommunication companies as well as others, the Commissioner will map how the industry views children's rights and where this is reflected in the design and delivery of their products and services. This will go further than establishing how well children and young people are protected from harmful content and contact online but will establish who takes a broader understanding of children's rights, and how this is done effectively.

This will culminate in a map of how well industry engages with a child's right to be heard and informed as well as how well they are protected. In doing this, the Commissioner intends to highlight best practice as well as the gaps in current attitudes and provision.

Finally, the Commissioner will look to launch unique digital content, in collaboration with the Children's BBC. This content will help children and young people to better understand their rights in a digital context and what this means with regard to the apps and websites they sign up to and use every day.

5. Parenting Expert Group

Alongside the Digital Taskforce, the Commissioner has also convened a Parenting Expert Group to provide advice to parents to help them navigate their children's increasingly complex digital lives. Experts from Mumsnet, Parent Gym and the Tavistock and Portman NHS Foundation Trust will look at how parents can best support their children to make the most of the opportunities offered by digital engagement whilst ensuring they stay safe and healthy.

The Commissioner has heard from parents that they struggle to keep up with children's digital activities with increasing worries about the impact of digital

time on their wellbeing. Whilst most parents understand the benefits that the digital world can bring, they can often feel at a loss of how to offer guidance and ensure that children can be supported to 'switch off' when necessary.

The Group hopes to report their key findings and advice in February 2017.

August 2016

Children’s Media Foundation – written evidence (CHI0027)

SUMMARY

The Children's Media Foundation is a not-for-profit organisation dedicated to ensuring UK kids have the best possible media choices, on all platforms and at all ages. We bring together academic research institutions, the children's media industries, regulators, politicians and concerned individuals who recognise that media is not only a powerful force in children's lives, but a valuable one. This submission has drafted by our non-exec advisory team who comprise industry leaders from the children’s digital sector, ex-BBC executives and representatives from the tech-start up community.

Traditionally in the children’s TV media industry there has been a 3-way relationship between broadcasters, parents and children about what constitutes child-appropriate content and when and how it can be accessed.

This manifested itself as discreet programming blocks on the mainstream TV channels or dedicated children’s channels in multichannel homes. Television outside these walled-gardens was widely understood to be designed primarily for grown-ups but, before the watershed, still had to take account of children who might be watching.

However, the always-on nature of the internet, the rise of on-demand services, the advent of new distribution platforms, the dominance of certain search tools for 90%+ of all discovery, the shift from ‘push’ broadcast delivery mechanics to individualised ‘pull’ services, and personal device ownership have changed all that - forever.

These developments, are not by themselves inherently bad for our children. And as with previous generations, when grown adults adapt and embrace the new opportunities offered by the changing technology, so children naturally want to emulate these behaviours. The rapid speed of recent digital developments has meant that many scenarios we could never previously imagine are now possible, and we need to adapt our interventions to suit.

In addition to the response to the individual questions below we argue that the UK needs

i. A means to bench-mark and clearly flag age-appropriate content to help parents and children make informed decisions.

ii. Any public health recommendations about appropriate levels of screen-time must be based on evidence

iii. Clear rules about what age verification is required for non-children’s content with an emphasis on the platforms to demonstrate that users are the age they say they are

iv. Definitions about what content and services are appropriate with the right parental permission with clear guidelines about how to collect and verify parental consent

v. Clearer demarcation of ads in search results

vi. Much more effective child-specific search tools (not hidden at the bottom of a page)

vii. Tighter regulation on automated links that lead children out of these safe havens

viii. Commitment not to mine children's data or target or manipulate children based on their online activity - particularly regarding marketing and advertising

ix. Rules against behavioral mechanics that try to draw children into addictive behaviours or exhortation.

x. Commitment to make UK specific children's content visible in the first page of search or app store results.

INTRODUCTION

(1) The Children's Media Foundation is a not-for-profit organisation dedicated to ensuring UK kids have the best possible media choices, on all platforms and at all ages. We bring together academic research institutions, the children's media industries, regulators, politicians and concerned individuals who recognise that media is not only a powerful force in children's lives, but a valuable one. This submission has drafted by our non-exec advisory team who comprise industry leaders from the children's digital sector, ex-BBC executives and representatives from the tech-start up community.

(2) Traditionally in the children's TV media industry there has been a 3-way relationship between broadcasters, parents and children about what constitutes child-appropriate content and when and how it can be accessed.

(3) This manifested itself as discreet programming blocks on the mainstream TV channels and more latterly dedicated children's channels in multichannel homes. The presence of these blocks/channels represented a 'safe space' where parents knew they could leave their children unmediated to enjoy and learn from a variety of imported and home-grown production.

(4) Television outside these walled-gardens was widely understood to be designed primarily for grown-ups but, before the watershed, still had to take account of children who might be watching with or without their parents up until 9pm.

(5) (Cinemas and book shops followed a similar model for films and publications with discreet times and labelling for those shows that were best suited for young children, pre-teens and adolescents)

(6) However, the always-on nature of the internet, the rise of on-demand services, the advent of new distribution platforms, the dominance of certain search tools for 90%+ of all discovery, the shift from 'push' broadcast delivery mechanics to individualised 'pull' services, and

personal device ownership have changed all that - forever.

(7) These developments, are not by themselves inherently bad for our children. And as with previous generations, when grown adults adapt and embrace the new opportunities offered by the changing technology, so children naturally want to emulate these behaviours.

(8) However, we have to appreciate that internet does not offer the same safeguards to minors that was common with more traditional media services (which were limited by spectrum and came with in-built limitations). The rapid speed of recent digital developments has meant that many scenarios we could never previously imagine are now possible, and we need to adapt our interventions to suit.

(9) To date, the main focus of industry efforts on safe-guarding children has been levelled at better parental information. This is partially because of a lack of consensus about how to address the issues, but also because of lobbying from the main industry players that they are merely proving the 'pipes' for content providers and therefore not responsible for any digressions.

(10) In our opinion, this approach is not sufficient. And we would like to see the new distributors, gatekeepers and search providers make a 21st contract with parents and children that they will in future put the needs of children first and foremost, ahead of advertisers, data-miners and brands who all have a vested interest in the manipulate or influence of younger audiences for commercial gain.

(11) That is not to say that commercial organisations have no place alongside children's services, but where children naturally congregate online, there needs to be much more transparency about the potential risks they face in that environment with a commitment to building new tools to prevent those problems arising.

(12) We would also argue that any online platform that benefits from a sizeable children's audience (a potential threshold could be 1% of the under 13s audience - approximately 91,000 junior users per annum) or their own user base comprises over 5% of under 13s, then that platform would be legally obliged to have a clearly published children's policy stating the safety provision they have in place.

(13) At the outset, we think it's important to emphasise that 'children', and their relationship with digital media are not a single group. In broad terms:

(14) Access by very young children is MEDIATED. Essentially, parents choose a channel, and the child watches. This is the main model for pre-schoolers. The development stage of this age group tends to mean that their use of digital technology is focused on specific characters and brands through apps and games. Social media is not widely used, although young children often use You Tube to watch videos. VOD platforms such as Amazon and Netflix are important too.

(15) As a child gets older and moves towards school age (6-12), traditionally their access is MANAGED: A social contract exists between children, parents and wider society to try and protect them from unsuitable content. The 9pm watershed is an example. Digital is changing this: the prevalence of mobile devices means children become increasingly autonomous in their media consumption. While most 6 year olds will focus on apps, games and You Tube, as they get older they use social platforms such as WhatsApp and Instagram and routinely share media and content.

(16) By the time a child reaches their teenage years, it's natural for them to start experimenting and exploring. Most parents will try and MONITOR their child's use. But this is increasingly difficult as platforms evolve, and children constantly search for the next thing to play with and use.

(17) While this offers a useful starting point, the digital world is much more porous than old media, and the ages and thresholds are getting younger and younger. This raises some consistent issues:

- Parents do not have the tools or experience to understand and help their children navigate the digital world.
- Industry does not share a consistent, collective responsibility to provide safe environments for children.
- Children are gaining access to devices at a much earlier age – creating new challenges for providing age appropriate media literacy education
- The on demand nature of the technology means traditional parameters such as the watershed are irrelevant. Content is available any time, any place and anywhere.

(18) Parents and carers clearly have a role to play in protecting children online. However, the CMF maintains that parents cannot be expected to do this alone. Digital platforms and content providers must assume some responsibility too.

RULES AND BENEFITS

1. What risks and benefits does increase internet usage present to children, with particular regard to:

i. Social development and wellbeing
ii. Neurological, cognitive and emotional development,
iii. Data security.

(19) There have been concerns around screen time since the dawn of television. The same applies for digital devices. However, the benefits of interactive and touch screen technologies are huge for both adults and children.

(20) The interactive nature of the media including personalized feedback, gesture/touch based interfaces and spatial navigation are a natural

way of interacting for children and provide an engagement that traditional media cannot challenge.

(21) Multiple studies from respected institutions such as Joan Gantz Cooney Center and Sesame Foundation have pointed to the benefits to children of appropriate digital platforms and content. Better hand eye coordination, dynamic spatial skills, improved language skills, self-discovery, and greater understanding the world around them are a few of the positives. Accessing content on the internet – just like reading – is extremely empowering.

(22) The oft-quoted health risks to children – such as attention deficit, imitative violence are by no means unique to the internet. That does not mean they should be dismissed, but the hazards and approach to tackle them must be kept in perspective.

(23) The CMF considers the benefits of well-made appropriate content are clear. The risks come from unmediated access and discovery of inappropriate content and/or inappropriate communication. The problem is that in the digital space, there is little delineation between experiences intended for children and experiences produced for a general audience that may not be appropriate for young people.

(24) There is no doubt that parents need to be helped to play a bigger part in their children's media literacy and media use. However, in our view the efforts to help adults understand their children's digital lives are disjointed and piecemeal and therefore ineffective. So much of the advice is general, and therefore irrelevant to parents at their time of need, when confronting specific problems.

(25) The oral evidence to the committee suggests thinking of media literacy as a public health matter tackled (for instance) by providing resources at shops and in health centres. While this would a useful approach, we consider that more focus needs to be placed on the ease or discoverability and the relevance of this type of material for parents. This content needs to be compelling, searchable, relevant and shareable via digital platforms too.

(26) In our view, one of the major issues in this area is data protection. A recent piece of research by VARN (varn.co.uk) found that 55% of adults are unable to tell whether search results are real or paid adverts. If this is true for adults, it is unrealistic to expect that children can make sensible choices around the use of their data by media platforms.

(27) While digital industry follows the letter of the law, they should be encouraged to think about the intention of the law too. When it comes to data, children need to be protected. They should have the right to be forgotten – and the media industry needs to do more to make that easily achievable.

2. Which platforms and sites are most popular among children and how do young people use them? Many of the online services used by children are not specifically designed for children. What problems does this present?

(28) The CMF actively supports and collaborates in research into children's media consumption and media literacy.

(29) The platforms used by children vary according to their age and developmental stage. Factors affecting the popularity of services can include immediacy of content, social engagement, cost and novelty.

(30) You Tube, the Apple App store and Google are universally popular and dominant for all ages from preschool to teens, along with games such as Pokemon Go.

(31) Preschool children tend to rely on apps to consume games and content. However, they default to You Tube and Amazon (in preference to Google) when searching for information and entertainment.

(32) Primary age children's choices develop as they mature. Younger children in this group use apps, and increasingly game platforms such as Minecraft, Friv and Girls Go Games. Older children often have phones and are socially aware. WhatsApp and Instagram are widely used.

(33) In addition to WhatsApp and Instagram, teenagers use Snapchat and Tumblr. But they are agnostic and will always be searching for the next thing that meets their needs.

(34) The market dominance of a few digital platforms is shapes society's perspective and unfortunately masks whether enough is being done to protect children.

(35) All the main social media platforms require users to be over 13, but very few actively police it. Many digital platforms have an ambivalent attitude to whether or not they support children's access. Spotify, for instance, promotes a 'Family Subscription' implicitly inviting parents to add their children, and therefore with parental consent inherently built in. However, after payment is taken, the only way to register a child is to ensure Spotify 'thinks' the child is over 13 – potentially encouraging an adult to become complicit in lying about a child's age.

(36) You Tube is now the ubiquitous video distribution platform, especially for children. While under 13's cannot create an account, the platform works with broadcasters to carry and promote huge volumes of content for children. However - search YouTube for "Lindsey Russell" – a Blue Peter presenter and great female role model – and the second clip is tagged 'Leather Mini Skirt and Black Tights' with denigrating comments and expletives about Lindsey and her appearance. Search

for the cartoon character Shrek, and not far away are series of hard core animated porn videos featuring the green ogre.

(37) There are filters on You Tube: many inappropriate videos are not available in 'Restricted' mode. But by default, this is switched off. Nor do they apply is a user is not signed in. By default, children do not generally sign in!

3. What are the technical challenges for introducing greater controls on internet usage by children?

(38) Without a central record of identities (a controversial thought in itself), it is easy to lie, and extremely tough to verify whether a user logging in to a digital service is who they say they are

(39) Most people dislike passwords, so most platforms such as Google help by keeping a user persistently signed in once they've logged in. If a child is using their parent's device, the likelihood is they will have unrestricted access to content.

(40) The CMF maintains there needs to be a standard that ensures consistent best practice and expectations across the industry. However, there is no real motivation from the industry to tackle this problem.

4. What are the potential future harms and benefits to children from emerging technology, such as Artificial Intelligence, Machine Learning and the Internet of Things

(41) Futurologist Alan Kay once remarked that 'Technology is anything invented before you were born'. It's scary – and scares around technology are common place and alarmist. In recent months we have heard about Barbie Doll's talking to users and the Talking Tom app recording conversations to share with hackers. None of these are true.

(42) Many of the benefits and hazards do not concern the innate technology, but rather the way it is used. This applied to content and services for adults as well as children. However, as new technologies emerge, it is vital that risks and benefits are properly researched.

(43) Work is already underway to look at VR and potential physical effects such as eye strain as well as possible mental effects. However, the potential for negative impact has to be considered in tandem with the benefits: when well implemented, VR has fantastic potential as a tool for learning and entertainment.

(44) The internet of things posed new risks. As more and more devices become 'connected', and more and more businesses collect data, there is the potential for data protection standards to degrade as a result of hacks, mishaps or simple complacency. If this were to

happen, it could have important implications for children as well as adults.

EDUCATION

5. What roles can schools play in educating and supporting children in relation to the internet? What guidance is provided about the internet to schools and teachers? Is guidance consistently adopted and are there any gaps?

(45) Educating children in online safety and digital media literacy is an Ofsted requirement. In our experience, schools work hard to meet their obligations and reflect the guidance from Ofsted and third parties organisations such as the NSPCC et al.

(46) Secondary schools in particular work hard to help children learn and deal with issues around digital platforms.

(47) However much of the guidance is based on the dated assumption that it is teenagers who are using digital services and therefore most at risk and in most need of education and support.

(48) The CMF is concerned as younger children have increasingly autonomous access to platforms and content, we must ensure that education for children and their parents at primary or even infant stages reflects these cultural changes.

6. Who currently informs parents of risks? What is the role for commercial organisations to teach e-safety to parents? How could parents be better informed about risks?

(49) Some parents have an introduction at an early age while their children are at primary school, but provision is poor. We worry that the most consistent source of information is the tabloid press. However, while tabloid stories have a wide reach, unfortunately the information they contain is often ill considered or inaccurate.

(50) In digital jargon, media literacy itself needs to be treated as a product that best serves its audience. While we recognize that many organisations endeavor to provide useful information and guidance for parents, our assessment is that this content is often too generalized to be useful. Nor is it presented in a way that is easily discoverable the time of need. Parents, carers and teachers need guidance they can find easily, and that helps them address their specific concerns.

(51) Industry can and must do more. One approach may be to collect a levy from the major platforms to help fund a coherent media literacy strategy. However, a useful step would be to ensure that terms and conditions are presented much more clearly and succinctly so they can be properly understood by users – parents and children.

GOVERNANCE

7. What are the challenges for media companies in providing services that take account of children? How do content providers differentiate their services for children, for example in respect of design?

(52) When considering digital services, it is important to be clear on definitions:

(53) On one extreme there are the platforms such as You Tube or Instagram. These provide a publishing platform and tend to aggregate and distribute rather than creating content. While platforms are often popular with children as well as adults, the specific needs of children are rarely considered – which means inappropriate content is easily found or discovered inadvertently.

(54) On the other extreme are the producers who create content. The production of children's media tends to be vocational. As a consequence, content produced specifically for children has tended to be well balanced around risk and benefit. A mutual trust has existed between content creators, publishers and parents that producers will do the best they can for children.

(55) Many of the CMF's members who work in the children's digital sector believe that the same ethos should apply to digital space. However, it's clear that the status quo which based on self-regulation is not adequate to ensure this is maintained.

8. What voluntary measures have already been put in place by providers of content to protect children? Are these sufficient? If not, what more could be done? Are company guidelines about child safety and rights accessible to parents and other users?

(56) It's important to recognize that there is no substantive regulation in the UK that specifically protects children's rights online. Therefore, all measures are voluntary

(57) The BBC are the standard bearers in this space. Over the years they have developed mutual trust with parents and children around TV that has evolved to encompass their digital platforms. The guidelines and policies are easily available online and frequently updated to reflect new issues and societal changes.

(58) The commercial sector is more of a mixed bag. Some organisations such as Popjam have worked hard to ensure their platforms are safe for children. Bigger American players, such as You Tube and Facebook/Instagram tend to expect parents to take responsibility for children's access to content.

(59) While these companies clearly meet their legal and regulatory obligations, and their policies are available to parents on their websites. In practice, these documents are hard to find, rarely read by parents who therefore fail to understand the measures they could take to look after their children.

LEGISLATION AND REGULATION

9. What are the regulatory frameworks in different media? Is current legislation adequate in the area of child protection online? Is the law routinely enforced across different media? What, if any, are the gaps? What impact does the legislation and regulation have on the way children and young people experience and use the internet? Should there be a more consistent approach?

(60) Broadcast is essentially regulated and policed by Ofcom and ATVOD. The ASA is responsible for administering and self-regulating how ads are used in a child's context. Pure digital platforms are not covered by either of these.

(61) The most common regulatory framework in digital space is the US Child Online Protection and Privacy Act (COPPA). In the CMF's opinion, while this is the best regulatory framework available, it has been designed for American rather than British children and is not flexible enough to keep up with changing landscape. For instance, COPPA guidance suggests that the favored route to obtain parental consent is by fax! It is simply not fit for purpose.

(62) COPPA allows the predominantly US platforms to side step any societal responsibility to protecting children. The platforms claim they are merely the pipes for delivering content, with no responsibility for the content itself. They can therefore do the minimum to stay within national rules

(63) While there is an EU directive in process – it's primarily designed to address content plurality and reflect indigenous culture.

(64) In the UK, the Information Commissioners office is responsible for policing best practice about data protection and children. However, the ICO is really a passive organization. Potentially unsafe practices are unlikely to be addressed unless there is a problem.

(65) The CMF considers that there are currently three issues around regulation:

i - Many major digital businesses popular with children fall outside UK jurisdiction

ii - The regulations we are forced to use to safeguard British children has not been designed with needs of British children in mind. While we would expect some European countries such as France to strictly

legislate, the UK's approach is to let the market self-regulate. So far this has not been successful, and we have no reason to consider that the situation will improve in future.

iii - The wheels of technology move at a much faster rate than the cogs of the legal system. Legislation needs to be flexible to accommodate new challenges – and the industry needs to interpret the intention of guidance as well as the specifics.

(66) When services are developed or launched, we would like children to be considered by default. It is much easier to create a safe environment for kids and then unshackle it for adults, than to try and retrospectively react to make something child friendly

10. What challenges face the development and application of effective legislation? In particular, in relation to the use of national laws in an international/cross-national context and the constantly changing nature and availability of internet sites and digital technologies? To what extent can legislation anticipate and manage future risks?

(67) The internet is designed to be distributed and not limited by national borders, therefore legislation needs to be developed collaboratively with other countries.

(68) UK regulators need to have 'teeth' to ensure that regulation can be enforced.

(69) However, it is also important to ensure that future innovation is not inadvertently stifled.

(70) Platforms, distributors and content makers need to take a clear and accessible position regarding the provision of services for children, including explicit information about how data is collected and used, and targeted advertising applied. This could mean three levels:

i – Appropriate for Children (default)
ii – Not appropriate for children
iii – Approriate with parental consent

11. Does the upcoming General Data Protection Regulation take sufficient account of the needs of children? As the UK leaves the EU, what provisions of the Regulation or other Directives should it seek to retain, or continue to implement, with specific regard to children? Should any other legislation should be introduced?

(71) The CMF is not convinced the new regulation will adequately address the needs of children.

(72) Within the framework of the regulation there is too much uncertainty about when children are responsible for their own data, nor does it lay down clear guidance on when and how children's data can be collected. A right to be forgotten should also be included, with an expectation on platform owners that it needs to be easy and quick to enact – and its implementation should be clearly evidenced

(73) The CMF considers that any platform widely used by children should have an accessible, clear children's policy

12. What more could be done by the Government? Could there be a more joined-up approach involving the collaboration of the Government with research, civil society and commerce?

(74) Previous evidence heard by the committee suggested that digital literacy should be treated as a public health matter – encompassing parents, platforms, producers and regulators

(75) The CMF agrees that the government has a clear role in facilitating a clearer conversation and proper guidance on the expectations and best practice for ensuring children are safe.

August 2016

The Children’s Society – written evidence (CHI0004)

About The Children’s Society

The Children’s Society is a leading charity committed to improving the lives of thousands of children and young people every year. We work across the country with the most disadvantaged children through our specialist services. Our direct work with vulnerable groups including missing children, children with experiences of sexual exploitation, children in or leaving care, refugee, and migrant and trafficked children, means that we can place the voices of children at the centre of our work.

Introduction and key messages

The Children’s Society welcomes the inquiry into children and the internet to review the benefits and risks the internet poses to children and young people.

We recognise that the internet is increasingly a part of children and young people’s daily lives. Most young people use the internet positively to learn and connect but at any given time they can be exposed to an array of inappropriate content and networking sites that place them at risk. Children and young people should be empowered to make use of the internet in a positive way. This starts with education about how to avoid risky interactions online and where to seek help. Parents and carers also need to be supported and trained on how best to empower and protect their children online.

The Children’s Society forms part of the Children’s Charities' Coalition on Internet Safety (CHIS) which looks to use the knowledge and power of a number of UK charities to ensure best practice and strong policies to safeguard children when using the internet. We therefore endorse the submission and contributions made by the coalition to this inquiry.
We have chosen to respond to only those questions where we can offer the committee evidence and insight based on our recent research and direct practice. We have developed the following recommendations to help young people access the internet safely:

Our key recommendations:

- The role of sex and relationships education. We believe that schools can play a vital role in promoting online safety as part of personal, social, health and economic education (PSHE) alongside education about consent, exploitation grooming and healthy relationships in general. To ensure a consistent approach is taken, we have been calling for PSHE to become a statutory part of the curriculum in all schools.
- Education on sexting. Young people should be educated about the risk of being groomed for sexual exploitation as a result of sexting, about the images remaining in circulation even after children change their mind about sharing the image and about the legal implications of sexting.
- Guidance for schools on how to recognise and respond to sexual online behaviours. The revised and forthcoming statutory guidance on Keeping Children Safe in Schools should outline the training requirement of staff in schools in keeping children and young people safe online. The guidance should also include a requirement for safeguarding leads to receive regular training on online safety.
- Robust age verification for online pornography. The Digital Economy Bill 2016-17 presents an important opportunity to further enhance protections for children and prevent them from accessing pornography from both commercially regulated and non-regulated digital channels.
- Age ratings for music videos. The government should explore the effectiveness of introducing a universal age rating on music videos, including those that are produced abroad.
- A national campaign aimed at children and parents. As concerns continue to grow around the safety of children and young people online, we believe a national campaign should be developed to promote the positive and safe use of the internet and to educate children, their families and the public about the risks accessing the internet can pose for children.

1) RISKS AND BENEFITS

What risks and benefits does increased internet usage present to children, with particular regard to: (i) Social development and wellbeing (ii) Neurological, cognitive and emotional development (iii) Data security?

The benefits

1.1. The links between internet usage and children's subjective well-being

Our Good Childhood Report 2014 showed that there were links between various activities that children took part in, including internet usage, and their subjective

well-being[103]. The findings in the report showed that children who use computers and the internet less have lower levels of well-being than those who reported using the internet most days or on a regular basis. This is illustrated by Figure 1 below.

Our analysis suggests that children who never use the internet outside school have much lower well-being than children who did so regularly.

Figure 1. Frequency of using the internet (not at school), and low well-being

Source: Millennium Cohort Study, 2011. Age: around 11 years old. Scope: UK. Sample size: 13,469.

1.2. *Children's use of social networking websites and well-being*

In relation to using social networking sites on the internet, children who never did this activity had the highest levels of well-being, although the association was relatively weak[104]. It should be noted here that there are recommended lower age limits for the use of some social networking sites which are higher than the age group covered in the Millennium Cohort Study (MCS), around 11 years old at the time of our research[105]. In fact, perhaps reflecting this, over half of children in the MCS said that they never visited social networking sites even though 86% said that they used the internet outside school at least once a week or more[106].

The risks:

1.3. Online grooming

103 The Children's Society (2014) The Good Childhood Report 2014. http://www.childrenssociety.org.uk/what-we-do/research/well-being-1/good-childhood-report-2014

104 Ibid, Page 35.

105 Minimum age restrictions for most social media platforms currently vary between anywhere between 13 and 18 years old.

106 Ibid.

Through our direct practice with young people at risk or experiencing Child Sexual Exploitation (CSE), our practitioners are increasingly reporting cases of children and young people who are being groomed online via social networking sites for sexual exploitation. It is easier for sexual predators to groom teenagers online as it is faster, they remain anonymous and teenagers are more likely to trust an online 'friend' more quickly than one they meet face-to-face. This is illustrated by Marnie's story below.

Marnie's story [107]
'Before I got referred to The Children's Society there was a lot of things going on. I found it hard to make friends, I felt like I wasn't accepted. I didn't feel confident and didn't feel myself. I just felt really lonely, like I was torn in different pieces and I couldn't find myself.

'I found it more easy talking through the internet. I used to have five dating apps that were for over 21 year olds. It made me feel accepted, not so lonely. But I didn't take into consideration the grooming process, I didn't know anything about that. I thought when people text, it was just normal chatting.'

1.4. Online sexual bullying

The internet and social media sites have provided a new channel for people to bully children and young people, including bullying of a sexual nature. Our previous research revealed the profound impact bullying can have on children's lives, with children in England who were frequently bullied being six times more likely to have low well-being than children who have never[108].

Through our work in schools, we have seen increased cases of children affected by or engaging in peer on peer sexually bullying. This can include the making and sharing of indecent imagery or videos and circulation amongst peers for the purpose of humiliating the victim. Not only are these incidents taking place on school grounds but they are also increasingly occurring during and after school via digital and social media platforms and communities.

Given these concerns, we feel that it is crucial to explore interventions that can be taken to improve children and young people's experience in education. This includes emotional support to help young people overcome their experiences of online bullying, including sexual bullying.

***Recommendation**: The Government should introduce a legally binding entitlement for children and young people to be able to access mental health and well-being support in educational settings in England and Wales. This must include sufficient funding.*

---

107 Marnie is a secondary school-aged girl. She was referred to The Children's Society to help her overcome her experience of child sexual exploitation. Marnie's story is written in first person.

108 The Children's Society. 2015. The Good Childhood Report 2015.

1.5. Pressures to take and share explicit pictures and to share indecent imagery and videos

Concerns have been raised about young people's increased access to online sexual imagery and content as well as the making and sharing of imagery and videos themselves. However as Moultrie[109] explains it can be difficult to establish who commits these offences as those who sexually harm online do not always fit with those whom are known to child care and youth justice professionals.

In some instances, and as our research shows, the pressure to take and send explicit images comes from contacts young people meet online[110]. Our Seriously Awkward report[111] revealed the pressures young people face to send sexually explicit pictures of themselves online. We found that around 6% of 16 and 17 year olds reported feeling under pressure to take and send explicit pictures of themselves and around 10% reported that they do it.

1.6. Inappropriate and harmful sexualised content

The impact of viewing sexualised content including pornography on children and its influence on their opinions on sexual relationships is worrying. We are committed to ensuring that children are protected from materials that they may find distressing and which could negatively impact on their emotional and social growth.

Research demonstrates that young people under 18 are still in the stages of cognitive development and several studies have shown that early exposure to porn can have a profound impact on their sexual behaviours including addiction to sex and being more likely to sexually harass others[112.] This is of grave concern particularly in an environment when findings have shown sex and relationship education (SRE) to be of inconsistent quality and requiring improvement. It is vital that young people learn about the dangers and risks involved in partaking in sexual activity including learning about related issues such as sexual health and consent. This is particularly important when we consider that young women aged between 16 and 19 are at the highest risk of reporting having been a victim of a sexual offence (8.2 per cent)[113].

1.7. Young people with learning disabilities

Our recent joint report[114], *Unprotected*, *overprotected*, reveals that children with learning disabilities are more vulnerable to sexual exploitation than other

---

109 Moultrie D (2006) 'Adolescents Convicted of Possession of Abuse Images of Children: A new type of adolescent sex offender?' Journal of Sexual Aggression 12 (2) 165-174.

110 The Children's Society. 2015. Seriously Awkward report: http://www.childrenssociety.org.uk/what-we-do/resources-and-publications/seriously-awkward-how-vulnerable-16-and-17-year-olds-are

111 Ibid.

112 Office of the Children's Commissioner. 2013. Basically…porn is everywhere.

113 The Children's Society. 2015. Seriously Awkward: How vulnerable 16–17 year olds are falling through the cracks.

114 The report, which was commissioned by Comic Relief, and undertaken by Barnardo's, The Children's Society, British Institute of Learning Disabilities (BILD), Paradigm Research and Coventry University.

children, facing additional barriers to their protection and to receiving support. This issue is particularly hidden because few children with learning disabilities meet high thresholds for support from services. There is also limited awareness that young people with learning disabilities are sexually exploited.

While there are notable benefits the internet can bring to young people with learning disabilities, they are also at greater risk of being groomed and sexually exploited online than their peers[115]. Young people with learning disabilities may turn to social networking to alleviate their social isolation and thus could become particularly vulnerable to being groomed online[116].

Recommendation: *There is a recognised need to empower young people with learning disabilities, so that they can recognise exploitation in general and disclose abuse, but there also needs to be more preventative work through education and safety skills development. All educational establishments should provide high-quality, age appropriate sex and relationships education, including same-sex relationships, with information adapted and made accessible.*

Which platforms and sites are most popular among children and how do young people use them? Many of the online services used by children are not specifically designed for children. What problems does this present?

1.8. Social media usage and children's well-being

Our forthcoming Good Childhood Report 2016[117] finds that a significant gender gap in well-being has opened up in recent years, with girls becoming increasingly unhappy with their lives overall and, especially, with their appearance. Analysis in the report shows that more than one third (34%) of girls are unhappy with their appearance – up from 30% over five years. By contrast, the proportion of boys of the same age who are unhappy with their appearance has remained stable at around 20%. This means the estimated number of girls in the UK who are unhappy with their appearance has risen by 8% from 647,400 to 699,700 between 2009/10 and 2013/14.

This new trend also builds on findings from last year's Good Childhood Report, in which England ranked last out of 15 countries for happiness with appearance and also had the most pronounced gender differences of all participating countries.

Our research does not offer explanations for these trends but other studies – including ONS trends showing a rise in social media usage amongst teenage girls but not teenage boys, and research highlighting an association between mental health problems and social media usage - suggests that future research needs to consider the role that social media plays in the lives of girls in particular.

115 Ibid, Page 46.
116 Ibid
117 Findings from our forthcoming Good Childhood Report 2016

Recommendation: *The Department for Culture, Media and Sport should commission research to explore the links between young people's mental health and well-being, girls in particular, and social media usage.*

2. EDUCATION

What roles can schools play in educating and supporting children in relation to the internet? What guidance is provided about the internet to schools and teachers? Is guidance consistently adopted and are there any gaps?

2.1. The role of sex and relationships education

Physical, Social, Health and Economic (PSHE) education is designed to equip young people with the necessary knowledge, skills and attributes to stay safe and healthy and to develop into independent and productive members of our society. We believe PSHE is a vital component of a child's school experience, but more needs to be done to introduce relevant and up to date content to warn young people about the dangers they may face, including those that exist online.

For several years we have been delivering programmes in secondary schools to help young people understand the risks of child sexual exploitation and running away. Our sessions empower young people to make safe choices and learn about positive, healthy relationships including staying safe online including the impact of sexting and online grooming. Giving PSHE a stronger status in the national curriculum will ensure that these messages are taught to all children in secondary schools. To give PSHE this status, we have been calling for PSHE to become a statutory part of the curriculum in all schools to teach children and young people about their health and well-being.

2.2. Education on sexting

'Sexting' is the exchange of self-generated, sexually explicit images or videos through mobile phones, computer and other devices such as tablets. Sexting has become a common activity among young people, and research[3] suggests that sexting often occurs as a result of sexual pressure from peers, which can lead to harassment, bullying and even physical or sexual abuse. In some instances as our research shows the pressure to take and send explicit images comes from contacts young people meet online[118]. Young people should be educated about the dangers and long-term implications of sexting to enable them to withstand the pressure to engage in inappropriate forms of communication for children and young people.

Recommendations*:*

- *We believe that schools can play a vital role in promoting online safety as part of personal, social, health and economic education (PSHE) alongside education about consent, exploitation grooming and healthy relationships*

118 Seriously Awkward report (June 2015)

in general. To ensure a consistent approach is taken, we have been calling for PSHE to become a statutory part of the curriculum in all schools.

- *Young people should be educated about the risk of being groomed for sexual exploitation as a result of sexting, about the images remaining in circulation even children change their mind about sharing the image and about the legal implications of sexting.*
- *Parents, teachers and other professionals must be willing to discuss sexting in the context of more general bullying cases, and help make young people aware that sexting can be an unacceptable form of harassment.*
- *Young people should be encouraged to speak about their experiences to parents and trained professionals, and be offered support and advice to recover from any trauma caused as a result of sexting.*

2.3. Guidance for schools on how to recognise and respond to sexual online behaviours

Our practitioners who deliver workshops in schools report that many teachers lack the confidence and skills to prevent and monitor children accessing sexual material online in school. With many children having access to their own devices that is not regulated by schools, this becomes even more challenging. Children are not only viewing inappropriate sexual content but in many cases are making and distributing them themselves.

The draft revised Department for Education guidance on keeping children safe in schools acknowledges the importance of addressing online safety. However, we feel that it does not go far enough in recognising the needs training needs of staff in schools; especially as new websites and social media platforms are constantly developing.

Recommendation: *The revised and forthcoming statutory guidance on Keeping Children Safe in Schools should outline the training requirement of staff in schools in keeping children and young people safe online. The guidance should also include a requirement for safeguarding leads to receive regular training on online safety.*

Who currently informs parents of risks? What is the role for commercial organisations to teach e-safety to parents? How could parents be better informed about risks?

2.4. Pressures to take and share explicit pictures and to share indecent imagery and videos

Concerns have been raised about young people's increased access to online sexual imagery and content as well as the making and sharing of imagery and videos themselves. Our Seriously Awkward report[119] revealed the pressures young people face to send sexually explicit pictures of themselves online. In our poll for Seriously Awkward report around 6% of 16 and 17 year olds reported feeling under pressure to take and send explicit pictures of themselves and around 10% reported that they do it. The report found that parents of 16 and 17

119 Ibid.

year olds underestimate some of the pressures young people facing young people online; for example, to take and send explicit photos of themselves. Just 13% of parents thought pressure to do this came from online contacts, but of 16–17 year olds who felt under pressure to do this, nearly four in 10 (38%) said they felt this pressure from contacts they met online. This may lead parents to not discuss these issues with their children.

Recommendations:

- *We believe that more needs to be done to educate young people about the dangers and long-term implications of sharing indecent images and videos to enable them to withstand the pressure to engage in this unhealthy form of communication for children and young people.*
- *Parents and professionals should be encouraged and supported to apply suitable filters and safety measures to prevent exposure to explicit content on electronic devices. Age verification checks should be better integrated with online and mobile parental controls to ensure parents have oversight over their children's digital activities.*

3. GOVERNANCE

What voluntary measures have already been put in place by providers of content to protect children? Are these sufficient? If not, what more could be done? Are company guidelines about child safety and rights accessible to parents and other users?

3.1. Age ratings for online music videos

Research recently commissioned by the British Board of Film Classification (BBFC) found that up to 60 per cent of children aged 10 to 17 say they are watching music videos online that they do not think their parents would approve of[120].

The Children's Society welcomed last year's announcement that following a successful pilot, the BBFC has partnered on a long-term basis with Sony Music, Universal Music and Warner Music who will send videos to the BBFC before putting them on YouTube and Vevo meaning that videos produced by these industries will now get the same age ratings as films. This is a positive step forward however it is currently only a voluntary basis and does not apply to international artists. We believe that much more needs to be done to verify the age of viewers of music videos, particularly on poorly regulated websites. Children and young people can too easily by-pass current age verification methods as they simply request a date of birth.

Recommendation*: The government should explore the effectiveness of introducing a universal age rating on music videos, including those that are produced abroad.*

4. LEGISLATION AND REGULATION

120 https://www.gov.uk/government/news/action-to-protect-children-from-viewing-age-inappropriate-music-videos-online

What are the regulatory frameworks in different media? Is current legislation adequate in the area of child protection online? Is the law routinely enforced across different media? What, if any, are the gaps? What impact does the legislation and regulation have on the way children and young people experience and use the internet? Should there be a more consistent approach?

4.1. Recent legislative proposals to protect children and young people online

We believe that all legislative and regulatory initiatives to protect children and young people online should be accompanied by good quality online safety education for children and their parents that outlines the risks and benefits of the changes introduced.

4.2. Policing and Crime Bill 2015-16

The Policing and Crime Bill currently passing through parliament proposes a new welcome measure to extend the definition of child sexual exploitation to incorporate live streaming and transmission of indecent images[121]. We welcome this crucial provision set out in the bill that seeks to protect children and young people from sexual exploitation by ensuring that relevant offences in the Sexual Offences Act 2003 cover the live streaming of images of child sex abuse. Our practitioners increasingly see the use of live streaming applications to sexually abuse and exploit children and young people.

4.3. *Age verification for pornography websites and the Digital Economy Bill 2016-17*

We welcome that the recently introduced Digital Economy Bill that seeks to address the important issue of protecting and preventing children and young people from accessing online pornographic material. We believe the introduction of age verification for commercial porn websites will greatly contribute to this aim. However, our practitioners tell us that young people are regularly accessing inappropriate and sexualised content online beyond commercial porn websites and are circulating these materials.

With respect to children accessing websites using false credentials, we believe a combination of age verification methods need to be used to stop children from successfully gaining access. We believe proof of credit card ownership (or other form of payment) on entry to the site, plus the use of a reputable personal digital identity management service (such as the electoral register) and another proof of age (such as ownership of a mobile phone contract or other direct debit) would better ensure that children cannot enter pornographic websites.

We believe that age-verification on pornography websites is necessary to prevent children from learning about sex and relationships through these domains.

---

121 Policing and Crime Bill 2015-16, Part 9, 144. http://www.publications.parliament.uk/pa/bills/lbill/2016-2017/0055/17055.pdf

Recommendation: *The Digital Economy Bill 2016-17 presents an important opportunity to further enhance protections for children and prevent them from accessing pornography from both commercially regulated and non-regulated digital channels.*

What more could be done by the Government? Could there be a more joined-up approach involving the collaboration of the Government with research, civil society and commerce?

4.4. National campaign aimed at promoting child internet safety

Every year, The Children's Society celebrates global Safer Internet Day in February to help promote the responsible and positive use of the internet. We believe that a coordinated national campaign aimed at children, young people and their parents is necessary. This should include schools and further educational establishments to help educate young people, challenge inappropriate online behaviours, and empower them use the internet positively, including supporting their well-being and educational attainment.

Recommendation: *As concerns continue to grow around the safety of children and young people online, we believe a national campaign should be developed to promote the positive and safe use of the internet and to educate children, their families and the public about the risks accessing the internet can pose for children.*

August 2016

Department for Culture, Media and Sport – written evidence (CHI0055)

Children and the Internet Inquiry

Risks and benefits

1. **What risks and benefits does increased internet usage present to children, with particular regard to:**

    i. **Social development and wellbeing**
    ii. **Neurological, cognitive and emotional development,**
    iii. **Data security.**

1. The Government remains committed to improving the safety of children online.

2. There is no doubt that the internet plays an important part in the lives of children and young people. Many are sophisticated in the way they use apps and websites, tailoring their communication for different audiences, and using a range of devices including smartphones, tablets, and games consoles.

3. The internet has brought fantastic opportunities for children and young people as they grow. It lets them express their creativity, research a wide range of subjects, participate in dialogue and debate, and learn about different cultures and places around the world. It helps improve their educational attainment and enrich their lives, helping them reach their potential, encourage their participation, and learn about social responsibility. Their exposure to diverse views and people can also help them develop their own identity by enabling them to explore relationships, find peer groups online, share their problems and seek support services and information. This can be of particular benefit for vulnerable and isolated children and young people.

4. However, we know that children and young people can feel unable to switch off from their online lives, which can be a source of stress. The Department of Health, with NHS Choices, has worked to address this by providing information on mental health so that young people can understand more about issues, symptoms and where to find support: http://www.nhs.uk/livewell/youth-mental-health/pages/Youth-mental-health-help.aspx

5. In addition, as a response to the recommendation of the Health Select Committee on Children's Mental Health on the impact of the online world on children and young people, the Department of Health has also created a specific training package in partnership with MindEd and Xenzone. MindEd is a free e-learning platform launched in March 2014, aimed at improving the knowledge of children and young people's mental health among professionals who work with children. The resources were developed by a

consortium of expert organisations, led by the Royal College of Paediatrics and Child Health. The programme was developed after a £3 million investment by the Department of Health, and its ongoing maintenance is funded by Health Education England. It is designed to help professionals understand the digital world and online risk better, with input from young people and professionals, and is being well received: https://www.minded.org.uk/course/view.php?id=403

6. The Department of Health has also commissioned an update of the 2004 prevalence survey in partnership with NatCen Social Research and the Office of National Statistics. It will include information on issues like cyberbullying and its impact. In addition, the Department of Health is commissioning a suite of evidence-based digital tools with NHS England, expected to be available through NHS Choices in spring 2017.

7. In order to future-proof our children's digital skills, the Government has introduced the new computer science curriculum, which includes topics such as online safety and security, providing the computational thinking skills which will enable young people to adapt to emerging technologies.

8. The digital transformation of the economy is changing the shape of the labour market and the types of skills needed by businesses, and children will need to gain confidence to navigate this new world. Digital skills, including the safe and effective use of the internet, are therefore increasingly important to our children's future employability and prospects.

9. Like all forms of public communication, internet usage can bring risks and the Government is aware of parental concerns about content and inappropriate or upsetting behaviour on online services.

10. Getting the most out of what the internet has to offer also means learning to use it responsibly at each developmental stage of childhood. Children will have to be supported in this so that they have adequate opportunities to learn how to communicate safely online, the relevance of their online reputation and that inappropriate behaviour online is not acceptable. The Government is very clear that alongside industry, parents, the education community and specialist charities, we must all work together to ensure that children are supported in their journey into adulthood.

2. Which platforms and sites are most popular among children and how do young people use them? Many of the online services used by children are not specifically designed for children. What problems does this present?

11. While not all social media and interactive services (e.g. social networks, messaging, Q&A sites, interactive games, cloud services or ephemeral messaging services) may be designed with children in mind, the Government expects online industries to ensure that they have relevant safeguards and processes in place, including access restrictions, for children and young people who use such services.

12. In particular, the Government expects social media and interactive services to have robust processes in place to address inappropriate and abusive content on their sites. This includes having clear reporting channels, acting promptly to assess reports, and removing content that does not comply with their acceptable use policies or terms and conditions. The internet can also help signpost vulnerable users to useful sources of information and support.

13. However, the Government understands the need for services specifically for children, so asked Ofcom, in its role as Chair of the UK Council for Child Internet Safety (UKCCIS)[122] Social Media Working Group, to encourage businesses to think about 'safety by design' to help make their platforms safer for children and young people under the age of 18.

14. The Social Media Working Group has therefore developed a practical guide for providers of social media and interactive services, working with major platforms (including Twitter, Facebook, Google, Ask.FM, MindCandy and Microsoft), charities, and law enforcement agencies. The guide includes examples of good practice from leading technology companies, and advice from NGOs and other online child safety experts. UKCCIS members are currently working with other partners to ensure this guidance influences policy and practice by online service providers both within and outside the UK.

15. The Government has also published a guide for parents and carers of children using social media. It includes practical tips about the use of safety and privacy features on apps and platforms, as well as conversation prompts to help families begin talking about online safety. It also contains pointers to further advice and support. The guide is available here: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/490001/Social_Media_Guidance_UKCCIS_Final_18122015.pdf.pdf

16. The UKCCIS guide for social media and interactive services and the UKCCIS parents' guide can be accessed at: www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis

3. What are the technical challenges for introducing greater controls on internet usage by children?

17. Ultimately, industry is best placed to facilitate the best technical tools for their services and to stay apace with the challenges brought by rapid technological progress. Industry must also remain alive to children's media consumption patterns and behaviour towards technology when developing any technical tools - how and where children use the Internet is as important as what type of apps and devices might appeal to them.

18. Family-friendly filters are a key tool in keeping our children safe online. The Government has encouraged Internet Service Providers (ISPs) to provide parents with the ability to easily filter content. The four major ISPs (BT, Sky, TalkTalk and Virgin Media together constitute an estimated 90% of the

122 UKCCIS is a body responsible for developing and overseeing child internet safety solutions. See question 12.

UK's broadband market) provide an unavoidable choice on whether to switch on family friendly network level filters to all their customers. Government is also working with the Internet Service Providers Trade Association (ISPA) to see what more smaller providers can do and many - KCom, Plusnet, and Claranet Soho - offer free of charge filters to customers. Should families choose an ISP that does not filter, there are plenty of free filtering solutions on offer.

19. All the ISPs' family-friendly filters allow tailoring and choice based on the age of children in the family. The categories of content that are filtered differs by provider, but typically websites allowing access to pornography, violence, suicide, self-harm and sites that require the user to be over 18, will be filtered. The Government believes the filtering solutions on offer deliver the best of both worlds; engaging parents to think about online safety but applying filters where parents don't engage.

20. We know that technology tools are not a silver bullet, and that savvy children may be able to circumvent them. Therefore education and awareness of internet safety remains of fundamental importance to help children and young people to think critically about what they do online, what information they share, and how they interact with others. This way, they will be able to make the most of their experiences and know to speak to an adult for guidance or help.

21. With this in mind, in 2013, the former Prime Minister David Cameron asked ISPs and others to focus their skills on parental awareness. BT, Sky, TalkTalk and Virgin Media, supported by education, charity, industry and law enforcement, launched a large-scale awareness campaign in Spring 2014, 'Internet Matters', the aim of which is to help parents make informed and confident choices about online safety.

4. What are the potential future harms and benefits to children from emerging technology, such as Artificial Intelligence, Machine Learning and the Internet of Things?

22. The Government has created a mechanism through UKCCIS to better understand the future harms and benefits to children and young people from emerging technology by setting up a new Technical Working Group to bring together experts to explore and understand relevant technological developments that relate to child internet safety. UKCCIS is co-Chaired by Edward Timpson MP, Minister of State for Vulnerable Children and Families (Department for Education), Sarah Newton MP, Minister for Vulnerability, Safeguarding and Countering Extremism (Home Office), and Baroness Joanna Shields, Minister for internet Safety and Security (Department for Media Culture and Sport).

23. This Technical Working Group will aim to identify both harms and benefits and will draw on expertise from the Internet Watch Foundation (IWF), ISPs, technology companies, experts on age verification, and charities working with children and young people. The main aim of this Working Group will be to keep UKCCIS Ministers and the Government informed of emerging technology, such as the Internet of Things, and how this may impact

adversely on children and young people.

24. UKCCIS also has an Evidence Working Group, chaired by Professor Julia Davidson, which informs its Executive Board of potential future harms and benefits to children. It is a unique forum that brings together leading experts at the forefront of research on online child safety and child sexual abuse. It provides UKCCIS with a 'timely, critical and rigorous account of relevant national and international research' on child internet safety and online child abuse. For example, on children's use of technology (including gaming); parental awareness and supervision; vulnerable children and young people; and research informed practice. It also provides an annual overview of child internet safety based upon research indicators.

25. The terms of reference for all UKCCIS working groups are available online - https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis#working-groups

Education

5. What roles can schools play in educating and supporting children in relation to the internet? What guidance is provided about the internet to schools and teachers? Is guidance consistently adopted and are there any gaps?

26. The introduction of e-safety content in key stages 1 and 2 (ages 5-11 years) reflects the fact that younger children are increasingly accessing the internet, and is intended to inform pupils of good practice in staying safe online from an early age. Since September 2014, children in primary schools are taught how to use technology safely and respectfully, how to keep personal information private, recognise acceptable/unacceptable behaviour and where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

27. In secondary schools, pupils are taught about responsible, respectful and secure use of technology, as well as age-appropriate ways of reporting any concerns they may have about what they see or encounter online. There is progression in the content across the key stages to reflect the different and escalating risks that young people face as they get older (initially relating to online content, then to the conduct of and contact with others). This content was developed with input from e-safety experts including Childnet, NSPCC and the UK Safer Internet Centre.

28. Teachers in all schools are being supported by the Department for Education to deliver all aspects of the new curriculum, including e-safety. This support has included:

- over £5 million to establish and grow the Network of Teaching Excellence in Computer Science, building a national network of over 400 'Master Teachers' whom schools can commission to provide training for their teachers;
- £1 million for Computing at School to meet the needs of primary schools teachers who lacked the specialist computer science subject knowledge required to teach the new curriculum; and

- a £500,000 competitive match-funded scheme that has supported innovative approaches to promoting excellent computing teaching, levering in additional investment and engagement from business, such as Microsoft, Google and Raspberry Pi.

29. In addition, there are a wide range of free and independent sources of advice available for schools. This includes advice from the Safer Internet Centre, Child Exploitation and Online Protection Command (CEOP), NSPCC, Childnet International and Internet Matters, among others.

30. Keeping Children Safe in Education (KCSIE) is the statutory guidance to which all schools and colleges must have regard when carrying out their duties to safeguard and promote the welfare of children. The guidance sets out that all school staff have a responsibility to provide a safe environment in which children can learn. All staff should escalate safeguarding concerns about children to the school's designated safeguarding lead and or children's social care. All school staff should receive safeguarding training during their induction and should have regular updated safeguarding training.

31. Newly revised KCSIE guidance came into force on 5 September 2016 for all schools in England and includes for the first time a section covering online safety in schools. This sets out the importance of protecting children from harmful and inappropriate content. The guidance states that schools should ensure appropriate filters and monitoring systems are in place. Additional information to support schools in keeping their children safe online has also been provided. This includes expert advice from the UK Safer Internet Centre as to what appropriate filters and monitoring might look like. The KCSIE guidance can be found online at https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

32. All schools are required by law to have a behaviour policy with measures to tackle all forms of bullying among pupils. Schools are free to develop their own anti-bullying strategies but they are held clearly to account for their effectiveness through Ofsted. To support schools to tackle bullying, including cyberbullying, the Department for Education has produced a factsheet for schools which outlines their responsibilities to support children who are bullied and advice to help teachers protect themselves against cyberbullying, and what to do if it happens.

33. The UKCCIS Education Group (of which the Department of Education is a member) has recently produced advice for schools and colleges on responding to incidents of 'sexting.' The advice aims to support them in tackling the range of issues which these incidents present including responding to disclosures, handling devices and imagery, risk assessing situations and involving other agencies. It explains how schools can best support the children involved and includes case studies for staff training purposes and links to further sources of support and advice. The advice also contains information about preventative education, working with parents and reporting imagery to providers. The recently revised KCSIE includes a link to the advice,which is also available at:

https://www.gov.uk/government/groups/uk-council-for-child- internet-safety- ukccis

34. The Government has also changed legislation to strengthen teachers' powers to enforce discipline and promote good behaviour in schools. Teachers can search pupils for banned items, issue same day detentions and use reasonable force when necessary. Search powers included in the Education Act 2011 have given teachers stronger powers to tackle cyberbullying (via text message or the internet) by providing that when an electronic device, such as a mobile phone, has been seized, a teacher who has been formally authorised by the head teacher can examine data or files, and delete these, where there is good reason to do so.

35. In addition, the Government has moved the emphasis from schools 'considering' how children are taught about safeguarding, including online safety to 'ensuring' children are taught about safeguarding, including online. We would expect this to be achieved through teaching and learning opportunities as part of providing a broad and balanced curriculum. This may include covering relevant issues via personal, social, health and economic education (PSHE).

36. The Government Equalities Office (GEO), has funded the development of resources to educate young people about staying safe online. In 2015-16, the Government invested almost £500,000 in the UK Safer Internet Centre to provide advice on how to keep children safe, and deliver the following resources to be published shortly:

- updated cyberbullying guidance for schools to help them understand, prevent and respond to cyberbullying, including sexting; sharing good practice developed in schools;
- a PSHE toolkit, to help schools deliver sessions about cyberbullying, peer pressure and sexting;
- support to professionals through a Professionals Online Safety Helpline; and
- a series of Online Safety Briefings for professionals working with children.

37. Recently, the Department for Education and GEO announced funding for ten innovative projects to support schools to address bullying, including online bullying - totalling £4.4 million.

38. One of these initiatives will use the online reporting platform, Tootoot at its core. Tootoot will provide 24 hour support to young people who are victims of all forms of bullying or online abuse. Young people can screenshot abusive messages or even take photographs of bullies in action then send them via the app. These reports will then be read by staff at the child's school, but no one else. This significant increase in funding will reach more schools and teachers across the country to prevent and respond to all forms of bullying and build inclusive school environments.

39. The Government wants all young people to develop healthy, respectful relationships. GEO and the Home Office jointly funded £3.85 million to

launch the second phase of the *This is Abuse* campaign, called 'Disrespect NoBody,' in February 2016. The campaign encourages young people to rethink their understanding of abuse within relationships, which includes issues like sexting.

40. To support the campaign, the Government has worked with the PSHE Association to produce a new resource for teachers, support workers and other professionals working with young people. The guide uses the new campaign adverts to help professionals facilitate discussions with teenagers on what constitutes abuse in all types of relationships – including relationships involving lesbian, gay, bi and transgender (LGB&T) young people. The discussion guide is available online - www.pshe-association.org.uk/curriculum-and-resources/resources/disrespect-nobody-discussion-guide

41. The Government has also taken steps to ensure children are safe from terrorist and extremist material when accessing the internet in school.

42. The Prevent Duty Guidance for England and Wales and the Prevent Duty Guidance for Scotland (www.gov.uk/government/publications/prevent-duty-guidance) makes clear that specified authorities, in complying with the duty, ensure that publicly owned venues and resources do not provide a platform for extremists and are not used to disseminate extremist views. This includes considering whether IT equipment available to the general public should use filtering solutions that limit access to terrorist and extremist material.

43. The duty specifically makes clear that schools will be expected to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering to limit access to terrorist and extremist material. In addition to this, the Department for Education consultation (https://www.gov.uk/government/consultations/keeping-children-safe-in-education-proposed-changes), launched in December 2015, proposes changes to keeping children safe which obligate schools to ensure appropriate filtering and monitoring systems are in place.[123]

44. As part of meeting the requirement in the Prevent Duty Guidance, schools will want to check with their filtering company if their filtering product includes the police assessed list of unlawful terrorist content, (produced by the Counter Terrorism Internet Referral Unit (CTIRU) on behalf of the Home Office).[124]

45. All these aspects of schools' duties to safeguard children and young people are covered in Ofsted's school inspection framework and we consider that schools take them seriously.

---

123 For more on what constitutes 'appropriate' filtering, schools may consult the UK Safer Internet Centre's guidance titled "Appropriate Filtering for Schools".

124 Filtering companies may contact the CTIRU at NCTPFC.CTIRU.Public@met.pnn.police.uk.

46. The Counter Extremism Strategy, published in 2015, proposed to empower those who wish to challenge extremists online, including the proposal to run a programme nationally to make young people more resilient to the risk of radicalisation online and to provide schools and teachers with more support to address the risk posed by online radicalisation. The Home Office have been working with a number of local projects looking at this issue and cataloguing best practice. They have also been working with UKCCIS on their wider Digital Resilience project.

6. Who currently informs parents of risks? What is the role for commercial organisations to teach e-safety to parents? How could parents be better informed about risks?

47. Helping parents and carers to protect their children from inappropriate and harmful content online is a priority for this Government. Some parents are more knowledgeable than others, and we recognise the need to raise awareness of online child safety issues and how they can be addressed, but very few adults these days are not using the internet as part of their daily lives.

48. Following a request from Government, the leading four ISPs (Virgin, Sky, BT and TalkTalk) launched Internet Matters (www.internetmatters.org) to support parents to make informed and confident choices about online safety. Internet Matters develops media campaigns, supported by a central website, that reach out to millions of parents to highlight relevant issues, and to encourage them to get more involved in their children's digital lives. The site contains links and information about keeping pre-schoolers, young children, pre-teens and teens safe online. Internet Matters continues to work with industry, in particular, the BBC, Google, Barclays, Disney, EY and Twitter have all made significant contributions to its work over the last year.

49. As noted above, the Government has encouraged ISPs to enable parents to easily filter content by giving them an unavoidable choice to switch family friendly network level filters on. We believe that this will help empower parents, driving them to expect more from their ISP.

50. The Government has also worked to ensure content is filtered in public places where children are likely to be. Six major providers (BT, O2, Virgin Media, Sky, Nomad and Arqiva), who are estimated to cover around 90% of the market, committed to provide family-friendly public Wi-Fi. A Friendly Wi-Fi Logo was launched by the RDI (UK) Holdings in July 2014, to help parents identify the safest places to browse the internet. The logo gives parents the assurance that a particular business, retailer, or public space is filtering to an agreed and clearly communicated minimum (illegal child abuse content, and also pornography). This is now in place in many stores in the UK, including Tesco, Starbucks and IKEA.

51. We also need to help parents to have important conversations with children, and to spot warning signs early. The National Crime Agency's (NCA) Child Exploitation and Online Protection (CEOP) Command has developed a comprehensive education programme, called *Thinkuknow*,

which provides targeted advice to children, parents and carers, including on how to use social media safely. A specific site for parents, which provides valuable guidance on protecting their children from online risks, is available at www.thinkuknow.co.uk/parents/.

52. The Department for Education has also produced advice aimed at parents to help them keep their children safe from cyberbullying, spot the signs that suggest they might be being bullied and what to do if they are. The advice is available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/444865/Advice_for_parents_on_cyberbullying.pdf

53. There are a range of other resources available for parents and carers to inform them of how best to protect their children including, among many others, the websites of the NSPCC (www.nspcc.org.uk), Childnet (www.childnet.com), ParentZone (www.parentzone.org.uk), GetSafeOnline (www.getsafeonline.org), Cyber Streetwise (www.cyberstreetwise.com) and Internet Matters (www.internetmatters.org). In addition, leading social media and interactive services often educate users about safety as part of the experience on their platform. For example, they do this with information on their Safety Centre with tips to use the service safely, by asking users to respect the rules of the community, or by offering different safety tools. Other examples include the CBBC "Stay Safe" hub (http://www.bbc.co.uk/cbbc/curations/stay-safe) for information on staying safe online and Vodafone's "The Digital Parenting Magazine", which is free to order online for organisations working with families. Facebook and Google have also created tools and advice for parents and educators.

54. The GEO provided £75,000 to CEOP in 2015-16 to support a national roll out of Parent Info (www.parentinfo.org) which is delivered through schools. This is a free service for parents, which helps them show their children how to use the Internet and mobile devices safely and appropriately.

55. Through UKCCIS, specifically the Education Working Group, the Government will continue to encourage industry and organisations working on online safety in education to provide relevant tools, and lead education and awareness programmes to help parents and the communities around children and young people stay safe online.

Governance

7. What are the challenges for media companies in providing services that take account of children? How do content providers differentiate their services for children, for example in respect of design?

56. The UKCCIS guide '*Child Safety Online. A Practical Guide for Providers of Social Media and Interactive Services*' includes examples of current good practice for services targeted at and attracting users who are under 18 years old. It describes for industry how different social media, interactive services and child safety charities are currently dealing with key challenges. The Guide uses the safety framework of the ICT Coalition for Children

Online, a European industry initiative to make their platforms safer for users. This framework includes six principles for business on:

- Managing content on their service.
- Parental controls.
- Dealing with abuse and misuse on their service.
- Dealing with child sexual abuse content and illegal contact.
- Privacy tools and controls.
- Education and awareness about child online safety.

57. The UKCCIS Guide explains each of these principles, illustrating them with advice and examples from industry. It also includes additional advice for services that are targeted at under 13s, providing guidance and examples on deeper safety and controls to protect the youngest users on their platforms.

58. The Guide explains in detail how some challenges can be addressed through in-house safety policies, content management systems, content labelling and clear signposting, age-gating protections and identity authentication solutions, internal reporting processes, adequate staff training and product design, among other activities and tools. The Guide is available online - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/517335/UKCCIS_Child_Safety_Online-Mar2016.pdf

8. What voluntary measures have already been put in place by providers of content to protect children? Are these sufficient? If not, what more could be done? Are company guidelines about child safety and rights accessible to parents and other users?

59. Government takes the issue of child safety online very seriously and continues to engage extensively with industry through events and outreach. We expect social media companies to respond quickly to incidents of abusive behaviour on their networks. This includes having easy to use reporting tools, robust processes in place to respond promptly when abuse is reported, and suspending or terminating the accounts of those who do not comply with acceptable use policies.

60. The UKCCIS guide '*Child Safety Online. A Practical Guide for Providers of Social Media and Interactive Services*' explains further measures in place by providers of content to protect children. These include community guidelines and/or terms of service setting out what the service prohibits (e.g. inappropriate behaviour such as threats or hateful content), product features (e.g. default privacy settings) to education and awareness programmes (e.g. in partnership with charities and specialist organisations with reach into schools).

61. The Government strongly encourages growing and emerging social media and interactive services to follow the advice of the UKCCIS guide, and for more established companies to regularly review their policies, tools and processes to ensure that these are fit to provide adequate protections for

children and young people accessing their services. Ofcom as Chair of the UKCCIS Social Media Working Group have been leading on this work.

62. The Government is also supportive of the work of the Internet Watch Foundation (IWF) in tackling illegal images, and recognises the work that the internet industry has done to make removing child sexual abuse content a real success.

63. The Government is also working closely with key Communication Service Providers (CSPs) to do more to restrict access to terrorist and extremist content online and to promote counter-narrative materials.

Legislation and Regulation

9. What are the regulatory frameworks in different media? Is current legislation adequate in the area of child protection online? Is the law routinely enforced across different media? What, if any, are the gaps? What impact does the legislation and regulation have on the way children and young people experience and use the internet? Should there be a more consistent approach? *NB: Given the Committee is keen to leave the scope of this inquiry quite broad, media companies might include traditional broadcasters, advertisers, social networks, platforms such as YouTube. We are also including gaming.*

64. The current law in England and Wales includes a number of criminal offences and rights to civil actions which may be relevant in cases of misuse of the internet or social media. Material published on the Internet, or by mobile phone, etc, is subject to the same restrictions as material published elsewhere: in other words, what is illegal offline is illegal online.

65. Self-regulation also allows a broad range of interested parties to participate and can be an effective way of coming up with innovative and effective solutions to issues which, due to the nature of the internet, are often global. However, Government is prepared, where necessary and effective, to take legislative action in order to deliver our objectives as is the case on age verification legislation for access to sites containing pornographic content.

<u>Criminal offences online</u>

66. The Government is absolutely clear that abusive and threatening behaviour online - whoever the target - is totally unacceptable. In general, an action which is illegal offline is also illegal online. The law does not differentiate between criminal offences committed on social media or anywhere else – it is the action that is illegal.

67. A number of criminal offences may be committed by those abusing others on social media, including: credible threats of violence to the person or damage to property; sending grossly offensive, indecent, obscene or menacing messages; harassment or stalking.

68. Legislation that can be used to prosecute online abuse and related offences includes the Protection from Harassment Act 1997; the Malicious Communications Act 1988; and the Communications Act 2003.

69. Under the **Protection of Children Act 1978** (as amended), the UK prohibits the taking, making, circulation and possession with a view to distribution of any indecent photograph or pseudo-photograph of a child under 16 and such offences carry a maximum sentence of 10 years imprisonment. Section 160 of the Criminal Justice Act 1988 also makes the simple possession of indecent photographs or pseudo-photograph of children an offence and carries a maximum sentence of 5 years imprisonment. This age was raised to 18 in the Sexual Offences Act 2003 and there are defences for those aged over the age of consent (16) who produce sexual photographs or pseudo-photographs for their own use within a marriage or civil partnership. These defences are lost if such images are distributed.

70. The **Sexual Offences 2003 Act**, which came into effect in May 2004, significantly modernised and strengthened the laws on sexual offences in England and Wales to provide extra protection to children from sexual abuse and sexual exploitation. The Act reflects what we know today about the patterns and impact of sexual abuse in childhood. It was designed to meet 21st century challenges of protecting children, and addresses issues including internet pornography and 'grooming' children for sexual abuse. It provides a range of offences that can be committed, and/or encouraged and assisted online. For example, section 15 of the Act: meeting a child following sexual grooming.

71. Section 1 of the **Malicious Communications Act 1988** makes it an offence to send material to another person which conveys an indecent or grossly offensive message, a threat or information which is false and known or believed to be false by the sender. The offence can also be committed by sending an article or electronic communication which is, in whole or part, of an indecent or grossly offensive nature. In order to be guilty of the offence the sender's purpose (or one of them) in sending the item must be to cause distress or anxiety to the recipient or to any other person to whom the sender intends that the item or its contents or nature should be communicated.

72. Changes to the law in the **Criminal Justice and Courts Act 2015** increased the maximum penalty for offences under the Malicious Communications Act 1988 to two years imprisonment, and removed the requirement that prosecutions should be brought within six months of the offence being committed.

73. The **Protection from Harassment Act 1997** makes it an offence for someone to pursue a course of conduct which amounts to harassment or causes someone to fear violence. Online harassment is not separately criminalised but may be considered as part of the general criminal offence of harassment. Offences under this Act have been deliberately worded in such a way as to capture a wide range of behaviours which include

harassment, stalking and bullying. Harassment is generally understood to involve improper, oppressive and unreasonable conduct that is targeted at an individual and calculated to alarm them or cause them distress. The conduct might be verbal or non-verbal and it does not have to be the same type of action on each occasion. Critically the individual elements of a course of conduct need not in themselves be criminal. However when a series of events are seen in combination, they may form a course of conduct which could amount to a criminal offence. A 'course of conduct' in a case of conduct in relation to a single person must involve conduct on at least two occasions.

74. Section 127(1) of the **Communications Act 2003** creates a specific offence of sending (or causing to be sent) grossly offensive, indecent, obscene or menacing messages over a public electronic communications network. Section 127(2) creates a separate offence of causing annoyance, inconvenience or needless anxiety to another either by sending or causing to be sent, by means of a public electronic communications network, a false message or by persistently using the network. Amendments were made to the Act by the Criminal Justice and Courts Act 2015 which extended the time within which prosecutions under section 127 of the Communications Act 2003 may be brought, to up to three years from commission of the offence, as long as this was also within 6 months of the prosecutor having knowledge of sufficient evidence to justify proceedings.

75. Sexual Risk Orders and Sexual Harm Prevention Orders were created by the Anti-Social Behaviour, Crime and Policing Act 2014, replacing previous civil orders designed to reduce the risk of future sexual offending. These orders allow prohibitions to be placed on individuals to reduce the risk of their (re)-offending in future. These prohibitions are tailored to the risk associated with an individual and can, if necessary, include restrictions relating to internet usage.

76. Public protection and investigating whether an offence has taken place are matters for the police. Where an individual is concerned they are at risk of an offence being committed against them or they believe an offence may have been committed, they should always contact the police. It is then for the police to investigate any reports that an offence has taken place and for the police or the Crown Prosecution Service to decide whether to prosecute, depending on the circumstances of the case.

77. Published guidelines for the application of the current statute law to prosecutions involving social media communications was consulted on and was recently updated. It is clear and readily accessible through the Crown Prosecution Service at http://www.cps.gov.uk/legal/a_to_c/communications_sent_via_social_media/.

78. The Government is committed to preventing these crimes and to giving every child the protection and support they need. Our laws in this area are rightly robust, strict and respected across the world and it is vital that victims of crime see strong and certain justice delivered to their offender.

Common framework for media standards

79. The Government set out its concerns relating to consumer confidence in, and safety in, accessing audiovisual content in a more converged world in the 2013 paper '*Connectivity, Content and Consumers'* so that a more consistent approach applied across different media. The paper is available online at https://www.gov.uk/government/publications/connectivity-content-and-consumers-britains-digital-platform-for-growth

80. Industry and regulators worked together on a voluntary basis to ensure a common framework for media standards. This framework aims to support a more consistent approach across different media and make sure consumers understand what content has been regulated.

81. Ofcom has been leading the work to develop the framework, focusing on linear broadcast and on demand television as well as 'TV-like' content in the internet television space where that is currently regulated by Ofcom.

82. Ofcom conducted a number of roundtables and bi-lateral meetings with individual industry stakeholders to discuss their current processes and approaches to ensuring standards protection, and will produce a report to DCMS on a way forward.

Video games

83. Video games are subject to a mixture of statutory and voluntary regulation mainly linked to the Pan-European Games Information (PEGI) classification system. The Government urge those caring for children to look carefully at the PEGI or other age classification information on video games and also to consider using the parental controls where they are available. On video games consoles for example, controls can be set to block access to games with certain PEGI age ratings and also to block internet access.

84. PEGI - which has been adopted in most countries across Europe - classifies video games content against criteria which includes for example, depictions of violence, sexual scenes or themes, depictions of self-harm, drug use, bad language, gambling and the ability to interact online with other players. Video games are awarded 3, 7, 12, 16 or 18 PEGI age ratings as appropriate and pictograms are attached to the games to indicate the type of content they contain.

85. On behalf of PEGI across Europe, the UK's Video Standards Council - operating as the Games Rating Authority (GRA) - reviews and classifies games that are unsuitable for children younger than 12.

86. In the UK, the PEGI age ratings awarded by the GRA for video games supplied on physical media (console and PC games on discs, for example) have statutory backing under the Video Recordings Act 1984. Under this Act, it is illegal to supply any games on physical media without a PEGI rating if they are unsuitable for children younger than 12. For the UK, the GRA is also able to refuse to classify a game entirely - and effectively ban it from sale - if it considers the content to be illegal under any area of UK law or be likely to cause harm.

87. The market for games produced and delivered specifically for distribution via online channels and mobile devices ('apps) is global and protections focus on self-regulation by games developers, publishers and platform providers. In Europe, Microsoft, Sony Computer Entertainment and Nintendo all require PEGI ratings for games supplied via their consoles' marketplaces - XBox Marketplace, Playstation Store and Nintendo eShop.

88. Beyond the consoles, a key initiative in this area is the International Age Rating Coalition (IARC). IARC ratings vary depending on cultural differences but a games company instantly has an age rating for all or most of the regions where their digital product will be delivered from a single application process, including in the UK.

89. The IARC system has been implemented on the Google Play Store, which is used for Android-powered devices, and by Microsoft for its Windows Store on PC, tablets and mobiles. This means that all apps and games on these storefronts now display PEGI ratings for users across the UK and Europe. Apple uses its own age ratings system for apps and games distributed through its Apps Store.

Statutory guidance for schools

90. Keeping Children Safe in Education (KCSIE) is the statutory guidance to which all schools and colleges must have regard, when carrying out their duties to safeguard and promote the welfare of children. Working Together to Safeguard Children is statutory guidance for all schools that sets out inter-agency working to safeguard and promote the welfare of children. The guidance is available online: https://www.gov.uk/government/publications/working-together-to-safeguard-children--2 (See also question 5.)

Age verification for access to sites containing pornographic content

91. The Audio Visual Media Services Directive sets out that content that might seriously impair the development of minors must only be offered behind access controls for video-on-demand (VOD) and it must not be broadcast (on television) at all. The Audiovisual Media Services Regulations 2014 amended section 368E of the Communications Act 2003 to make clear that that material that has been or would be rated R-18 by the British Board of Film Classification (BBFC), and also any other material that might seriously impair the physical, mental or moral development of minors must be subject to protection measures, i.e. age verification. Material which has been refused a classification by the BBFC is banned from being placed on VOD services.

92. The Government has committed to introduce Age Verification (AV) checks for all commercial sites providing pornographic material online and, following public consultation, introduced clauses on AV within the Digital Economy Bill in July 2016.

93. Our proposed legislation will require commercial providers of pornography to implement robust age verification controls on their websites to prevent under 18 year olds from accessing pornographic content. The Bill's

provisions enable the Government to set up a regulator or regulators with the authority to instruct ancillary services, such as payment and advertising services, to withdraw their facilities from non-compliant sites. The aim of this is to disrupt the business models underpinning online pornography (whether it is free at the point of use or a paid service) and to require companies to comply with UK law or risk losing their income streams. Our aim is to capture all sites regardless of where they are based, with a targeted and proportionate approach.

94. By introducing AV checks, we will help to create a safer online environment for children in the UK. Our proportionate regulatory approach ensures maximum impact on commercial providers, making it harder for children to see this content. It also holds commercial pornography providers responsible for the harms they might facilitate.

95. This approach will sit alongside existing initiatives and we will continue to work on broader child internet safety issues, including work led by UKCCIS.

10. What challenges face the development and application of effective legislation? In particular in relation to the use of national laws in an international/cross-national context and the constantly changing nature and availability of internet sites and digital technologies? To what extent can legislation anticipate and manage future risks?

96. Whilst we can pass legislation which provides for extraterritorial jurisdiction, there are issues with identifying and tracing those who provide services from abroad which include illegal content (e.g. indecent images of children). For example, servers may host websites and whilst we may be able to block them, taking effective legal action is difficult.

97. The definitions we use allow the courts to widely interpret various legislation and also to apply older statutes to cover modern offending. The law has been interpreted pragmatically and, when required, updated by way of case law and statute.

98. As and when new technology has outstripped legislative capacity we have taken steps to address the gaps identified. For example, S65 of the Coroners and Justice Act 2009 was introduced to provide a definition of images to include data capable of conversion into moving or still images. Further, S69 of the Criminal Justice and Immigration Act 2008 amended the Protection of Children Act 1978 to extend the definition of 'photograph' to include derivatives of photographs, such as other forms of data. These derivatives include computer traced images, for example, computer traced images of photographs taken on a mobile phone or images manipulated from photographs using computer software.

11. Does the upcoming General Data Protection Regulation take sufficient account of the needs of children? As the UK leaves the EU, what provisions of the Regulation or other Directives should

it seek to retain, or continue to implement, with specific regard to children? Should any other legislation should be introduced?

The EU General Data Protection Regulation

99. The EU General Data Protection Regulation (GDPR) will come into effect on 25 May 2018. Following on from the EU referendum, the Government is considering how best to approach the legislative and administrative requirements to most effectively provide a data protection framework that will work for citizens and business alike; and that can be assessed as providing an adequate level of data protection. This will be a relevant consideration in the UK's future negotiations. In this regard the Government will work to ensure that the emerging framework provides sufficient protections for children.

Online Child Sexual Exploitation

100. Measures contained in EU legislation relating to online child sexual exploitation are well-entrenched in UK law and processes and would remain in place regardless of decisions about the EU legislation on exit from the EU. However, Article 25 of Directive 2011/92/EU on combating the sexual abuse and sexual exploitation of children and child pornography, requires states to, *inter alia,* take necessary measures to ensure the prompt removal of web pages containing or disseminating child pornography and block access to web pages containing or disseminating child pornography towards the Internet users within their territory. In the UK this function is carried out by the IWF on a voluntary basis and we will ensure this activity can continue.

101. The Government is about to begin the European Union negotiations and we will work to ensure the best possible outcome for children and young people everywhere.

12. What more could be done by the Government? Could there be a more joined-up approach involving the collaboration of the Government with research, civil society and commerce?

102. The Government is at the forefront of a multi-stakeholder approach to dealing with child internet safety. The 2008 Byron Review '*Safer children in a digital world*' recommended the creation of a UKCCIS – a body which would be responsible for developing and overseeing child internet safety solutions.

103. Today, the UKCCIS Executive Board is chaired by Ministers across three Government departments, reflecting the cross-cutting nature of child internet safety: Edward Timpson MP, Minister of State for Vulnerable Children and Families (Department for Education), Sarah Newton MP, Minister for Vulnerability, Safeguarding and Countering Extremism (Home Office), and Baroness Joanna Shields, Minister for internet Safety and Security (Department for Media Culture and Sport). Its secretariat sits

within DCMS and Government officials, and other departments are involved as necessary (e.g. the Department of Health, CEOP) to ensure a consistent and joined-up approach across Government.

104. UKCCIS oversees child internet safety solutions, and the Government's commitment to it remains strong. It brings together Government, industry, law enforcement, academia, mental health experts, charities and parenting groups to work in partnership to help to keep children and young people safe online. It is a unique multi-stakeholder forum representing over 200 organisations with an interest in child internet safety, and we believe it is responsive and relevant in a fast-paced and changing landscape.

105. To that end, the Executive Board was reviewed in June 2016 to incorporate new voices and fresh experiences, as well as to retain existing expertise. Industry representatives include the leading social media and technology companies (e.g. Google, Facebook, Apple and Twitter), the largest ISPs and mobile network operators (e.g. BT, Sky, TalkTalk, Virgin Media, Vodafone, O2/Telefonica), child online safety experts, charities and academics (e.g. Childnet International, The Diana Award, NSPCC, Professor Sonia Livingstone, Internet Watch Foundation), and mental health practitioners (e.g. Tavistock and Portman NHS Foundation Trust). UKCCIS also incorporates the broader child internet safety community through associate membership.

106. The UKCCIS Executive Board responds to new and emerging issues by setting up working groups with the ability and expertise to examine in-depth these issues and their impact. Current UKCISS Working Groups include:

- **Evidence Working Group:** this group stays up to date on national and international research on child online safety, monitoring trends and challenges (see also question 4). It produces summaries of a large body of internet safety research, available at http://www.saferinternet.org.uk/research, to inform policy-making.
- **Digital Resilience Working Group:** this group will map the gaps in the provision of digital resilience programmes for children and young people, and to explore and present recommendations to Government. This will also aim to support children and young people, as well as their parents, carers and teachers, to have the digital skills and emotional understanding to feel empowered to take action when they encounter problems online – whether this relates to bullying, promotion of harmful social, physical, psychological or emotional behaviours for example self harm, anorexia; poor mental health and well-being, or pornographic or extremist content. This in turn will help equip children and young people to identify and help deal with online risks that might lead to possible harm. The Group will engage with schools, parents, industry, expert civil society organisations and children themselves.
- **Technical Working Group:** this group will monitor and identify technology trends that may have an impact on children and young people, with particular considerations for child internet safety including issues like the Internet of Things.

- **Social Media Working Group:** following publication of its Social Media Guide, it will continue its outreach programme for the UKCCIS guide for providers of social media and interactive services to reach the startup community.
- **Education Working Group:** this identifies challenges faced by education settings across policy implementation, standards, training and delivery of resources, and undertakes projects to support education settings to address gaps or weakness in their online safety practice.

107. UKCCIS has achieved considerable success, without the need for statutory regulation, and through the enthusiasm and voluntary efforts of its members, fostering discussion on child internet safety policy (See also question 1). Some of UKCCIS's achievements and future work plan, include:

- A guide for providers of social media and interactive services to encourage businesses to think about 'safety by design' to help make their platforms safer for children and young people under 18.
- The roll-out of free, network level filters for the vast majority of broadband customers with prompts to encourage parents to activate them, and automatic family-friendly public Wi-Fi in places children are likely to be, as well as considering potential problems around overblocking.
- Working with the RDI (UK) Holdings to design a Friendly Wi-Fi logo, to allow parents and families to easily identify places where they can be sure that the public Wi-Fi has filtered inappropriate websites.
- A guide for parents and carers whose children are using social media.
- Sexting guidance to support schools and colleges on responding to incidents of 'sexting'.
- A regular UKCCIS newsletter for associate members to provide updates on progress of the working groups, and to share news and information on research and relevant developments.

108. UKCCIS's full Executive Board and Associate membership and publications are available online - https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis

109. The sexual exploitation of children online cannot be dealt with by any one country, company or organisation working in isolation: a coordinated global response is needed to respond to this global threat. In response, the UK has supported the WePROTECT Global Alliance to End Child Sexual Exploitation Online: a global coalition of countries, technology firms and organisations committed to national and global action to end the online sexual exploitation of children, working together to identify and safeguard more victims of this terrible crime and apprehend more perpetrators. The

UK has already galvanised activity on a global scale through a £10 million programme of capacity building by UNICEF in 2015/16 and UNICEF has now launched the Fund to End Violence Against Children to deliver global responses.

23 September 2016

Department for Culture, Media and Sport; Department for Education; and Department of Health – oral evidence (QQ 129-137)

Tuesday 29 November 2016

Watch the meeting

Members present: Lord Best (Chairman); Baroness Benjamin; Earl of Caithness; Lord Gilbert of Panteg; Baroness Kidron; Baroness McIntosh of Hudnall; Baroness Quin; Lord Sherbourne of Didsbury.

Evidence Session No. 9 Heard in Public Questions 129 – 137

Examination of witnesses

Baroness Shields OBE, Parliamentary Under-Secretary of State for Internet Safety and Security, Department for Culture, Media and Sport; Edward Timpson MP, Minister of State for Vulnerable Children and Families, Department for Education; and Nicola Blackwood MP, Parliamentary Under-Secretary of State for Public Health and Innovation, Department of Health.

Q129 **The Chairman:** I welcome the Ministers. We are very privileged to have three of them. We have decided that the collective noun for Ministers is an abundance. It is great that you have all been able to come.

As you have gathered, our Committee is looking at children and the internet and all the issues with that. At lunchtime today, we met 30 children, who came to talk to us and told us about the issues as they saw them. That was fascinating for us. Baroness Shields, may we refer to you as Joanna, along with Nicola and Edward, to make life easier for all of us in these otherwise very formal proceedings? Thank you, Ministers, one and all for joining us.

We are trying to get through an awful lot of questions in a very short time, so we are going to target you. Questions are not necessarily to be answered by all three of you. Some will be for just one of you. Those asking the questions will make clear to whom they are directed in the first place. I assure you that we will get through a lot in the one and a quarter hours that we have allocated to this, with much gratitude to you for joining us. Away we go. Baroness McIntosh has the first question.

Baroness McIntosh of Hudnall: This one is for you, Lady Shields. It is fairly general. With all your experience of looking at this issue, do you think that we currently have suitable and effective systems that are already in place and have been put there by the social media platforms

to deal with the problematic content lots of people are very concerned about? Even if there are already protections, could more be done? Can you see what more could be done and how that could be achieved? In particular, should online platform providers be required to prioritise and to point up trusted sources of information in response to searches? We are increasingly aware that there is an issue about how young people, in particular, discriminate between one source of information and another. Would you like to give us your views on some of that?

Baroness Shields: Certainly. I will answer the question by saying that there are caveats, based on what type of internet harm or crime we are dealing with. We have a very good working relationship with the industry around the identification and removal of child sexual abuse imagery. That one is a lot easier, because it is illegal in every jurisdiction that they operate in. We have that very strong co-operation. They are very responsive to our requests.

In other areas, it is not quite as good. For example, content that is extremist or violence provoking—it may have been uploaded by a proscribed terror organisation or a far-right organisation—sometimes falls into a grey area with regard to the countries in which they are operating. We have a very clear idea of what should come down. In general, we are successful in that work, as well. The Counter Terrorism Internet Referral Unit does a very good job of identifying content that contravenes our legislation. We get a percentage rate in the high 90s in getting that content removed. On other content—violent and abusive content—there is a spotty track record. I would say that it varies, based on the internet harm or crime concerned.

The thing that is most challenging in this area, as we become a more and more digital society and more and more connected, is that children have a phone with them. I heard this morning that 80% of kids today have access to their own digital device. They are connecting almost 24/7, often unsupervised.

Baroness McIntosh of Hudnall: Can I interrupt you for a moment? When you say "children"—you referred to those statistics, for example—what do you mean? Do you mean people between the ages of 13 and 18, or do you mean children from as young as eight? What does that stat cover?

Baroness Shields: I believe that the figure that I heard this morning from Ofcom was for children from 12 to 18, but 80% is a high number. What is happening is that it is accelerating in complexity. My conversations with the industry are often around saying, "Okay, you have been very co-operative when we raise these issues with you, but it does not scale for government or users to be the primary contact to identify this material and to ask for it to be removed. It just does not scale". A lot of our conversations are therefore around developing technology that will automate that process. For example, how do we use artificial intelligence, machine learning and natural language processing to identify content so that they can flag that up proactively and remove it themselves, before we have to ask them to do it? That is the only way in which it can scale.

Baroness McIntosh of Hudnall: Can I ask you to talk for a moment about content that is not illegal but may not be appropriate? How can you better put in safeguards against the wrong people accessing that?

Baroness Shields: The major platforms have terms and conditions that generally prohibit this type of content—at least in an organised way, by organised content providers. User-generated content is really the challenging aspect. A young person may upload an explicit photo of themselves. That photo becomes part of the internet, and there is no way to recall it. It is much easier to take down a piece of content that is developed by a publishing company or an organisation than to take down something that is user generated. The best way in which to deal with the second scenario is to develop digital resilience. I am sure that my honourable friend Edward will talk more about the process of building digital resilience into the curriculum and helping young people to become digitally independent and confident in their choices, so that they do not make that mistake in the first place.

The Chairman: It has been pointed out to us that in other countries—mostly, I must say, totalitarian regimes—government simply takes down those sites that are undesirable and unhealthy for the recipients. We do not.

Baroness Shields: No.

The Chairman: Does that tell us that the technology enables that to happen relatively easily?

Baroness Shields: The products that we use most are not normally available in the countries you refer to. Most of the products—the social networks, for instance—will not be available in those countries. If you look at Russia or China, many of the products that you use every day will not be available. People who operate in those jurisdictions operate under the terms and conditions of government—whatever is placed upon them. Whatever those regulations are, they operate in that way in order to function in that environment. To answer your question, there are indeed technical ways of identifying this type of material, but generally it has to be done by the platform itself or by opening up a channel to a third party—in this case, a Government—that could do that.

Baroness McIntosh of Hudnall: Could I ask you either now or later—it may come up again—not to lose sight of the point about trusted sources?

Baroness Shields: I am sorry for not coming back to that; my apologies. It is a difficult question. It is part of the zeitgeist of the moment and had very real implications recently, in the election. We are still trying to decipher what happened. The reality is that this is not necessarily a requirement on a commercial company. However, it would be in its interest to look at the issue and to understand how its algorithms amplify content that ignites passion in people and how what works very well for advertisers can become problematic, in the sense that the algorithmic bias then moves that content to the top of the news feed. I have not deciphered it in depth, but it looks like that is what happened. I know that you have asked the companies about that. They are much better placed to answer the question, but it is an issue. It is a

challenging issue for their brands and an issue of trust with their users. If I were there, I would recommend that they be very keen to address it.

Baroness Kidron: Do you welcome the statement that the EU has just made that it is looking for more transparency around algorithms and is interrogating this for the first time?

Baroness Shields: When did that come up?

Baroness Kidron: Very recently. It announced that it is going to look at the issue specifically.

Baroness Shields: We have been looking at all the university research around algorithmic bias and how it manifests on the various social media platforms. It is a very real issue, because that very algorithmic bias is what enables products to communicate their value proposition. It makes us like great brands that we love and share them with our friends. It is part of the business model, so it is really important to make sure that that business model is not favouring nefarious interests.

Q130 **Earl of Caithness:** This is also for you, Lady Shields. Do you think that there is enough understanding between parents and children about how their online data can be collected and used? At what age can a child understand what agreement that child has signed up to? Do you think that 13 is the right age for that? If so, what is the evidence for that? Besides the age limit for consent, what other protections should children be entitled to regarding their personal data?

Baroness Shields: Your first question is about whether I believe that parents and children understand the data that is collected about them, their rights and what is available to them as regards removal. I do not think that people understand very effectively what their rights are in those scenarios and what is dictated by the terms and conditions of the companies that operate those platforms. It is interesting, because the information about that is available in the terms and conditions, but it is buried inside the legalese and is very complicated and difficult for a parent to teach or for a child to understand. You often give consent without care, just by accepting the terms and conditions. The companies have reacted very well, by creating safety centres where they detail exactly what types of data they are collecting. They are very good about privacy notices and various other things, but you have to know that you are looking for that and where to find it. There is an argument that it would be good if that information were more transparent.

With respect to your question about age, it has always been age 13, since the internet began. Most of the companies sprang out of Silicon Valley and were in the United States, where 13 was the age of consent for accessing internet services. I do not know whether that is the right age or not. In the general data protection regulation, which has been passed and will come into effect in May next year, the age of consent was agreed to be 16, but we and other countries wanted to have the opportunity to explore in more detail—through consultations and in other ways, working with experts—whether 13 was the desirable age. The UK therefore secured an agreement with Europe to look at that. We have the discretion to legislate to 13.

Earl of Caithness: The third question was: should there be any other conditions, besides age, to protect children and their data?

Edward Timpson MP: Shall we move the spotlight to a different part of the stage? To re-emphasise the point that has already been made, if we are truthful about it, adults are not very good at managing their personal data. We have a lot to learn ourselves before we espouse that in relation to children. That makes it all the more important when we look at the generation coming through, who are living their lives online, that we build in as early as possible their understanding that they have at their fingertips the ability to control their personal data and to protect themselves to a greater extent than we probably do ourselves. We will probably come on to the computer curriculum. Trying to build in the digital resilience of young people—from a much earlier age than we ever imagined—is one of the best defence mechanisms that we have available to us to ensure that, as we become more savvy as adults, we also have a generation of children coming through who are even better prepared for many of the risks, as well as the benefits, that the internet has to offer.

The Chairman: This leads on to you, Baroness Quin.

Q131 **Baroness Quin:** In the course of the inquiry, we have focused quite a bit on the role of schools and what they can and, perhaps, should do. It is fair to say that I, at least, have got the impression that there is quite a variety of practice in schools on this. I am therefore interested in asking you about the balance of responsibility among parents, schools, government and industry. What is the role of government, in particular, given that you are a Minister in the Department for Education? How much do you think schools should be doing? How much should government be aiming not just to spread best practice but to ensure that all schools follow certain practices?

Edward Timpson MP: The starting point is that sense of collective responsibility. We try to practise what we preach on that in relation to the cross-government work that we do with the UKCCIS board. I see that Professor Livingstone is one of your advisers. I know her very well from the work that the board has done, which is bringing together government, industry, charities and now, much more, the education world, to try to get them to work together for a common solution to many of the different issues that arise.

There is always a tension about where the greatest level of responsibility should be. There are those who, understandably, see it as the role of the parent to make sure that the child whom they bring into the world is equipped with the life skills that they need to cope with whatever modern life throws at them, but there is undoubtedly an important role for schools in enabling children to acquire the resilience that they need. Because this is a new and emerging area, not just for government or industry but for individual teachers, there will be a disparate level of response to what is required.

Our job as the Government is to try to set out a very clear approach that every school should follow. If you look at digital resilience, since September 2014 we have had the new computer curriculum, which sets

out all four key stages, right the way through primary and secondary school. Children will acquire an escalating level of knowledge at those four key stages. Those are exactly the tools that they will need to cope with what the demands of e-safety will be for them. There is also a need to provide teachers, as well as parents, not just with the information but with the confidence that what they are doing actually works. We must back that up by having any inspection of a school look at whether, under its behavioural policy and under the computer curriculum, it is fulfilling that and whether the outcomes of children are being improved as a consequence.

We have worked with a number of organisations in relation to keeping children safe in education guidance, for instance. That looks at the whole of safeguarding. We have worked with the NSPCC, Childnet and others to make sure that we are developing both that and the computer curriculum in a way that will be impactful for every school. Of course, there is always frustration that we cannot have that level of consistency across every single school on an ongoing basis, but we have to keep working towards having as much of it as we possibly can. There is more that we can do through the new filtering and monitoring—which we may come on to—that schools now have to provide to make sure that we have that wholesome response, but ultimately it has to be a whole-school approach. We cannot see this as the domain of just one or two people in a school. Where it works exceptionally well, that is because everybody buys into it and they all make it their business, rather than seeing it as something for which the maths teacher, the PE teacher or whoever it is has to take responsibility.

Schools have a central role to play, but at the same time we need to improve the level of understanding and engagement of parents when children leave the school gate. We know that the rise of cyberbullying and other online threats does not stop at school—it can follow children into their bedrooms. That is where working closely with parents pays off in trying to provide a better response.

Baroness Quin: Some of our witnesses have argued for PSHE to be made a statutory subject on the curriculum. Is that something that the Government are considering or favouring?

Edward Timpson MP: We are actively considering where we go next in relation to PSHE and SRE, principally around quality and access. You will appreciate that we have a still reasonably new Secretary of State who has come into the role. It is her prerogative to look at this afresh, from her own point of view. However, we are keen to make sure that we make progress. When I have given evidence to other Select Committees in Parliament, that has been very much the message.

I do not want anyone to get the impression that somehow there is a closed view about what the right approach is. There has certainly been no decision by the Government about whether to make PSHE or SRE statutory. We want to continue to look closely at what the advantages of doing that would be, as well as at how we can improve the quality of the teaching. There is no point in having a wholesale change to either the

curriculum or the duties on schools if that is not backed up with a high level of quality of teaching and learning from which children will benefit.

Baroness Quin: Presumably, resources for training in schools will also be important in this.

Edward Timpson MP: That is right. We work very closely with the PSHE Association, which provided guidance on SRE for the 21st century, for example, in 2014 and a programme of study for schools to use in this area. We want to build on that, to learn from where we know that it works well and to give a greater prospect of other schools following suit.

Baroness Kidron: What proportion of schoolchildren follow all the key stages of the computing curriculum?

Edward Timpson MP: Every maintained school has to follow the national curriculum. If it is an academy, it has to have a broad and balanced curriculum. That should form part of the work that it does. What we are seeing is an increased use of that, either as part of the computer curriculum or more widely, around PSHE or life skills—whatever you want to call it.

Baroness Kidron: That is what I was getting at. A few young people have mentioned that some of the information that they require is indeed in the computer curriculum but that, if they do not take the subject at GCSE level, they do not have access to it. Is it all enshrined in the computer curriculum? Is it not in PSHE and so on at the moment?

Edward Timpson MP: If you look at all four key stages, there is an escalation of the type of skills that children will learn as they develop their understanding of e-safety and digital resilience. That is reflected in the national curriculum. The computer element is relatively new—from September 2014—so it is still bedding in. The important thing for me is that it starts from key stage 1. Speaking from personal experience, I know that children are going to spend more and more time living their lives through a tablet. More of their homework is done online. There are some fantastic programmes and tools available. I spend more of my life than I care to mention on Maths-Whizz and Abacus with my children. It is the direction that we know will be taking hold for the foreseeable future, so we have to respond to that—hence the change to the curriculum, to make sure that it is embedded at every key stage.

Lord Gilbert of Panteg: I have a follow-up question for Edward Timpson on monitoring and filtering, which he referred to. The department is going to strengthen the duty on schools to have effective monitoring and filtering in place. We heard evidence from a provider of a monitoring and filtering service, which was quite extensive. We were surprised at the extent to which the work done by children on school networks is monitored. He said that he felt that the department did not fully understand the potential of monitoring, yet you have raised it with us. Could you address that? Secondly, could you address the balance generally between society's duty to protect children and individual children's right to have some privacy? How can that be safeguarded, particularly in relation to monitoring but also more generally?

Edward Timpson MP: First, the reason why we recently changed the statutory guidance on monitoring and filtering was not that schools were not predominantly making the sensible choice of putting in those systems in the school environment, but that there was not any consistency that we could demonstrate that meant that every child in every school would be able to benefit from having those restrictions put in place. At the same time, we accept that we do not want to restrict children's opportunity to use the power of the internet, whether it be at school or at home. It is about proportionality and having an appropriate level of filtering and monitoring. That is why we have worked with the UK Safer Internet Centre to put out some guidance to schools about where that level should be. Ultimately, each school will come up with a different solution that works for it and its cohort of pupils.

I do not profess to have the technical qualifications to understand the complexities of how this works in practice, but I know that more and more sophisticated solutions are coming on to the market. As a department, we probably need to understand more about what those options are, so that when we provide schools with either signposting or additional information about some of the routes that they can take we have a full understanding of the implications. I have seen the monitoring and filtering systems that the schools in my constituency have in place, which are pretty impressive and far reaching. There is still a bit of an information gap between that and what parents know about how they can supplement or complement it at home, so that a child is getting a consistent message. That does not prevent them from having the privacy you spoke about in their own engagement at school.

A problem in a number of schools that we have sought to address is the iPhone or the tablet coming into school, forming far too much of children's activities during the school day and being used inappropriately for some of the bullying and harassment that we know goes on, sadly, on the back of it. That is why we have strengthened the powers of teachers and head teachers to confiscate, to remove material and so on. We need to get the technology balance, but it is also about how teachers still interact with pupils, so that the internet does not become a battleground between them and becomes a place where they can do business together and enhance their opportunities to learn.

Lord Gilbert of Panteg: So your guidance covers all of that. It gives advice to schools on that balance.

Edward Timpson MP: It does. We have worked with the UK Safer Internet Centre on that guidance. Of course, technology is moving so fast that we need to make sure that it remains relevant and ensures that schools are making good decisions about what is appropriate for them and their cohort of children.

Q132 **Baroness Benjamin:** This question is aimed at both Nicola and Edward. We have said already that it is widely accepted by all that increasing use of technology in schools can greatly improve academic learning, but we know that it is also a platform that can facilitate harm, including grooming, child abuse, sexualisation, racism, bullying, self-harm, radicalisation, trafficking, gang culture and FGM—the list goes on and on.

I am sure that you will agree with me. However, Hilary Cass, president of the Royal College of Paediatrics and Child Health, said that failure to tackle emerging problems with young people's mental health meant that the issue was now "a hidden epidemic". Some feel that that is partly due to the impact of the internet on children and young people, especially through social media. How important do you think it is to build up resilience in young people—Ed touched on this earlier—to harm from the internet? How are the Government tackling that important issue?

Nicola Blackwood MP: You have touched on something that is hugely important. However, one of the problems that we face is that the evidence is not as robust as we would like it to be. The last serious prevalence study of mental health and internet use was done in 2004. If we think about what was going on with internet usage and young people back then, Facebook and YouTube had not even started, so that is not a good platform for us to base policies on.

The Chief Medical Officer did an annual report into mental health in which she investigated a lot of these issues. Her findings are that, while there are a lot of positive influences, as you say, bullying and repeated exposure to negative influences are also there. However, she found that prevalence rates do not seem to be increasing, possibly because of greater awareness and safety training. Her recommendation was that, because of the weakness of evidence, we need to do a thorough prevalence study to find out exactly what is going on and what the link is between usage and mental illness. We have commissioned a prevalence study, which will estimate the extent of mental ill health in the two to 19 year-old population. Publication is on track for 2018. It will give us up-to-date and comprehensive information—including on cyberbullying—for the first time. We have never had any proper health information on that, so this will be a step change in how we deal with it.

However, we cannot wait until we have that study to take any action, so there are steps that we have taken in the meantime. We have something called the *Five Year Forward View for Mental Health*, which was published in February. That is the Government's strategy for how we are going to transform mental health services in the UK, because we recognise not only that financial investment needs to go in but there needs to be a lot of restructuring. One of the strategy's recommendations was that we needed to have significant investment in research across mental health. The research document will come out in February, but we are already investing £70 million in mental health research specifically, because we recognise that this is an area where we need to make progress and to do so urgently.

In addition to that, of course, we recognise that we need to change areas like stigma. We have invested £12 million in Time to Change, which is the Government's flagship campaign on ending stigma for mental ill health and making sure that, if people have mental illnesses or challenges with cyberbullying and so on, they come forward for help. There is a specific strand within that for children and young people, which has used social marketing and online mechanisms to make sure that it is more effective. We are waiting for the evaluation of that at the moment.

We are also funding two other programmes I would like to draw the Committee's attention to. One is Rise Above, which is—exactly as you said—a resilience programme that targets young people and addresses different risky behaviours, to try to give them different strategies to manage those behaviours. It is run through Public Health England. We are looking at ways in which we can strengthen that going forward as a particular strand of work. The second goes back to Baroness Quin's question about resources—not just for teachers, but for health professionals, families and volunteers. It is called MindEd and is an e-learning platform that includes a module about digital risks to mental health, such as the creation of online identities and cyberbullying. It gives an idea of how to build digital resilience, not just by referring to relevant services but by offering direct help. The service was co-designed by young people themselves. That is why we have confidence in it as a useful service to have put in place.

Baroness Benjamin: When will it start?

Nicola Blackwood MP: It has already started. It is operational.

Edward Timpson MP: In fact, I met the MindEd leading group last week or the week before. I recommend that the Committee looks in more detail at the work that it is doing, because it is excellent and has some very impressive findings.

I will add one or two points. You asked what the Government are doing to try to address these issues. Nicola set it out from the Department of Health's perspective. We know that 72% of 12 to 15 year-olds have a social media account. There is a particularly large uplift around the 10, 11 and 12 age bracket, as you would expect, but it is still a significant increase on where we were only a few years ago. We know that that group of children will access all that the internet has to offer, unless there are opportunities for them to learn what they should or should not do. Are they getting the right filtering put on at home, as well as at school, and so on? One consequence of not doing that, of course, is the pressures and new threats that the internet poses for children, which we did not have to cope with: cyberbullying; sexting, which is a big problem; and the sense of isolation that you can feel, without having anyone to turn to, if you are on the receiving end of abuse through the internet.

One area we are working on together as two departments—the Department for Education and the Department of Health—is trying to link schools much more closely to mental health services. We are currently piloting what is called a single point of contact, where a school is linked to a mental health professional. It can refer a child on to them, if there is a clear and acute need for it to do so, but that mental health professional can also help to train and educate staff in the school to spot some of the early signs that things may be going wrong. The early evaluation is very encouraging. We want to look at the potential of trying to spread this more widely, particularly in the context that the interaction of children with the online world is having a deeper effect on their emotional and mental well-being than perhaps we imagined only a few years ago.

In UKCCIS, there is a group called the education group. Through that, we have produced some guidance for governors of schools, who have a more and more influential role, to make sure that they know what they should look out for and what questions they should ask their head teacher and their staff to be satisfied that a good enough response is happening within the school. There is also some guidance specifically about sexting and how to handle that in the school environment, because that can be extremely difficult. We continue to fund a number of anti-bullying charities, including on online bullying, to work with schools to try to ensure that they have the best possible understanding of what they can do, whether it is peer mentoring or using some of the charities that will come in and work with children.

On supporting teachers, between 2012 and about 2018, we will spend about £7 million as a department to provide online resources to primary school teachers to understand how better to build resilience in young people, through the computer curriculum. We are also creating what we call master teachers; in fact, they already exist. We are training about 300 of those, who can be commissioned by schools to go there to help to train their staff in e-safety and how they teach that. Earlier, I talked about having a whole-school approach. There should not be just one or two people in a school who understand what to do. Everyone needs to be able to spot the signs and to work together to come up with a solution.

There is a whole host of different areas where we are trying to have influence in order to tackle these issues. I hope that I speak for all of us here when I say that we are under no illusions. We are still uncovering the scale and extent of the issue. That is why the prevalence survey is so important. It will really help us to bottom out where we are on this—whether our response is sufficient and whether there is more that we need to do to ensure that we are equipping our children with the skills that they need not just to survive the trials of life but to thrive.

Baroness Benjamin: One thing that we have not covered and talked about so far is the anxiety that children and young people have about using their tablets and phones all the time. They even get up at night-time to look at their phones, to see who is on there. A lot of people feel that that constant contact with the rest of the world has been detrimental to children's health and well-being. Do you advocate the use of time-limitation mechanisms from providers themselves? How serious do you think the risk is that internet use by children and young people may cause compulsive or habit-forming behaviour—even addiction? Do you think that children being on all the time will affect their mental health and behaviour patterns?

Edward Timpson MP: We are starting to see time-limited apps becoming available. That is really encouraging. I have no doubt that there is a correlation—others will tell me whether the evidence exists—between a child's usage of a tablet or other device and their ability to concentrate on a task.

According to Ofcom this month, eight out of 10 parents of five to 15 year-olds who go online feel that they know enough to help that child to manage online risks, but I am not sure whether I am encouraged by or

slightly worried about that statistic. As I said earlier to the Earl of Caithness, there are many parents who still have a lot to learn about the effect that their child's use of a tablet or being online for long periods of time has on their mental or emotional well-being. There may be products that help to time-limit a child's usage. I think that CBeebies goes off at 6 o'clock. You cannot watch it beyond that. Of course, you can record it, but that is a matter for parents. There is a reason and a logic behind that, which is that we need to try to have learned behaviour in children that will be beneficial to them. At the moment, we do not really have any parameters that have been set that are made easily available to those who want to set them.

Of course, it goes back to the question that this is up to parents to sort out within the confines of their own home. Speaking as a parent, I think that we should not let ourselves escape that responsibility. However, there is more that we can do to try to make it easier for parents to find ways to put in those limits, which we know can be effective in ensuring that children do not lose the resilience that we want them to have.

Baroness Benjamin: Are you saying that providers should assist parents?

Edward Timpson MP: There is more that they can do to put products on the market that enable parents, as well as others within the school environment, to have a choice about how they manage time online.

Baroness Benjamin: Have you found that addictive behaviour and addiction are part of the problem that we face?

Nicola Blackwood MP: The findings of the Chief Medical Officer's report in 2013 were that electronic media have "positive influences, such as improved spatial perception, faster information processing and the provision of useful tools to motivate learning", which we have all discussed here. However, she noted that there were also risks of "increased physiological arousal, decreased attention, hyperactivity, aggression, antisocial or fearful behaviour, social isolation and excessive use or 'technological addiction'", as you have mentioned, and that, in association with frequent or persistent bullying, children "have higher rates of psychiatric disorder". She said that exposure to bullying is "associated with elevated rates of anxiety, depression and self-harm in adulthood" and that "More direct harm may arise from websites that normalise unhealthy behaviours as lifestyle choices, such as anorexia and self-harm". However, she was very clear that the evidence in relation to this "is sparse and contradictory". That is why she recommended the prevalence study that we are now undertaking, to make sure that there is a robust evidence base for taking forward policy on this issue.

If it is all right, I would like to draw the Committee's attention to some work that Samaritans undertook in a consultation called Digital Futures, which you may have heard of. It looked at how people used online resources in relation to suicide and self-harm content. As well as the negative experiences that we must all be familiar with, the study highlighted using sites to build peer networking. Three-quarters of the people who took part said that they looked for support online. When we

consider the harms and risks associated with this, it is very important that where people—especially young people—look for help online, they are able to find the help that they need.

A lot of the work that we are undertaking in relation to this at the moment in the Department of Health is to make sure that safe routes for help are available. We have some adult projects such as Big White Wall, which is an anonymous peer support programme for mental health, but it is not available to young people at the moment. This is a very important route to go down, to make sure that there are safe programmes for young people when they seek out help online and that they do not go down the wrong route by accident.

Q133 **Baroness Kidron:** My question or area of interest builds on what Baroness Benjamin talked about. Joanna, I remember when you came into the House. In your maiden speech, you used a phrase I was taken with: "safe by design". The Committee has been trying to look at childhood by design, recognising that the internet is not very good at recognising that a child is a child. What can we do to do that, to get away from the idea of harm? Perhaps we should talk about what is proactive and what is defensive. A lot of the solutions are necessarily after the event. The things we have been looking at are guidance for designers, programmes for delivering maximum privacy settings and platforms not suddenly turning on your GPS when you update. Those are all things that could, by default, be better for children but not stop adults having free choice. Age verification is another obvious one. Would you like to tell us what you think about that? Do you think that it is an interesting avenue to go down?

Baroness Shields: I have been in the industry for as long as it has existed; I was in digital for 25 years. Safety by design was a concept that started to emerge in services where kids spent a considerable amount of time and there was concern that they would be exposed. Initially, that concern was primarily about grooming for sexual exploitation, but it became about exposure to all kinds of harms and criminals.

We undertook a bit of work in UKCCIS. Last year, the companies came together to deliver a safe by design guide for all developers. It has become a very good best-practice document and has established a conversation and a co-operation between the companies that had not happened before. More and more, multi-stakeholder co-operation is vital to ensuring that we protect young people online. No Government, company or police force can do all of this in isolation, because the boundaries of the internet do not exist by country. We find that the problems that we have here are often the same one that they are trying to address in other countries. Bringing together that global community was the idea behind the formation of WePROTECT, which we created. I am very proud of that. This Government led it. Now it has 73 countries and all the top industry participating, with law enforcement, major NGOs and charities—all bringing together their expertise to try to solve this major challenge, which is evolving and changing every day.

I find that technology offers us these challenges, but it also holds the key to the solutions. Recently, I have been encouraged about the direction of certain companies. For instance, in *Wired* magazine last month, there was an article for the first time about a company wholly owned by Google, called Jigsaw, and the technology applications that it is developing to solve all kinds of problems. One was a redirect method. When someone was looking for extremist content, it delivered a credible news source or an article that was a counternarrative to that. It has developed the intelligence of that and is testing it. It is showing real promise. It has also developed cyberbullying detection and response mechanisms.

Technology is what got us here. I believe that it is also what can help to solve these problems, but it takes co-operation and Governments raising the issue. Reports like this one will bring the issues to the fore and encourage people to co-operate and to develop products that address these challenges. Whenever somebody is depressed and suicidal, they are exhibiting behaviours that are common to all other people who have that affliction. They are suffering. There are clues you can pick up. I was encouraged recently to hear that Facebook had developed a mechanism to identify young people—or any people—who might be at risk of suicide and to try to intervene. You do not need to know who that person is—you just need to understand what is going on. Then you can refer it to the proper authorities and get help for that person. The same applies to self-harm, anorexia and all kinds of things.

When you are connected to a device, it is an uncontested space out there. You can find people who will encourage you to harm yourself and to take the dreadful step of suicide. That is really scary, but the technology exists to recognise those patterns and to connect the dots. We have an enormous opportunity. There is a social responsibility for all the people involved in this, for Governments and for companies to come together. That is the idea behind WePROTECT. That is what is driving the strategy.

Baroness Kidron: Do you think that that idea and that responsibility extend into something slightly broader, which is about wellness and a certain sort of community care for children that means that they are not oversharing, even though it may be in the business interests of a social media site to have them share, by having privacy settings set at high or by not having easy or automatic access to GPS, for example—I am not making specific proposals—so that it is not identified where they are? Do you think that that duty of care, which is now established around very crucial and agreed harms, should go into a broader sense of what we all agree about childhood?

Baroness Shields: That comes from the communities, the schools and the work that we are doing around digital resilience to help people to understand the landscape they are living in. We used to teach kids to avoid strangers and how to cross the road. We still need to do all of that, but now we need to explain to them how to navigate a very complex, evolving and incredible world out there, which has its risks and harms. We need to give them the information so that they can be confident and

develop the independence to make the right choices. It comes from that direction as well.

Everyone has a role to play in this. When it comes to the safety and well-being of children, everyone—government, industry and charities—needs to up their game. We all need to do more, because society is evolving in a way in which it has never evolved before. It is almost the largest social experiment in history. We have never had this much change in such a short period of time, to the extent that young people are connecting with people all over the world. It requires all of us to increase our awareness and efforts and to work together, because no one can solve it on their own.

Baroness Kidron: Do you think that more work should be done by the sites that have hundreds of thousands of underage users, whether or not their parents tick or they lied about their age? One young boy said to me the other day, "How come they know that I want red sneakers but they do not know that I am 12?" That was a very valid question. Do you think that more resource and technology should be put in by those companies that say they do not have underage users but clearly do?

Baroness Shields: The very established companies are getting better at that and at recognising the patterns that kids use—the things that they say and the way in which they act—to figure out that they may be underage and to suspend accounts and various other things. The problem is that the more established platforms are the ones that we and their parents use. They do not use those any more—they use the more upstart types of products, which may not have the expertise or maturity of those companies that have those policies in place. The kids tend to go to the new—the bright, shiny object that everyone else is using. The more established platforms can identify young people who may be saying that they are an age that they are not.

There is so much opportunity in this area. Just last week, I was in China. We ran across a company called Musical.ly, which has 130 million users. I found its ethos very interesting. It has an ethos that says, "Do not judge me". I thought that was really interesting. There it is, building a product that says, "I am me. I am great. Do not judge me". It creates a certain ethos on the product that is different from that on other products. That is exciting. That is leadership. That is like saying, "We do not tolerate bullies here". There are some interesting developments.

Baroness Benjamin: We have "Don't drink and drive", especially at this time of the year. In the past, we had the Green Cross Code. Do you not think that there should be some sort of campaign of public awareness? If you are a responsible parent, you go to the school and find out what is going on, but there are other people who do not know or care—or even people without children themselves. Should some resources not be given to public awareness that you have on your screen and comes up, so that it becomes almost second nature to people that we should be aware of and take part in this world that is evolving before us?

Baroness Shields: That is a brilliant idea.

Baroness Benjamin: So you will put money into it.

Baroness Shields: When you used to put money into an advertising campaign, there were three or four newspapers and a couple of television channels. Now it is so widespread that we almost need that kind of communication to come from the platforms themselves. That is where kids are spending their time.

Baroness Benjamin: I know. A lot of the people whom we have met have said that they are doing that. We have been to see Google and Virgin. Everybody says that they are doing lots of good things, but you have to be a user of that particular service to find out. I am talking about a general advert so that people become aware, such as "Clunk Click", which everybody used to say, or "Don't drink and drive"—do not do that.

Baroness Shields: "Stranger danger".

Baroness Benjamin: You need to have something that tells the public, so that it becomes second nature.

Baroness Shields: Of course—public service announcements.

Edward Timpson MP: We have done two recent national campaigns. One is the This Girl Can campaign, which is trying to encourage girls to feel that, if they want to play sport or to push the boundaries, they can. That has been hugely successful. We have also done one called the This is Abuse campaign, to highlight the fact that child abuse can happen anywhere and, if people are worried about it and want to make contact with a professional or to report it, to make very clear how they do that. There is always a place for a national campaign.

Through the UKCCIS board, we managed to cajole the four main internet service providers to commit to a significant sum of money to lead a campaign. However, we need to look at the impact of that and to consider whether we need to do something that is more of the ilk that you have described, because it can resonate in a different way. The response that you are getting is that we will take that away and look carefully at what we might be able to do.

Baroness Benjamin: Please.

Baroness McIntosh of Hudnall: I want to ask you a very quick question on the back of that point. When you say "we", it is quite hard to know whether you mean "we, the Education Department", "we, the Department of Health" or "we, anybody else". The really important thing that is emerging—certainly in the research we are looking at and the evidence that we have seen—is that we need to know that when you say "we" you mean all of you. Each of you—not just you, obviously, but each department; you happen to be in front of us—must not only be aware of what other departments are doing in this field but you must join up the dots and make a coherent campaign that goes right across, so that we are not saying, "This is a Department of Health issue, because it has public health in the title", or whatever the reason is, or, "This is an education issue, because it has schools involved in it". Can you tell us how much genuine collaboration and joint thinking goes on between your departments—and any other department of government—that will begin to create coherent policy around these issues and not just say, "This belongs with education. That belongs with health"?

Edward Timpson MP: First, we have a natural forum, through the UK Council for Child Internet Safety, for us to work not only across government but across the industry and the charitable sector. That has proved a very productive way of meshing all our collective effort, not just in government but much more widely. I can reassure you that we are not strangers. Joanna and I met yesterday—

Baroness McIntosh of Hudnall: Not for the first time.

Edward Timpson MP: Not for the first time.

Baroness Shields: We co-chair the board.

Edward Timpson MP: That was the Inter-Ministerial Group on Child Sexual Abuse. There are lots of opportunities for us to work together on issues. As Joanna said, we cannot work in isolation. We can come up with a great initiative, but if no one else has bought into it and it is not complementary to what everyone else is doing, it will wither on the vine and you may get limited impact. We absolutely understand that message. Much as we would like to guarantee that the three of us will be here this time next year, we cannot. However, I think that that has resonated across government. The Prime Minister has a good track record of wanting to make sure that there is an inclusive government approach to these types of issues. I expect that to continue.

Q134 **Lord Sherbourne of Didsbury:** I have a question for Baroness Shields on the Digital Economy Bill. It is really a factual question, so that I can be absolutely clear in my own mind about what it is going to do. I have written it down, so that I get it absolutely correct. Will the Bill provide for ISPs to be legally required in certain circumstances to block websites? Is it the BBFC that will have the power to require ISPs to do that? Will any other body have that power as well? In what circumstances will they be required to block content?

Baroness Shields: To clarify, it was a manifesto commitment to ensure that age-inappropriate content—pornography—was not available to children under the age of 18. We were trying to harmonise the online world with the offline world. These proposals have been built into the Digital Economy Bill. The reason that the BBFC is involved is that the same types of ratings that we use to rate movies and films in the cinema should be applicable to this area. It is the right choice for that. Under the new Bill, it will contact a company that is delivering age-inappropriate material, if it does not have age verification that is robust, and notify it of that. If, for whatever reason, government is not able to resolve that with the company, it will be recommended that the ISPs block that content.

Lord Sherbourne of Didsbury: Recommended, not required.

Baroness Shields: It is required. If it does not offer age verification that is robust and suitable, it will be required.

Lord Sherbourne of Didsbury: Under law.

Baroness Shields: That is right. That is what my honourable friend Matthew Hancock announced last night.

Lord Sherbourne of Didsbury: The only regulator that will be able to do that will be the BBFC.

Baroness Shields: The BBFC is the body that will say that it does not comply.

Lord Sherbourne of Didsbury: That is very helpful to know. As a supplementary: presumably, user-generated content that is uploaded cannot be blocked.

Baroness Shields: The Bill covers ancillary services. There was a question about Twitter. Twitter is a user-generated uploading-content site. If there is pornography on Twitter, it will be considered covered under ancillary services.

The Chairman: Perhaps we ought to ask about the audiovisual media services directive as part of this. Are you concerned that the provisions of the directive could potentially lower standards for video-on-demand content? Have you recommended, or will you recommend, changes to the directive to ensure that it does not lower standards?

Baroness Shields: We believe that the proposals in the audiovisual media services directive strengthen, rather than weaken, the requirement for protection of minors by extending the amount of material that is required to be restricted to minors. That includes a requirement to ensure that there are appropriate measures in place to protect minors from harmful content, proportionate to the potential harm, including age verification for pornography. The requirement in the proposal ensures that the most harmful content, including pornography, must be behind age verification tools and other technical measures. We believe that moving to the system proposed by the AVMSD will mean that far more content is placed behind restrictions on on-demand services—which, after all, is where children view most of their content. That will help to create a safer online environment for children.

So far in the negotiations with member states, they are supportive of the proposed changes to protect minors online. We would resist any suggestion of lowering the standards on age verification requirements. The proposals cannot lower the standards in the UK. Member states are free to impose stricter measures on services in their jurisdiction than are required by the directive, hence our amendments to the Digital Economy Bill.

The Chairman: Thank you. We have got that on the record.

Q135 **Baroness Kidron:** We seem to have been told by almost everybody in the value chain on the industry side that self-regulation is a marvellous thing. We have been told by almost everybody else, whether it be academics, charities or teachers, that self-regulation is not sufficient, because we are seeing an ever-increasing number of children with some element of harm, risk or anxiety—however broadly you want to do it. From your perspective, is self-regulation working?

Baroness Shields: It is such a broad question.

Baroness Kidron: I know.

Baroness Shields: In this rapidly changing world, by the time you deliver legislation to two Houses of Parliament and get to Royal Assent, things have moved on dramatically. It takes a long time to regulate. The first choice is always to explain to the industry, "These are the problems that are created by people on, and technology used by, your platform", to have those conversations and to impress upon it the importance of that. The ultimate hammer, of course, is regulation, but it takes a long time to move through that process.

We need to get to a place where we can express a concern and get a response. For instance, three years ago, we went to Google and Microsoft and explained, "When you search on your platforms, there is an auto-complete function. If you are searching for child sexual abuse imagery, you get an auto-complete and it is easier to find it". The minute they saw that, they thought, "We are going to change that". They went back and changed it. Then they started to look at the patterns in the search terms that people use and adjusted their technology to break the chain and the links to child sexual abuse content. We found from working with them—from opening up and sharing the problem with them—that the solution that they developed was far better than anything we could ever have legislated for. Now we feel that it is really hard to find this stuff on the open web. There are other challenges in peer-to-peer networks and the dark web, which we can go on to, but I wanted to illustrate how this co-operation works.

If we had developed legislation for this issue, we would have come up with something that was technologically inferior to what they developed. They developed something that was custom-tailored to the technology on their platform, so it works with their platform. Every provider needs to do the same. Microsoft did the same. The last statistic that I heard from Google was that it had an eightfold decrease in people searching for this content. That is a big improvement. We will never solve it completely, but the onus is on government to share the depth of the problem, to bring the evidence forward and to ask for solutions. If that does not work, it is fully within the rights of government to go down the path of legislation, but we need to do a better job of explaining what we need. So far, when we have raised these issues, in general, we have got co-operation. We are having robust conversations on online extremism. We are getting far more co-operation than we could legislate for, because you cannot legislate for how to do this on everybody's platform.

Baroness Kidron: That is a fantastic answer. I want to ask two very precise questions around it. In that case, do you think that enough money, resource and attention is given from government to independent evaluation of what is going on, so that you can have these conversations in a very informed way? Secondary to that, one thing that we keep hearing from young people is that their concerns are nowhere in this conversation. Government is pursuing things on radicalisation, pornography and so on. In the meantime, they want to know about profiling and the right to be forgotten. Their feeling is that they have overwhelming amounts of information. They have all sorts of other issues. If you are going to guide these conversations, where is the children's voice in that—in a very real way, not in a tick-box way?

Baroness Shields: To take the first part of your question, we have much more power and influence when we bring a community together. WePROTECT having 73 countries, everybody involved and everyone saying the same thing raises this to a crescendo, where we get action. As I said earlier, we have been very successful so far—although we are nowhere near finished—in combatting child online abuse and exploitation. We have been reasonably successful in other areas as well.

However, you have to organise this in stacks and to have co-ordinated effort, because every Government tends to go to industry individually. It is death by 1,000 cuts, really. I remember working in industry and having 32 data protection officers. In Germany, they all had an issue at the same time. It was impossible for companies to prioritise and deal with these issues. It is incumbent upon us to organise and to deliver the highest-priority challenges in an effective way, with evidence. We need great academics—I am looking at Sonia—and their support to deliver a robust evidence base, so that we can show how this is harming people in society and what we need done. If you are not a technologist and do not know how the products work, that is far better than trying to come up with ideas or a solution yourself. A solution will never address the problem in the way in which it needs to be addressed, because you have to understand fundamentally how a particular product platform application chatbot works.

Nicola Blackwood MP: You have made an incredibly important point about the involvement of young people in the development of policy. One of the core principles that we have in the Department of Health—based on Future in Mind, which is about the future of young people's mental health—is what we call in our incredibly Department of Health jargony way "co-production of policy". Basically, it means that we include young people in the development of our mental health policy. I encourage the Committee to look at the Youth Parliament Select Committee's report on young people's mental health, which was incredibly professional and put a lot of Select Committee reports from this place to shame. It included commentary on cyberbullying and a lot of other issues. We responded with a debate in Parliament, which was of very high quality. The emphasis that it put was on involving young people in development of policy, to make sure not only that their views were taken into account but that they were included in evaluation, rather than just left at the door once they had had the initial input. Sometimes, you need that as it goes along. I encourage you to look at that report.

Edward Timpson MP: For completeness, I alert the Committee to the fact—which you may already know—that the Children's Commissioner is doing a large piece of work with children and young people about what they want from the internet. It is an absolutely valid point that we should not assume that we know what sort of world they want to inhabit online. The more we can involve them in the development of where it goes next, the more likely it is that they will embrace it as something they have ownership of, rather than something that is done to them.

Baroness Shields: It would be brilliant to have a Youth Parliament on these issues. I would be happy to help you to organise that.

Baroness Kidron: There are a number of things going on. If I may, I will let all three of you know. There are various youth groups that are trying to organise around this. It would be wonderful if government policy reflected the views that they are expressing, which are quite different from our own views.

Baroness Shields: We need to do this in our country, but we also need to do it globally. We need to bring all that knowledge to the conversations that we have around safety on these platforms.

Baroness Benjamin: It is a world that we are all discovering together. It is about common sense, everybody's point of view and throwing your mind beyond the horizon and coming back. Far too often, we leave things and then react.

Baroness Shields: That is right.

Baroness Benjamin: We must think ahead and have that ability. It is great to listen to children's voices, but they do not necessarily know what the implications are. They do not have that experience or wisdom. Children may say, "I want chocolate and crisps every day of my life", but it is not good for them.

We also have to look at things differently, in a way that reflects what might happen. It takes wisdom and visionaries to come up with a solution that deals with the problem. As we all agree, this is new territory. It is like Christopher Columbus going across to find the new world. That is what we are after. Even though we have discovered things in between, we have not quite got there yet.

Nicola Blackwood MP: The Information Commissioner once gave evidence when I was a Select Committee Chair. He said, "It is not completely new territory. If you apply the principles of safety that you apply in the real world to the digital world, that is a very good, common-sense place to start". You would not go into a tube station and give a stranger your home address. You would not take off all your clothes. You would not enter into conversation with big groups of people or go home with anybody. We have many more of the skills than we think we have. Sometimes, we talk ourselves out of the skills that we have by thinking that the innovative package everything is in means that we do not know how to keep ourselves and our children safe. If we applied some of the common-sense lessons that we all know from the real world to the digital world, we might find ourselves feeling a lot safer and calmer and less mentally stressed—says the Health Minister.

The Chairman: Very good.

Q136 **Baroness McIntosh of Hudnall:** I can see that we are getting near the time limit. There is the whole issue of data protection, on which we touched in the last few minutes in relation to some of the things that have come up. You mentioned the question of how data is used and shared. The increased profiling by media companies of the people who use their resources opens up a whole range of possible vulnerabilities. Can you tell us quickly—or write to us subsequently—about where you think there is more work to be done on the issue of data protection specifically for children, particularly in relation to how they can be better

equipped to understand what is being done with their data? That might include, for example, terms and conditions, which we all readily click on. I know that we all do it, but they do it. There may be more accessible ways—to use an overused word—of making clear to them what they were doing when they clicked on those. Also, do you have anything more to say about the role of the Information Commissioner's Office in this area? Are there powers that reside there that could be strengthened? That is a lot to ask you when you have about two minutes left. If you cannot say it now, maybe you can write to us.

Baroness Shields: I have prepared answers to four questions on this. I would be happy to hand them over straightaway.

Baroness McIntosh of Hudnall: It is the Chairman's call, of course.

Baroness Shields: I will leave the door open. If you want to probe it further, you can get in touch with us.

The Chairman: That is very kind; thank you very much. We come to our final question, from Lord Caithness.

Q137 **Earl of Caithness:** Minister, could you also write to us on what lessons you have learned from the work that the Australians and Canadians, in particular, have been doing? They have done a lot of good work.

Given everything that the three of you have said this afternoon, I think that you have made a very good case that there should be a one-stop-shop in government, with one Minister, where all the information that you have imparted to us can be found. Will you implement that, please?

Baroness Shields: We will definitely take it back.

The Chairman: We talked about co-ordination earlier, but there is that point, too.

Earl of Caithness: Do you think that it is feasible? Is it a sensible proposal?

Edward Timpson MP: It is fair to say that Baroness Shields is the government Minister for Internet Safety. I do not remember there being a government Minister for Internet Safety, who was specifically tasked with that in government, until Baroness Shields came along.

Earl of Caithness: Understood.

Edward Timpson MP: Of course, there will always be other departments that need to feed into that role. That is where there has to be a cross-government approach.

Earl of Caithness: Should all this information not be collated in a one-stop-shop in government where everybody can get it?

Edward Timpson MP: The outward-facing body that we use in order to do that is the UKCCIS board. Joanna, myself and Sarah Newton from the Home Office co-chair that board. That is a place where it all comes together. We will take away the suggestion and see how it fits in with the machinery of government.

Baroness McIntosh of Hudnall: It would be fair to say that that is not an aim that resonates widely among the public. I am sure that excellent work is being done—we know that it is—but it is partly about profile, is it not? Do you think that that body has the kind of profile now, or could develop the kind of profile, that would meet the challenge that has just been put down—of finding a one-stop-shop that people know about?

Edward Timpson MP: I have been on the board for over four years. It has gone through a number of iterations in that time. Initially, it was much more about liaising and working closely with the industry to try to improve our response to filtering, default systems and so on. We may be moving into a new phase, which is why we now have an education group and a digital resilience group. We are looking at how we can be more outward facing as a board—not just as government, but as others who will come into contact with parents, schools and other parts of the community—so that a clear and single message comes out of that. As for government more widely, Joanna does an excellent job of articulating what the Government's view is. We will continue to make sure that we support her in doing that.

Baroness Quin: There is something that I want to raise. Again, perhaps you can write to us about it if you have any further thoughts. When we met young people today, one of the messages that came over to me very clearly was their concern that, if you put something online unwisely at a really young age, you get saddled with it forever after, even to the extent that it may affect your future employment prospects. I know that we have not discussed the right to be forgotten much, but I wonder whether there is something particular that can be done around that subject to protect young people under a certain age.

The Chairman: Do you want to have a quick go at that one, Joanna?

Baroness Shields: Yes, quickly. We have talked a lot about digital resilience, whether it makes sense to build that into the curriculum and how we accomplish that. I take your point about people not being aware of UKCCIS. We need to raise the profile of the organisation, because the work that it is doing is multi-stakeholder, co-ordinated work. It is looking at this very issue—how we explain the issues to young people so that they can make informed choices and go out into the world with the digital independence that they need to relax, to lose the anxiety and to be confident in going forward in their lives. It is a huge issue. It could not be more important at this moment in time. I have a 17 year-old son, so I know exactly what you mean. This is what they are concerned about.

Baroness Kidron: I do not want to end on a difficult note. I know that UKCCIS does remarkable work and has wonderful people in it, but one slight issue that I have is that some of the things young people are asking for—for example, a one-stop-shop to report abuse, to get answers and all of that—are things that industry is somewhat reluctant to do, for all sorts of brand reasons. If the Government only have UKCCIS, where they all sit, where is the pressure from government on industry? Where is the answer for those young people on some of the things that they want, which fundamentally attack the business model

and say, "Hey, we need a little bit more insurance and care about our childhood"? There is a slight complication about where government sits with industry and where government policy is separate from industry.

Baroness Shields: I understand.

The Chairman: We may not be able to resolve that immediately.

Baroness Shields: If a young person has a particularly problematic piece of content and it is on multiple platforms, it is heartbreaking that they have to go through the resolving mechanism and to contact each company individually to report it. That is really tough. It is not fair.

Baroness Kidron: Yes.

Nicola Blackwood MP: One of the challenges that we have had historically is that the evidence base around the mental health impacts is not strong enough. That is why the prevalence study is really important, so that we have that robust and unarguable evidence base.

Baroness Shields: That is right.

Nicola Blackwood MP: Around cyberbullying and bullying, in particular, one concern that we have in the department is about the sense of no escape, which has been linked to higher suicide and self-harm rates. It used to be that if you were bullied in one school you could leave, go to another school and leave it behind. You cannot really do that now. However, if we do not have the robust evidence base, it is very difficult to make arguments that are perhaps commercially difficult. I know that I keep talking about it, but I think that that will be a real game changer going forward.

Baroness Shields: When will it be finished?

Nicola Blackwood MP: In 2018.

The Chairman: Great. It is 5 pm. We went way over time. We are extremely grateful to you for staying with us and sharing all those thoughts. Telling us that we are part of the largest social experiment in history is wonderful, but you also made the point that all of us must up our game in relation to children. That is a fundamental point that was clearly shared by all three of you. Thank you very much for joining us and keeping us safe.

Baroness Shields OBE, Parliamentary Under Secretary of State for Internet Safety and Security, Department for Culture, Media and Sport – supplementary written evidence (CHI0067)

Thank you for inviting me to give evidence to the Committee on 29 November – I welcomed the opportunity to share the Government's action on child internet safety with my Hon. friends, the Minister of State for Vulnerable Children and Families at the Department of Education, and the Parliamentary Under Secretary of State for Public Health and Innovation. I undertook to write to you on a number of matters which arose during the hearing.

Data protection and children

I was asked about work done on the issue of data protection specifically for children. The Data Protection Act 1998 is the UK's data protection legal framework. It will be updated by the General Data Protection Regulation (GDPR), which will apply in the UK from May 2018. GDPR will introduce a higher threshold of data protection to all individuals, including children, by providing:

- Easier access to individuals' own data. Individuals will have more information on how their data is processed and this information should be available in a clear and plain language;
- A right to data portability. It will be easier to transfer personal data between service providers;
- A clarified "right to be forgotten". When individuals no longer want their data to be processed, and provided that there are no legitimate grounds for retaining it, the data will be deleted; and
- The right to know when personal data held by companies has been hacked. For example, companies and organisations must notify the national supervisory authority of serious data breaches as soon as possible so that users can take appropriate measures.

Regarding the profiling of online activity, marketers must not knowingly collect personal information from children under 12, for marketing purposes without first obtaining the consent of the child's parent or guardian. Several sections of the UK Advertising Code contain rules relating specifically to children, including prohibited advertising of age-restricted products such as alcohol, gambling and electronic cigarettes. Marketing communications addressed to, targeted directly at, or featuring children must not contain content that is likely to result in their physical, mental or moral harm.

Equipping children with information about online privacy

I was also asked how children and young people can be better equipped to understand what is being done with their data. There is a range of online resources funded by Government, industry and the third sector that are all

relevant to helping children think about their privacy - and what happens to the information they share online. To exemplify:

- The Government published a guide for parents and carers of children using social media, with practical tips about the use of safety and privacy features on apps and platforms, and conversation prompts to help families talk about online safety. (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/490001/Social_Media_Guidance_UKCCIS_Final_18122015.pdf.pdf);
- The UK Safer Internet Centre delivers a wide range of activity to promote the safe and responsible use of technology (http://www.saferinternet.org.uk/advice-centre;.
- Advice to parents is also important. Government has funded ParentInfo (http://parentinfo.org/article/your-child-s-digital-footprint), a free service for parents, which helps them show their children how to use the internet and mobile devices safely and appropriately. Internet Matters, funded by the major UK Internet Service Providers (BT, TalkTalk, Virgin and Sky), Google and the BBC, also offers relevant advice on how adults can support children learn to protect their privacy. (https://www.internetmatters.org/issues/privacy-identity/)

We also work very closely with industry to support the safety and privacy of children and young people by providing privacy tools and advice on how to share and protect their information. While we keep these developments under review, good progress is being made for example:

- On Facebook, by default, anyone under 18 has more restrictive privacy settings: they do not have public search listings; their email and phone number will not be set to "public"; and messages from adults who are not their friends are filtered out of the minor's inbox;
- On BBC services, children are encouraged to ask for their parents'/carers' permission before creating a user account, and to make sure their parents know they will be using the message boards;
- Disney Club Penguin run an "It Starts With You" campaign on online safety on their platform to encourage children to spread positive behaviour. This includes tips for parents and children, and an online safety quiz in the virtual world;
- Moshi Monsters has developed activity cards with The Vodafone Foundation to help parents educate children about online safety;
- All major social media companies offer user-friendly privacy information in their Safety or Help Centres, and often run specific awareness campaigns within their platforms (e.g. Facebook's Privacy Checkup).

Baroness Shields OBE, Parliamentary Under Secretary of State for Internet Safety and Security, Department for Culture, Media and Sport – supplementary written evidence (CHI0067)

Child internet safety lessons from Australia and Canada

I undertook to write to you about lessons learned from the work on child internet safety by Australia and Canada. We are always ready to learn from the good practice of other countries. For example, I know my officials just recently met with the Chief Executive of Netsafe in New Zealand to hear about their new statutory role to keep children safe online. I shall ask my officials and also my ministerial colleagues in the Department for Education and Department of Health to look into the successes of Australia and Canada to see what further we can learn to support child internet safety in the UK.

Duty of social media companies to protect children from harm

I was asked about the duties of social media companies to protect children from harm, and the use of social media by under-age users. We consider social media companies and interactive services (e.g. social networks, messaging, Q&A sites, interactive games, cloud services or ephemeral messaging services) should do everything possible to protect children and young people from harm.

Different sites have different age limits - on many social media sites, users should be at least 13 years old. Social media sites encourage other members of the community to report accounts they believe are held by underage users, and take other actions to discourage underage users. For example, on Facebook, parents can request the closure of accounts opened by their children. The account, once closed, cannot be reopened.

Finally, I would like to reiterate that this Government takes these issues extremely seriously. Government will continue its regular dialogue with industry through the UK Council for Child Internet Safety (UKCCIS), where we work with charities and others to stay up to date on the effects of children's exposure to the digital world, and innovative solutions to address this. This is an important check and balance within the Government's multi-stakeholder approach. We will continue to work together closely with industry and encourage the key players to keep their safety practices under review, updating them to reflect children's media consumption trends and technology advancements. Through the efforts of UKCCIS, we also expect them to continue to promote a 'safety-by-design' culture among the tech community to ensure they understand the reputational and business benefits of having safe platforms, and to regard upholding user safety as key to their long-term success.

I hope this information is helpful. I am copying this letter to the Clerk of the Committee and to Edward Timpson, the Minister of State, and Nicola Blackwood, the Parliamentary Under Secretary of State.

6 December 2016

David Miles Consulting – written evidence (CHI0012)

A UK Perspective

1) The UK is widely acknowledged as a global leader in the field of online child safety. That leadership is based on centres of excellence, expertise and a proven track record of best practice. We a fortunate to have a disproportionately large concentration of world class organisations and initiatives including UKCCIS, CEOP, IWF, NSPCC and WePROTECT Global Alliance. Through Ofcom, the LSE and other academic research bodies, for the most part, there is a sound, evidence-based approach to the digital lives of children and young people.

2) Since the beginning of the new millennium, successive UK Governments have made child online safety a priority. A strong charitable base, responsive industry and campaigning approach from the press and media, have combined to make the UK progressive in many areas. In 2008, the UK Government commissioned an independent landmark report that has done much to shape the policy discourse to date. Professor Tanya Byron's 'Safer Children in a Digital World' made a series of important recommendations, all accepted by the government. One of the most significant of these was the establishment of the UK Council for Internet Safety (UKCCIS) in 2010. This voluntary, multi-stakeholder organisation, has acted as a focal point and through its working groups delivered a wide range of progressive initiatives, that deserve greater attention and credit. Any inquiry into children and internet would not be complete without a better understanding not just of the extraordinary progress made through these groups but also the UK's relative global position in the field of child online safety.

3) Let's start first with UKCCIS and the working groups. UKCCIS remains a unique body and internationally is seen as a model of best practice. Other countries do have convening councils or bodies but few have the voluntary, multi-stakeholder ethos that has enabled the UK to deliver genuine progress in the field of child online safety. Key to that, are its working groups in areas like education, research, filtering and social media. Over the years, the working groups have evolved and varied in number, often in response to specific challenges or needs. In addition, these working groups have published a range of policy reports and expert-moderated documents that have provided valuable insights and guidance to the wider stakeholder community.

4) A good example of the focus that UKCCIS brings to both to UK policy and best practice in the field of child online safety, is in its approach to filtering. In the last few years, no other democracy has implemented such a comprehensive range of filtering tools and guidance for its citizens. This required the UK's four leading ISP's (BT, Sky, Virgin Media and TalkTalk) to deploy a whole new generation of network-level filters to both existing and new subscribers in more than 19.6 million

households (85% of UK households). Significant investment was required to integrate these products seamlessly into their offerings. Along with £25 million parent portal called Internet Matters, funded by the same four ISPs, it represents a remarkable example of how industry can play a pivotal role.

5) Few countries have been bolder in their approach towards filtering. Apart from the costs, predominantly borne by industry, it has inevitably required dealing with a number of complex issues. For example, youth charities and advocates for freedom of expression were rightly worried about the impact of these new filters on online support services and resources. Vitally important to young people, there was a real danger that teenagers in particular, in seeking online confidential advice through web sites, would be blocked. The risks of overblocking or underblocking legitimate web sites could have significant consequences. The online gaming community, LGBT and sexual health charities felt particularly vulnerable. As a result, the UKCCIS Overblocking Working Group was established in September 2013. Its aim was to measure the impact of the new filters and calibrate them to be as proportional and age appropriate as possible. As its chair, I was able convene a wide range of stakeholder organisations, often with very different perspectives. Over an eighteen-month period and in parallel with the deployment of ISP filters, the group worked together to refine these filters and along with the charities find the right balance between protection and ensuring young people continued to get access to trusted online advice and guidance.

6) Through a series of working group meetings and workshops, the ISPs and mobile operators established a range of new services, enabling web masters and consumers to report mis-categorisation, overblocking or underblocking. This data enabled access providers to refine their filtering products, as well ensure overblocking was kept to an absolute minimum. Youth charities also worked hard to ensure vitally important online support services remained accessible and were kept informed of the working groups efforts on their behalf. This task was carried through into the UKCCIS Filtering Working Group and remains ongoing.

7) In addition, ISPs themselves sought feedback from their own users in terms of uptake and providing feature enhancements. Parents for example, can tailor ISP filters to reflect their families' values and priorities. 'Active choice' has done much to prioritise filtering and encourage parents to discuss internet safety in UK households. Independently reviewed by Ofcom, parents made it clear that they saw this new generation of ISP filters as an easy to use, set of new tools.

8) It's important to acknowledge broader UK industry efforts to filter age appropriate content. Since 2007, all UK mobile operators implemented default-on filtering of pornography on their mobile devices. From 2013, the BBFC provided an independent, voluntary Classification Framework for UK mobile operators filtering online content. The Classification Framework defines content that is unsuitable for customers under the age of 18 and is based on the BBFC's Classification Guidelines for film

and video. The Framework enables mobile operators to calibrate filters they use to restrict access via mobile networks to age appropriate internet content, including entire web sites, by those under 18. Open to webmasters, access providers and consumers, it includes a free appeals procedure and quarterly reports on the outcome of each case.

9) Concerns around children's increasing use of public Wi-Fi is being addressed through RDI's Friendly WiFi accreditation scheme established in 2013. More than 3,000 retailers and small businesses have now been accredited and the scheme is now being adopted in the USA and a number of other European countries.

10) It is important to note that the UK has persisted with these filtering policies in spite of considerable scepticism from other countries and some notable challenges in implementing national programmes of filtering. Australia's difficulties in mandating filtering for its citizens and the Germany's mixed results around age verification provide valuable lessons.

11) The growing encryption of browsers, websites, messaging services and many popular apps, is likely to make it increasingly difficult for parents to control or manage their children's activities online. Accessibility through gaming devices, TV's and the inexorable move towards the Internet of Things (IoT), will only serve to compound the problem.

12) The implementation of age verification for minors in relation to online sexually explicit content through the Digital Economy Bill, is a significant and timely step. However, if the balanced and collaborative approach used in filtering is anything to go by, it's likely to be robust and effective.

A Global Perspective

13) Most countries around the world share similar concerns to those raised through this inquiry. Indeed, one of the surprising attributes of the digital lives of children and young people, is that in spite of often diverse cultures and social norms, the way they use technology and the concerns of parents remain remarkably similar. The biggest variable is in fact the way adults within society respond to the needs of young people and their increasingly digital lives. The lack of a coherent global approach to child online safety is of major concern and this given an added urgency, as a growing global youth demographic emerges.

14) According to the UN ITU, by the end of 2016, 3.9 billion people (47% of the world population) will be using the internet. However, the really significant factor is that for this first time, nearly half of those accessing the internet are under 25 years of age. Coupled with a dramatic fall in the average age of access (in the UK for example, more than third of 3-4 year olds access the internet weekly) and it's clear that from an early age, children will be exposed both to the risks and rewards of an increasingly digital era.

15) Until now, most internet growth has been in countries with mature economies, robust institutions (government, law enforcement, education) and in digital terms (10-15 years) with time to adapt. However, in emerging economies, high-speed internet access is being deployed in a fraction that time (3-5 years), often against the backdrop of institutions ill-equipped to deal with the online risks and harms that children and young people may face. And once again, in the field of child online sexual exploitation and abuse, the UK is providing exemplary global leadership through the WePROTECT Global Alliance to End Child Sexual Exploitation Online.

16) Founded in 2014, by Baroness Joanna Shields, the UK brings that same collaborative blend of concern, funding and leadership to an issue that will require a global response if it is to be successful. It's probably the first genuinely global response to a child online safety issue and requires engaging with a new range of international and regional stakeholders, including UNICEF. More than 70 countries are already committed to the initiative and many, until now, have been focused predominantly on issues that have had a relatively limited digital dimension. Criminality, violent extremism and abuse always targets the vulnerable and will take the least line of resistance. The growing global pervasiveness of the internet acts as an accelerant to all these issues, its borderless nature, demanding a new response.

17) I chaired the Industry and Media Break Out Group at its 2nd WePROTECT Summit in Abu Dhabi (November 2015) and with Child Helpline International met representatives from all 17 priority countries through four two-day conference in Cairo, London, Nairobi and Paraguay. I have seen first-hand the impact of high-speed internet access on countries ill-equipped to deal with issues like online child sexual exploitation and abuse. There is a unique opportunity to get ahead of this emerging crime, by deploying new technologies, convening stakeholders and capacity building, particularly in countries with fast growing and often vulnerable youth populations.

Conclusion

18) The UK should be proud of its track record in the field of child online safety. Internationally, it's widely admired for having a number of world class organisations and proven examples of best practice. It also displays strong international leadership, founded on a vibrant and ongoing UK multi-stakeholder expert discourse.

19) Once senses, that the WePROTECT Global Alliance is ushering in a new era for the UK, as it leverages its world class reputation in the field of child online safety. It is already acting as a catalyst to a more coherent global approach, not just to the risks but the opportunities, for children and young people as they learn to navigate their digital lives.

August 2016

Brief Biography

1) I am an independent consultant in the field of child online safety. I recently advised the British Board of Film Classification (BBFC), as part of the consultation on age verification and Child Helpline International, headquartered in Amsterdam, as part of its UNICEF funded WePROTECT Global Alliance to End Sexual Exploitation of Children Online initiative.

2) As former Director of the Family Online Safety Institute (FOSI), I have served on the UK Council for Child Internet Safety (UKCCIS) Executive Board for three years and chaired the UKCCIS Overblocking Working Group and UKCCIS Filtering Working Group thereafter. I remain a member of the UKCCIS Evidence Working Group.

3) I was the architect of FOSI's Global Resource and Information Directory (GRID). Launched in 2010, it remains the only comprehensive source of peer-reviewed online safety information on a global scale. In May 2016, FOSI GRID was relaunched with funding from UNICEF, as part of the WePROTECT Global Alliance initiative to tackle online child sexual exploitation and abuse.

4) With more than thirty years of executive management experience at leading technology and telecommunication companies including Motorola, Compaq and IBM, I am a member of the Worshipful Company of Information Technologists and Freeman of the City of London.

Useful links:

http://www.bbfc.co.uk

http://www.childhelplineinternational.org

https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis

http://www.weprotect.org

http://fosigrid.org

http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

http://stakeholders.ofcom.org.uk/binaries/internet/fourth_internet_safety_report.pdf

https://www.internetmatters.org

http://www.friendlywifi.com

defenddigitalme - written evidence (CHI0042)

Inquiry into Children and the Internet

About defenddigitalme

Defenddigitalme is a volunteer non-profit campaign group for children's privacy rights formed in 2015 in response to concerns from parents and privacy advocates about increasingly invasive uses of children's personal data. The campaign asks the Department for Education (DfE) to change their policies and practices to protect 20 million children's identifiable personal and confidential data in the National Pupil Database (NPD):

- stop giving out identifiable personal data to commercial third parties and press without consent
- start telling school staff, pupils, and parents what DfE does with individuals' personal data
- be transparent about policy and practice

More information: http://defenddigitalme.com/

Summary

Our submission responds to the consultation two-part statement that, 'data protection poses a problem for children':

"There is a risk that their personal data may be collected or transferred without them being aware. There is also concern that the online activity of children may remain visible to future employers or academic institutions."

We focus on two areas of the State's collection and use of children's personal and education data which need attention:

I. **Secondary uses of children's personal confidential data collected in schools and provided under statutory obligation to the Department for Education**:

   A. The Department for Education release of these data to third parties.
   B. Privacy notices' failure to effectively communicate an understanding of the use and effects of personal data to data subjects, in particular to children, their inadequacy, and derived lack of Data Controller accountability.
   C. Subject Access Request rights
   D. Public awareness and attitudes towards the National Pupil Database

II. **Surveillance of children's use of the Internet and collection of personal data through third party software as part of a Department for Education web monitoring statutory requirement, effective September 5, 2016**

A. Web monitoring through third party software
B. Biometrics in schools and personal data collection
C. App surveillance tools and online data collection

Department for Education data policy, practice, and children's rights about the use of confidential data

1. Recent amendments to the Department for Education (DfE) data policy and practice, as well as changes that will shortly impose statutory web surveillance, affect children across all State education, age 2-19 in England. These changes have been characterised by lack of transparent due diligence, public engagement, or democratic debate before imposing significant policy with far reaching potential, and that encroach on children's rights.

2. Data policy and practice about children's confidential data at the Department for Education since 2012, impinge on principles set out in the United Nations Convention on the Rights of the Child, Article 12, *the right to express views and be heard in decisions about them* and Article 16 *a right to privacy and respect for a child's family and home life*. Similar rights that are included in the common law of confidentiality, Article 8 of the Human Rights Act 1998 incorporating the European Convention on Human Rights Article 8.1 and 8.2 *that there shall be no interference by a public authority on the respect of private and family life that is neither necessary or proportionate*, and Data Protection Act 1998, that *data must be processed fairly and for limited purposes, relevant and not excessive, and kept securely for no longer than necessary*. Judgment of the Court of Justice of the European Union in the Bara case (C-201/14) (October 2015) reiterated the need for public bodies to fairly process personal data before transferring it between themselves.[125] The EU Charter of Fundamental Rights,[126] Article 52 also protects the rights of individuals about data and privacy and Article 52 protects the essence of these freedoms. These are fundamental rights that help children develop, and grow. This encroachment into rights has come about over time and incremental scope creep through legislative changes since 2000.

3. We would like to suggest a legislative review of the National Pupil Database with respect to children's rights because technological change in those sixteen years has outstripped the capacity of laws to keep up, and keep pupil data safe. What was designed to enable public benefit from pupil data, has resulted in what the public perceives as misuse of their personal data, namely having been obliged to provide data for a service (their child's education) those same data are being used for purposes far beyond what parents and pupils think reasonable and fair.

---

125 Judgment of the Court of Justice of the European Union in the Bara case (C-201/14) http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150110en.pdf

126 http://fra.europa.eu/en/charterpedia/article/52-scope-and-interpretation-rights-and-principles, *EU Charter of Fundamental Rights,* The European Union Agency for Fundamental Rights (FRA)

Data handling of children's confidential data at the Department for Education

4. Exploiting personal data from individuals for short term economic well-being in the name of the public interest, must not be at the long term expense of societal benefit which can be gained from trusted use of public data.

   Public benefit has been the key purpose of using data in academic research and used to address 'some of the most pressing challenges facing society,' (ESRC, 2016) for a number of years. However recent legal and policy changes in who can access education data and what they can use it for, have expanded the scope of use to exploitation of data beyond the Public Interest to also mean commercial users and individual companies, charities and the press.

5. It is this disparity between government departments and safe research data handling infrastructures, which means inconsistent policy and practices exist in parallel. Secure handling is key to public trust, poor policy and practices jeopardise this and risk data misuse and potential resulting harm.

6. The uses of data by different types of user today are accessed via different pathways, and it is perhaps surprising that the use of the most sensitive individual identifiable data is made via the least safe method and techniques today, opened up to non-safe accredited researchers. There are a number of concerns around the differences between risk level of data release by the Department for Education internal process (DMAP) and identifiable data use outwith any oversight, and without audit and transparency after its release into the wild, which are mitigated by the use of the physical infrastructure of safe settings, safe data practices following UKAN anonymisation techniques, and accreditation of safe researchers. Principles that enable safe and trusted public interest research using population-wide data for the purposes of public benefit, with transparent oversight and outputs, but which the Department practices do not follow.

Expanding the scope of children's confidential data use beyond Education

7. The future scope of children's data to be collected and who these data may be shared with, is about to expand. New Department for Education policy starting in the 2016-17 academic year will increase the volume of individual-level personal data to be extracted to the national database and include country-of-birth, and nationality. There is no legislative difference that will mean these data items would be treated any differently from current use, including other government departments.

8. The government-wide 'datasharing' of all public data is set out in the Digital Economy Bill 2016, will use more identifiable data for a wider range of purposes, and also expand its use in deidentified research or statistical outputs, together with increasing the use of data that have been linked with multiple datasets across different sources.

9. The upcoming Digital Economy Bill 2016 as it is now, comes with a risk that parts of the bill around the use of further expanding scope use of identifiable data by government are likely to result in further unexpected outcomes for children and young people as individuals from unseen data processing in the areas of debt collection such as student loans, and targeted public services (i.e. 'Troubled Families') from stigmatisation from application, or where 'freedoms, rights, or interests' of the individual are contrary to those of 'the State'.

Public voice and expectations about their personal data entrusted to Government

10. We submit evidence of public opinion, the qualitative and narrative responses we have gathered over the course of 2015-16 about public awareness of how personal and education data gathered in school are used by the State, through the National Pupil Database. And we reference the extended public engagement work of the ESRC, Wellcome, and the 2010 Royal Society of Engineering with 14-19 year olds. Our work to date shows young people, parents and school staff are surprised by uses of children's data from the National Pupil Database, especially by commercial use.

11. Young people, age 14-19 were asked in the 2010 study Privacy and Prejudice,[127] conducted by The Royal Academy of Engineering (Paterson, L. and Grant, L. (eds) supported by three Research Councils, and Wellcome, about attitudes towards the use of electronic medical records, their concerns and questions centred on privacy, and data getting into 'the wrong hands'.

12. Trust in use of their confidential health data was affected by understanding data security, anonymisation, having autonomy and control, knowing who will have access, maintaining records accuracy, how will people be kept informed of changes, who will maintain and regulate the database, and how people will be protected from prejudice and discrimination [through use of their data].

13. The report concluded: "These questions and concerns must be addressed by policy makers, regulators, developers and engineers before progressing with the design, development and implementation of EPR record keeping systems and the linking of any databases."(p40)

14. On a small scale, we asked similar questions of young people on use of their education data. We include those findings later.

---

127 Paterson, L. and Grant, L. The Royal Academy of Engineering (2010), *Privacy and Prejudice: Young people's views on Electronic Patient Records*. http://jenpersson.com/wp-content/uploads/2016/08/Privacy_and_Prejudice.pdf

15. The Royal Statistical Society Data-Trust-Deficit with Lessons for Policymakers, 2014[128] measured public trust levels and found that individuals' trust in government to use personal data in their best interest is low. Only 11% of those asked in the 2014 surveys had a high level of trust in government to use their personal data in their best interest.

16. If public trust is to be increased, the use of personal data needs to return data sovereignty to individuals, and reduce data used for covert surveillance. Baroness Kidron talked in the House of Lords in January 2014 (Hansard), of creating a regulatory framework that protects young people from routine collection of their data, from it being stored and sold in perpetuity without recourse.

17. We see opportunity to address these issues in upcoming legislative changes, and to make the spectrum of public data work well, in a consensual and trusted relationship between individual and State, by restoring the rights of the individuals from whom data come to the core of data policy, setting public benefit as the central purpose of use, framed in good data security practices, data integrity, and other uses filtered in an ethics-based framework of decision-making.

Introduction - "There is a risk that their personal data may be collected or transferred without them being aware."

18. The 2014 report to which the consultation makes reference, *Children's online behaviour: issues of risk and trust - Qualitative research findings*,[129] groups some known risks into a hierarchy, of 'contact' risks (e.g., unsolicited approaches from strangers), and 'conduct' risks (e.g., engaging in cyber-bullying). And it said, "There is less consideration of content-associated risks (e.g. viewing inappropriate content), or the perceived repercussions of these risks."

19. Risks children face now, include those they cannot perceive because they are hidden from the user. They can be disempowered through the mining of their individual personal data in machine-based decision making, in profiling, use of predictive data, and targeted behavioural influence, whether by commercial companies or under the care of the State.

20. Protecting children's integrity of their identity, their being online or offline, should be seen as sharing a common goal: enabling the development of their full potential and safeguarding children's future selves so as to protect them from harm generated as a child, following them in perpetuity. As Frankie Boyle wrote in the Guardian in 2015[130] whether of

---

128 Royal Statistical Society Data Trust Deficit with Lessons for Policy Makers (2014) https://www.statslife.org.uk/news/1672-new-rss-research-finds-data-trust-deficit-with-lessons-for-policymakers

129 Ofcom Children's online behaviour: issues of risk and trust Qualitative research findings (2014) http://stakeholders.ofcom.org.uk/binaries/research/research-publications/childrens/report.pdf

130 *The snooper's charter: one misspelled Google search for 'bong-making' and you'll be in an orange jumpsuit*: Frankie Boyle (Nov 2015)

children or adults, "Perhaps we've got so involved in the false selves we project on social media that we've forgotten that our real selves, our private selves, are different, are worth saving."

21. Writing about the Investigatory Powers Bill, that will enable every person in the UK's web browsing history to be stored and used by third parties, he could also have been writing about the statutory guidance that makes web monitoring of children compulsory from September 5th 2016. He reminds readers that we need to consider what our internet history is. "The legislation seems to view it as a list of actions, but it's not. It's a document that shows what we're thinking about." Children think and act in ways that they may not as an adult. People also think and act differently in private from they may in public. So the fact that our private online activity may become visible to the State, future employers or academic institutions — whether as photographs capturing momentary actions, or trails of transitive thinking via our web history — and those third-parties may make judgements and reach conclusions about us, correctly or not, behind the scenes without transparency, oversight or recourse, is of concern.

22. Children's personal data, which are now available from birth in health and may be joined to education data available from age 2, means that longitudinal data increasingly offers a richness and depth of life stories that has not been available before. For academic researchers this presents an opportunity to see into lives, and infer connections, and patterns that they could not otherwise. The same is true for other data users. This knowledge creates a power imbalance between what is known to the data user and what is known by the subject themselves. Power has the potential to be used for good, or not.

23. Data Protection needs reframed in many discussions as not about protecting data, although data security plays a big role in the discussion, but the purpose of protecting data is to protect the person from whom the data comes, from potential harm through abuse of power; labelling, stigma and discrimination, or any kind of unwanted intervention as a result of the knowledge obtained from their data.

24. The term 'datasharing' is often used when in fact copying and using data without consent is a more accurate description from the data subject's point of view. This introduction goes some way as to be an explanation why protecting children's data entrusted to schools — the personal data provided by parents and pupils themselves, combined with the individual attainment, behavioural and opinion based data created in schools — really matters. Who has access to these data and what they are permitted to do with it may affect our children in their everyday life, beyond school, and forever.

25. Risk for this generation through the covert manipulation of free will and behaviours online or censorship of their Internet access go beyond their

---

https://www.theguardian.com/commentisfree/2015/nov/10/frankie-boyle-theresa-may-internet-surveillance

own personal risk but have potential offline risk for the functioning of a fair and democratic society as we know it: influencing voting, emotional contagion (see the Facebook experiment), manipulated Internet search returns — to show only certain providers' services, goods, information about certain people, candidates or events.

I. Secondary uses of children's data collected aged 2-19

26. All the named data collected starting from the Early Years settings for children aged 2-19 at the time of collection, are processed to the National Pupil Database (NPD) and given away to third parties by the Department for Education (DfE). The NPD is one of the richest education datasets in the world and holds a wide range of information, extracted since 2000. Any school pupil's full educational record is made up of personal data given to schools by parents, and the pupil data created in school from testing and tracking; attainment records, absence, exclusions, sensitive data like ethnicity and date of birth, SEN, indicators of armed forces, and indicators of children in care.[131] It includes a number of different linked data collections from schools, Local Authorities and awarding bodies, processed by the DfE's Education Data Division (NPD User Guide, 2015, p5).[132] We obtained the size of the database through Freedom-of-Information[133] as this is not published. 'The total number of Unique Pupil Numbers (UPNs) in the NPD as at 28/12/2015 was 19,807,973. This covers pupil records since 2000.'

A. Data releases from the Department

27. The National Pupil Database data are released outside the Department for Education process for academic research purposes. Those deidentified uses are not the subject of this submission. All the releases we mention here are those made by the Department of identifiable data. In addition to requests for use in public interest research from academic institutions, data have been released to commercial companies, charities and journalists. Recipients of sensitive identifying individual-level personal data include national papers[134] and television.[135] An August 2016 FOI request shows not all releases are publicly documented. Since 2012 children's data were given to the Home Office 18 times, and the Police made 31 requests.[136]

---

131 DfE *Common basic data set (CBDS): database* https://www.gov.uk/government/publications/common-basic-data-set-cbds-database

132 Copy of the 2015 NPD user guide http://defenddigitalme.com/wp-content/uploads/2016/08/NPD_user_guide.pdf

133 FOI request for total pupil numbers in the NPD https://www.whatdotheyknow.com/request/pupil_data_national_pupil_databa_2

134 FOI request September 2015 https://www.whatdotheyknow.com/request/293030/response/723407/attach/5/The%20Times.pdf WhatDoTheyKnow.com

135 https://www.whatdotheyknow.com/request/293030/response/723407/attach/10/BBC%20Newsnight.pdf

136 FOI request July 2016, Pippa King https://www.whatdotheyknow.com/request/pupil_data_sharing_with_the_poli WhatDoTheyKnow.com

28. The DfE publishes online a spreadsheet register[137] of third-party recipients to whom it has released data since 2012 through its own application and approvals process (DMAP). Of the registered 462 releases of identifiable data that went through the DMAP in 2012-2014, 53 were aggregated data. All others are individual level. A recent May 2016 update shows 650+ releases (2012- 2015).

B. Privacy notices and legal uses

Question 5 in the consultation asks what roles schools can play in educating and supporting children in relation to the internet? What guidance is provided about the internet to schools and teachers? Is guidance consistently adopted and are there any gaps?

29. Schools use a variety of system providers to collect a vast amount of personal data from pupils, and create additional data in schools about children's educational achievement, behaviour, attendance, absence and more. Schools are ineffectively informed about national use of their pupils' data collected locally. Communication is on transmit mode only from the national Department, made through an overly complex and under transparent template privacy notice, which leaves a knowledge gap between the Department and schools. It is potentially big enough to protect the Department from legal challenge on use of pupils' personal data, but not to rescind its responsibility to do the right thing. The Department is accountable to make sure the public expectations are met that our data are safe and used transparently with 'no surprises' (Wellcome, 2015),[138] the alternative, keeping things hidden was to the cost of public trust in use of health data in the care.data programme and has ongoing repercussions for public interest research, and individuals' accessing healthcare.

30. Changes in 2012-13 Education policy and law, permitted the release of individual data, by amending section 114 of the Education Act 2005, section 537A of the Education Act 1996, and together with the 2009 Prescribed Persons Act changed the purposes for which data about individuals could be released, and changed to whom it could be given. When the database was first opened up, then Ministers gave verbal assurances the Department was not interested in names.

31. The uses that were limited in 2003, to a "small number of technical staff engaged in collating the pupil level data and creating the profiles have access to pupils' UPNs and names. Analysts in the Department and partner agencies (Ofsted, QCA and LSC) have access to anonymised

137 NPD third party online release register https://www.gov.uk/government/publications/national-pupil-database-requests-received

138 Wellcome Trust Briefing (2015), *Ensuring the effective use of patient data* https://wellcome.ac.uk/sites/default/files/ensuring-the-effective-use-of-patient-data-briefing-aug15.pdf

profiles for use for statistical purposes only"[139] as described by Stephen Twigg, are long since exceeded.

32. For detail of the legislative changes before 2007 see Children's Databases - Safety and Privacy (Anderson, R., et al. 2006 pp112-115).[140] The 2012-13 changes enabled individual pupil information to be released for the first time:

> "Persons who, for the purpose of promoting the education or well-being of children in England are— (i) conducting research or analysis, (ii) producing statistics, or (iii) providing information, advice or guidance, and who require individual pupil information for that purpose."

33. The revised privacy notice template of May 2016, included for the first time, a link to the organisations that the DfE gives individuals' data, including commercial companies, charities and journalists, recipients of children's identifiable personal data from the National Pupil Database between 2012 and December 2015.

34. Notices adapted from the national template and then used in schools are however widely variable in how they reach schools, via Local Authorities or other channels depending on the school structure, and those forms content we have seen vary from including as little as one line on purposes, 'Data may be shared with the Department for Education'.

35. However even if children in school between 2000 and 2012 had read the then school issued privacy notice in detail and knew that their data from the census was sent to the Department for Education, then passed on to organisational bodies in the style of Ofsted or HESA, no child whose data were collected before 2012 has been contacted to tell them that the law changed in 2012-13 to permit the giving away of their named, confidential personal data, or of giving out individual level data to journalists, charities, and commercial business.

36. Further the Department appears to have had no clearly recorded legal basis for handing out sensitive data.[141]

37. These gaps needs attention if the uses of the pupil data are to meet current and future legislative requirements, particularly with regards the EUGDPR on consent, limitation of purposes, profiling, necessity, and proportionality.

38. At the time of writing the School Census and Early Years Census collection are about to be further expanded, beginning in the 2016-17 school

---

139 Hansard 14 Apr 2003 : Column 557W—continued http://www.publications.parliament.uk/pa/cm200203/cmhansrd/vo030414/text/30414w22.htm

140 *Children's Databases - Safety and Privacy* (Anderson, R., et al. 2006) http://www.fipr.org/childrens_databases.pdf

141 https://www.whatdotheyknow.com/request/pupil_data_sensitive_data_releas#comment-69968

year.[142] The collection has had no privacy impact assessment,[143] no public or parliamentary debate.

39. Given recent Supreme Court ruling on the limitation of purposes, no provision for removal of information at third parties contravening Google Spain,[144] and interference with privacy, it should be examined as to its legislative basis.[145] The purpose of the collection for country-of-birth and nationality at national level are not being well communicated to pupils, or schools.[146] While 'no requirement' is made to see passports, "The country of birth would be expected to appear on — or be derived from — the child's birth certificate or passport." Wording that leads some schools to ask for passports.[147]

40. The DfE school census video[148] made for school staff, explicitly says schools staff need not get consent, because there is a statutory gateway for the collection, and schools cannot be held accountable for breach of pupil confidentiality — so the Department for Education takes that decision and responsibility away from schools although the Minister has said, "We do not advise schools directly on their collection and processing of personal data or regulate their compliance with the Data Protection Act."

41. The same video does not tell them about any expanded purposes of the data use since 2012 changes. They indirectly therefore tell schools to rely therefore on fair processing but don't inform them explicitly, simply and transparently about all the Department releases of data to all third parties, so schools can't fair process because they aren't given simply all the facts to share.

42. Privacy notices policy at the Department for Education fails to adequately inform children of uses of their data, fail to take responsibility for communication if they can be amended at will after the data collection, and fail to offer the opportunity to remove or correct the data subjects' data before the purposes and users are amended.

43. We were told that the Director General for Regulation at the UK Statistics Authority wrote to the Department for Education calling for improved

142 http://blogs.lse.ac.uk/parenting4digitalfuture/2016/07/19/school-census-changes-add-concerns-to-the-richest-education-database-in-the-world/

143 http://defenddigitalme.com/wp-content/uploads/2016/08/Gibb_response_Aug2016_36177.pdf

144 http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf Google Spain ruling

145 http://panopticonblog.com/2016/08/25/donald-wheres-schedule-3-condition-share-information-aboot-troosers/

146 https://www.buzzfeed.com/laurasilver/parents-are-worried-about-schools-plan-to-ask-what-country-t?utm_term=.mmolpAkP#.de9P4yJX

147 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/544214/2016_to_2017_School_Census_Guide_V1_2.pdf

148 https://registration.livegroup.co.uk/efa/contenttabs/embed.aspx?dfid=12620&ctid=242&cat=1937 (listen from 40 seconds in)

transparency and handling in April.[149] Much remains to be done to achieve this. See our FAQs for more information: http://defenddigitalme.com/faqs/ and sample case studies of use.

C. Subject Access Request rights — are data accurate and if not how do I correct it?

44. The Information Commissioner's Office has made it clear to the Department that in principle it supports data subject good practice rights of access[150] to enable individuals to check that the data held in a database are accurate and correct them if necessary. Given that these data are used for direct interventions it is vital data are accurate. The effect of an incorrect address being used by academic researchers for a health or education survey is potentially quite different from it being used by the Home Office. The Department refuses subject access requests, basing withholding on exemption Section 33 in the Data Protection Act. This exemption is used where data are held for research purposes, where data are not used to have any direct effect or intervention with individuals. Our case studies show that named interventions[151] use these data, as well as being used by at least one Data Processor to create predictive scoring on children, which is fed back to Local Authorities and schools. These data are processed without the knowledge or consent of parents or pupils. At present national newspaper journalists have greater access to children's identifiable data in the NPD than parents or children themselves. Clearly any changes in this would need strict regulation to enable appropriate and approved access.

D. Public Awareness and Attitudes towards the National Pupil Database

45. We set out to make a preliminary qualitative assessment of awareness in school staff, parents and young people about the NPD, asking them what they know about how children's data collected in school and its use beyond state education. These results could be seen as a pilot for a broader engagement in how the public relate to information and NPD data, and its use.

Summary of responses gathered

46. In autumn 2015, we asked school staff about when they last received or made an update to their own privacy policies, but we encountered consistent difficulty asking about it, as none were familiar with the concept or uses from the NPD. In this atmosphere we promised anonymity to schools and staff in the publication of their responses. Students who gave us recorded interviews gave us only their first name, age, and hometown. We did not ask for contact details to re-contact. We

149 http://defenddigitalme.com/2016/04/director-general-for-regulation-uk-statistics-authority-suppports-call-for-transparency-and-better-data-handling-of-20-million-pupils-data/

150 https://ico.org.uk/for-organisations/guide-to-data-protection/principle-6-rights/subject-access-request/

151 http://defenddigitalme.com/wp-content/uploads/2016/04/DDM_shared_examples_April2016.pdf

focussed on questions of awareness of data existence and use, and asked young people about control of their data.

Schools - talking about their pupil data

47. From a list available online of all state sector schools, and 100 asked, we had replies from 30 primary and 45 secondary schools in Dorset, East and West Sussex, in London, Oxfordshire, and Yorkshire. We selected a spread between rural and city schools, those under Local Authority or academies. We did not ask Free Schools. When we first asked schools about it by email or telephone, respondents said it was because they had never heard of the NPD and felt unable to give an informed opinion. We then instead asked for concrete copies of privacy notice documents via FOI and comment. Privacy policies returned demonstrated a wide variety of wording and consistent gap in communicating NPD use.

Education practitioners' questions and answers

48. We interviewed 100 teaching or affiliated school staff face-to-face at three education events in spring 2016. None were aware of the NPD. Most were aware of the school census but did not know who see pupil data outside school or the Local Authority. Some suggested only statistics are shared outside their school or at national level. Ten staff sampled from Independent schools asked at the Festival of Education, in June, were also unaware of data uses though one had heard of the database created from the census, as they used a copy of personal data collected for alumni fundraising.

Parents' questions and summary answers

49. We interviewed 100+ parents face-to-face in November 2015 at the Mumsnet Blogfest in King's Place, NW London. These were parents of children, in education in England, 90% in state education. We discounted 2 home schooling. They came from across England. No one had heard of the NPD or knew that named identifiable data are released beyond school for use by third parties. All were surprised that commercial businesses and journalists could access data. Comments ranged from questions of trust, to a lack of concern 'as long as they've not done anything wrong with it.'

Young people questions and their answers

50. We gathered interviews over two separate hours on two days in May 2016 at the University of Sussex with 25 individuals under 35, only if they had been to school in England, and in different parts of the country. Six agreed to recorded statements. We introduced the idea of the NPD. None had heard of it. We explained that the data has been opened up to third parties since 2012, the approvals process, rules for use, and the wording of the legislation on uses. Comments from interviews include:

51. Ben 26, from Reading: "I don't think commercial businesses should have access to student data. You have not necessarily been exploited, but definitely used."

52. Catherine, 21, from Gloucestershire: "Parents and pupils should have access to their own data and should know who else has it. I don't think anyone else should have access to the identifiable data without consent."

53. Johann 18, from Paris (completed A-levels in England): "I'm not surprised my data is used by others, probably some of it is used for good causes, but we should know who has it […] we should define our privacy (not the government) and they should ask us before they use it for anything we don't expect."

54. John 30, from UK: "I've never heard of the National Pupil Database. I'm really surprised, it's a bit weird. I don't think anyone should have it unless it's to do with my education. We should definitely be asked."

55. Ruby 28, from Newcastle: "I'm surprised to hear my school data could be used outside schools without my consent. It's a personal thing and can affect lives."

56. Steph 19, from London: "In school I remember being told to do biometric fingerprints for buying lunch. We had no idea what it would be used for and I've no idea if they ever delete them. Parents should be asked for consent. As pupils get older we should decide ourselves."

57. Public and school professionals' familiarity with the National Pupil Database is almost zero. If uses across the data spectrum are to best serve our public interest needs, then consistent legal, safe and transparent policy and practices are needed across education, underpinned by accountability. Respect for the opinion and rights of children (many now in the NPD) about how their data can and should be used must be restored, as the foundation of all data use is public trust.

II. Surveillance of children's use of the Internet

58. Without Parliamentary debate or public discussion, children's internet use will be monitored by third parties from September 5th 2016, under statutory guidance issued by the Department for Education. This is despite widespread associated concerns – including choking off free speech, religious freedom, and staff feeling vulnerable — shared with the Joint Select Committee for Human Rights by experts in education and security legislation.[152]

59. The brief paragraph 75 in The Department for Education (DfE) "New measures to keep children safe online at school and at home"[153] statutory

152 http://www.parliament.uk/business/committees/committees-a-z/joint-select/human-rights-committee/legislative-scrutiny/parliament-2015/extremism-bill/?type=Oral#pnlPublicationFilter

153 https://www.gov.uk/government/news/new-measures-to-keep-children-safe-online-at-school-and-at-home

guidance, *Safeguarding in Schools*, will impose a change from a duty 'to consider' web monitoring to one that 'should ensure' it for educational establishments, excluding 16-19 academies and free schools.

60. We suggest that this proposal which will monitor every child in England's in-school's online activity and communications is significant and opens a slippery can of worms.[154] Some providers manage the monitoring entirely offsite outside school, removing the oversight of the classroom teacher from the process. It is unclear whether Bring-Your-Own-Device policies offered by some well known providers in the market means surveillance software is carried into personal time and use at home, yet there has been no standard code-of-practice to tell schools this would be unacceptable practice, to accompany the guidance.

61. Before imposing this statutory practice, its cost, technical risks and impact where it has already been used in practice, should be assessed more deeply and widely debated in public and Parliament. Due diligence of providers should ensure appropriate standards and regulation when providers may have access to millions of children's computers and devices and it is left to independent experts to demonstrate flaws that put children at risk.[155] Basic flaws such as using a default password of "password" to connect clients to its servers should never happen.[156] This programme has been imposed without understanding its impact or checking that known issues or questions asked in consultation[157] have been solved.

62. Children aged nine and under were among 3,955 people reported to Channel in 2015, up from 1,681 in 2014.[158] How many of these stemmed from being flagged by algorithms, or web browsing and monitoring?

63. Children have rights to be able to access information. Web monitoring, the surveillance of search terms and web uses, looking for keywords and logging behaviour is not to be confused with web filtering, which restricts access to certain material to protect children from content deemed inappropriate. Others feel it is ineffective[159] and counter productive, and lack of communication and transparency about its implementation even leaving parents feeling betrayed.[160]

---

154 http://schoolsweek.co.uk/mandatory-web-monitoring-in-schools-opens-a-slippery-can-of-worms/

155 July 2015, Security flaw found in school internet monitoring software https://www.theguardian.com/technology/2015/jul/14/security-flaw-found-in-school-internet-monitoring-software

156 https://www.techdirt.com/articles/20150715/10274131649/shocking-software-used-to-monitor-uk-students-against-radicalization-found-to-be-exploitable.shtml

157 http://defenddigitalme.com/wp-content/uploads/2016/04/DfE_consultation_Feb2016v4.pdf *Keeping Children Safe in Education* consultation response

158 http://www.npcc.police.uk/Publication/NPCC%20FOI/CT/02616ChannelReferrals.pdf

159 http://www.wired.co.uk/article/schools-monitor-children-internet-use

160 https://webdevlaw.uk/2015/10/30/the-ugly-truth-behind-uk-schools-monitoring-students-keyword-searches/

64. A statutory requirement should be explicit in its terms. Yet what "has appropriate filters and monitoring systems in place" means for different age groups, types of pupils, staff, school and home settings, is not.

65. On filtering however there are also concerns about how framing can mean over cautious implementation restricts children's rights to information. The UN Special Rapporteur's 2014 report on children's rights and freedom of expression stated: "The result of vague and broad definitions of harmful information, for example in determining how to set Internet filters, can prevent children from gaining access to information that can support them to make informed choices, including honest, objective and age-appropriate information about issues such as sex education and drug use. This may exacerbate rather than diminish children's vulnerability to risks."

66. This new guidance, 'Safeguarding in Schools' makes no attempt to ensure informed changes about new national policy on web monitoring reaches children and parents. The potential for risk undermining trust between teacher and pupil should not be underestimated. The chilling effects associated with online surveillance[161] and long term effects and impact on children's curiosity, willingness to take risk, innovate, and challenge thinking of the day, are as yet unassessed.

A. Biometrics and surveillance of children in schools online and through new technology

67. The opportunity for online surveillance of children through new web applications has been lauded by some. Nicky Morgan former Education Secretary at the BETT trade show in both 2015[162] and 2016,[163] praised an app that enabled parents, or others, to track children's movement.

68. The general use of apps in schools, their educational value and technical safety, appears unregulated and without oversight. We have started to look at privacy policies in some commonly used apps, and in particular those who send enrolled children's personal data abroad, typically to the US. Many aware parents agree with academics who feel we are sleepwalking into the use of these systems which pose risk.[164] Some commercial companies have been to date unresponsive to questions on their practices and children's privacy rights.

69. Schools can fail to ask parental permission for signing up children in the classroom and inadequate attention is given to privacy or long-term implications. We have begun conversations to see whether opportunity to improve teachers' understanding of Data Protection and privacy in the classroom can come through teacher training — up to date with current technology, and with privacy rights. If and how the current teaching

161 Penney, Jon, *Chilling Effects: Online Surveillance and Wikipedia Use* (2016). Berkeley Technology Law Journal, 2016. Available at SSRN: http://ssrn.com/abstract=2769645

162 https://www.gov.uk/government/speeches/nicky-morgan-speaks-at-the-2015-bett-show

163 https://www.gov.uk/government/speeches/nicky-morgan-bett-show-2016

164 https://www.theguardian.com/education/2016/mar/05/education-parent-children-behaviour-app

training curriculum includes this in a consistent and up-to-date way we don't yet know, but if not, it is a serious gap that needs filled.

70. The first instance of a school in the UK using RFID technology to track individual children's activity and behaviour in schools was scrapped in February 2013 at West Cheshire College after significant financial cost.[165]

71. The full national extent of using fingerprint and other biometric technology in schools is unknown.[166] Since 2001 iris scanning and facial recognition have also been used in schools.[167] There is no transparent assessment of the technological capacity, false positives, cost and benefit, or effectiveness. There is no clear oversight of technologies specific to schools.

72. These practices seem to be praised before they are proven to be of benefit, or before measuring their impact against a business plan and cost, or indeed as technology becomes increasingly invasive, against ethical standards and human rights legislation, or even it appears often, before communication to parents and pupils of its use.[168]

73. The report in the consultation mentions awareness of access to inappropriate material but does not mention access to material which is targeted at them with the intent of behavioural change. Some apps in school are explicit in their intent to change behaviour. Others have indirect or covert influence, and nudge behaviour. How these behaviour changes and their indirect effects will effect children's willingness to search freely for information or concern about what being watched online may mean appears to have little research to date. Very recent preliminary studies indicate that 18-24 year olds, the youngest age group asked in a survey,[169] were the least likely to trust biometrics. Questions remain if schools using theses technologies are gambling with children's identities.[170]

Conclusion

74. For children in educational settings, the people responsible for systems, policy and practice can compromise children's privacy rights and civil liberties, not only for their school life but potentially for their whole lifetime, when they collect personal and other data without consent or communicating an effective understanding of what is being signed up to.

165 https://www.whatdotheyknow.com/request/procurement_procedure_regarding#incoming-446369
166 https://www.bigbrotherwatch.org.uk/files/reports/Biometrics_final.pdf
167 https://www.youtube.com/watch?v=acbSj5m5o5g
168 https://rfidinschools.files.wordpress.com/2013/10/west-cheshire-college-10th-december-2012-foir-fs50488835-report.pdf
169 http://cyber.uk/biometrics/
170 And therein lies another issue: with the potential for life-long consequences, are pupils, some below the age of 16, competent to opt in to such a scheme?

75. The Joint Committee on Human Rights previously found, "failure to root human rights in the mainstream of departmental decision-making."[171] Children's human rights are failed by current practice in the use of personal data entrusted to the State and released onwards to third parties. We suggest careful consideration by the Committee to the upcoming legislation and amendment to address an appropriate balance in this area, especially with regard to children, their personal data used for public benefit, for commercial profit, and uses to their potential personal detriment.

76. Consistent safe data policies, settings in which data are accessed, standards and oversight — how public data not only 'can be' used, but 'should be' used, accommodating consensual data subject rights — are needed across public data, to make data secure, future-proof public trust, and above all to ensure our young people feel sovereignty of their personal data is returned to them, so that they no longer feel, they have "not necessarily been exploited, but definitely used."

77. The quantity of apps and online tools is increasing and being actively encouraged by those who profit from a growing ed tech market[172] and many are exciting with opportunities to learn and have fun. The front door to our children's data "for government, educators, companies and investors from Britain and globally" is wide open. Tools for schools to use to assess whether the latest digital offering is legal, and educationally and ethically sound however, seem to be lacking.

78. Web monitoring and filtering using third party providers is exposing children to new security risks. The loose definitions of inappropriate content used setting Internet filters, can prevent children from gaining access to information that can support them to make informed choices, and may exacerbate rather than diminish children's vulnerability to risks.

79. The CMA report (June 2015)[173] on consumer data, highlighted that to secure the benefits of data, people should know when and how their data is being collected and used and decide if and how to participate.

80. The House of Commons Science and Technology Committee 2014 in their report, Responsible Use of Data,[174] said the Government has a clear responsibility to explain to the public how personal data is being used. This needs to be actioned by government. Their Big Data Dilemma 2015-16 report, concluded:

---

171 Joint Committee on Human Rights, *Data Protection and Human Rights*, Fourteenth Report of Session 2007–08
http://www.publications.parliament.uk/pa/jt200708/jtselect/jtrights/72/72.pdf

172 *The front door to our children's personal data in schools* - Jen Persson, February 2016
http://jenpersson.com/front-door-childrens-data-for-government-educators-companies-investors-britain-globally/

173 CMA report (2015) *Commercial use of consumer data*
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/435817/The_commercial_use_of_consumer_data.pdf

174 The House of Commons Science and Technology Committee 2014 Report, *Responsible Use of Data*
http://www.publications.parliament.uk/pa/cm201415/cmselect/cmsctech/245/245.pdf

> "seeking to balance the potential benefits of processing data (some collected many years before and no longer with a clear consent trail) and people's justified privacy concerns will not be straightforward. It is unsatisfactory, however, for the matter to be left unaddressed by Government and without a clear public-policy position set out. The Government should clarify its interpretation of the EU Regulation on the re-use and de anonymisation of personal data, and after consultation introduce changes to the 1998 Act as soon as possible to strike a transparent and appropriate balance between those benefits and privacy concerns."[175]

81. We conclude that there is not only a risk but already a widespread reality that children's personal data are collected and transferred without them being aware of it. There is also concern that the online activity of children is being used by third parties to make decisions about them without transparency of how those decisions were reached or to assess their impact.

82. Action is needed to safeguard children from use of their data gathered by the State or commercial companies in the course of their education and without transparency, or clear oversight, for a range of secondary purposes which can expose them to risk from outside third parties, decisions based on inaccurate data, or misinformed intervention without clear course of redress. Upcoming legislation may offer opportunity to create Baroness Kidron's suggested framework that protects young people from routine collection of their data, from it being used in perpetuity without recourse.

26 August 2016

175 The Science and Technology Committee, *The big data dilemma* (2015-16) http://www.publications.parliament.uk/pa/cm201516/cmselect/cmsctech/468/468.pdf

Department for Education; Department for Culture, Media and Sport; and Department of Health – oral evidence (QQ 129-137)

Transcript to be found under Department for Culture, Media and Sport

e-Safe Systems Ltd – written evidence (CHI0015)

1. Background

1.1. It is widely accepted that the increasing use of technology in schools can greatly improve academic learning, yet it has become a platform that also facilitates harm - including grooming, paedophile activity, child abuse, sexualisation, HBT, racism, bullying and harassment, possible self- harm/suicide, radicalisation, threats of violence, terrorist activity, FGM, trafficking and gang culture.

1.2. Our goal at e-Safe is to provide early warning of harmful behaviour, the safeguarding support that education leaders need so that they can focus on the core of what they do; teaching and inspiring the new generation

1.3. To this end we offer a complete outsourced monitoring service for schools and colleges specifically designed to take away the burden that statutory safeguarding requirements bring in terms of the dedicated resource and interpretive skills needed.

1.4. This is the only centralised communications tracking, behaviour analysis and early-warning-of-harm service of its kind in the UK and the EU.

1.5. With over 500,000 students and staff monitored in primary, secondary and further education e-Safe affords a unique insight into how children and young people use the digital environment 24 hours per day, 365 days a year, irrespective of whether the user is on-site (school) or off-site (home), using a device online or offline.

1.6. This combination of technology and professional behavioural assessment gives e-Safe unparalleled visibility of:

- The nature of safeguarding risk
- The relative prevalence of that risk and
- The trend in each risk category.

2. How it works

2.1. The e-Safe service uses intelligent detection technology to track static and moving imagery, words and phrases appearing on screen, and keystroke input. All incidents are reviewed by a team of behaviour specialists and any requiring intervention are escalated to nominated school contacts against a pre agreed reporting protocol.

- A sophisticated image detection engine determines whether a static image, a video or webcam activity is pornographic or indicates illegal behaviour such as abuse, grooming

- The word and contextual phrase detection engine monitors for the occurrence of words and/or phrases in any language, including script based languages, which are indicative of various behaviours. The service monitors against a dynamically maintained library of markers (the "Threat Library"), and will only capture user activity when a marker is detected e.g. a word or term in the Threat Library. At e-Safe, new markers of threats are sourced from continuous research by our team of experts, as well as through ongoing collaboration with external specialist agencies and schools. The threat libraries are updated on a daily basis to reflect emerging behavioural trends from a broad, worldwide perspective, right down to local level

- All incidents captured are reviewed in context by a team of multi-lingual behaviour specialists (24/7, 365 days per year) to identify the genuine risks. Incidents are escalated directly to a school's nominated safeguarding and leadership contacts, either directly by phone call (if the incident is illegal or life threatening) or via emailed report - against a pre-agreed reporting protocol determined by incident severity.

2.2. Unfortunately, there is no space in this six-page submission adequately to explain by example the behavioural assessment techniques associated with each of the ten harm categories set out in the analyses below. This could best be handled in face to face discussion with the committee.

3. The evidence base: sample behaviour analysis

To illustrate the nature, trends and prevalence of risk in terms of harmful behaviour and material, we have extracted two subsets of incident data from the monitoring of secondary level and primary age students over the last two years.

3.1. Secondary education

The following incident data analysis from a subset of English secondary schools monitored by e-Safe provides a comparison of behaviour volume and trends during the period 1st August 2014 to 31st July 2016. The total number of students in the sample is 33,669 (2015/16) and 34,012 (2014/15), across 34 urban and rural secondary schools

Table 1: Serious incidents escalated between 1st Aug 2014 and 31st Jul 2015

	Illegal	Self Harm	Bullying	Porn	Sexting	Misuse	Violence/ Threat	Depressed	Concerning	HBT, Racist Comment
Year 2014/15	34	267	663	371	196	597	2007	227	2485	1823

Total: 8670

257 serious incidents per average sized English secondary school (1000 pupils) per year

Table 2: Serious incidents escalated between 1st Aug 2015 and 31st July 2016

	Illegal	Self Harm	Bullying	Porn	Sexting	Misuse	Violence/ Threat	Depressed	Concerning	HBT, Racist Comment
Year 2015/16	51	484	1085	1592	391	2294	5065	1236	4773	3241

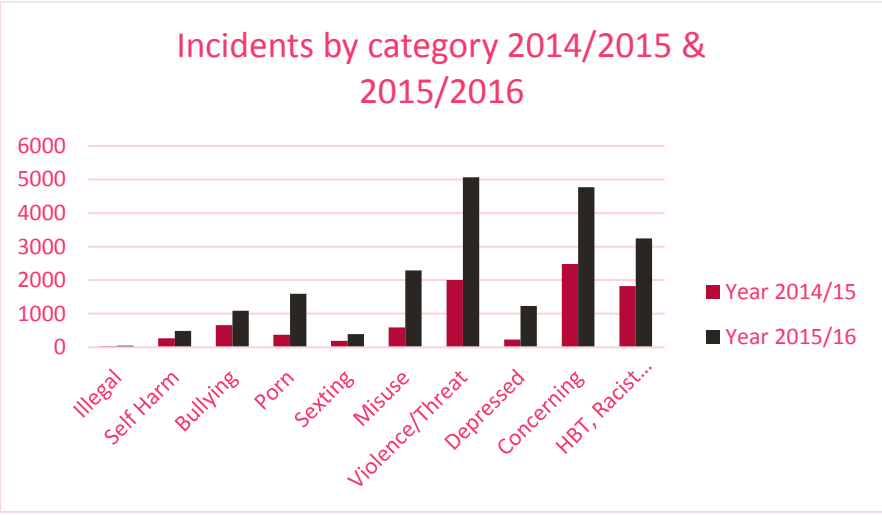
Total: 20212

594 serious incidents per average sized English secondary school (1000 pupils) per year

Table 3: Percentage increase in reported incidents by behaviour category over the last two years

2014 -2016	Illegal	Self Harm	Bullying	Porn	Sexting	Misuse	Violence/ Threat	Depressed	Concerning	HBT, Racist Comment
% Increase	150%	181%	164%	429%	199%	384%	252%	544%	192%	178%

Table 4: Graph illustrating increasing trend of behaviour by category between 2014 & 2016



3.2. Core observations:

3.2.1. The trend of risk and harmful behaviour in the secondary level age group is upward across all serious behaviour categories. The average number of serious incidents per school in the sample reveals a more than 2x increase in school year 2015/16 versus the previous 12-month period

3.2.2. The increase in mental health specific categories (Depression & Self-Harm combined) is significantly higher than all other categories.

3.2.3. The broad range of serious behaviours identified illustrates the importance of the digital environment as a source of risk and a barometer of the social and emotional development and wellbeing of young people

3.2.4. What the analysis does not show but we can support by additional evidence is that 28% of all the behaviour detected and escalated by e-Safe in the period 2015/2016 is the subject of offline activity (i.e. away from the Internet). In our experience this is consistent with the percentage of offline behaviour contributing to serious safeguarding risk in previous years

3.3. Primary education

The following incident data analysis from a subset of English primary schools monitored by e-Safe provides a comparison of behaviour volume and trends during the period 1st April 2014 to 31st March 2016. The total number of students in the sample is 9,081 (2014/15) and 10,073 (2015/16) across 38 primary/infant's schools in a single local authority.

Table 1: Serious incidents escalated between 1st April 2014 and 31st March 2015

	Illegal	Self Harm	Bullying	Porn	Sexting	Misuse	Violence/ Threat	Depressed	Concerning	HBT, Racist, Vulgar Comment
Incidents	0	4	35	27	0	69	104	8	57	11

Total:	315

7 serious incidents per average sized English primary school (200 pupils) per year

Table 2: Serious incidents escalated between 1st April 2015 and 31st March 2016

	Illegal	Self Harm	Bullying	Porn	Sexting	Misuse	Violence/ Threat	Depressed	Concerning	HBT, Racist, Vulgar Comment
Incidents	1	3	9	10	3	51	95	11	60	175

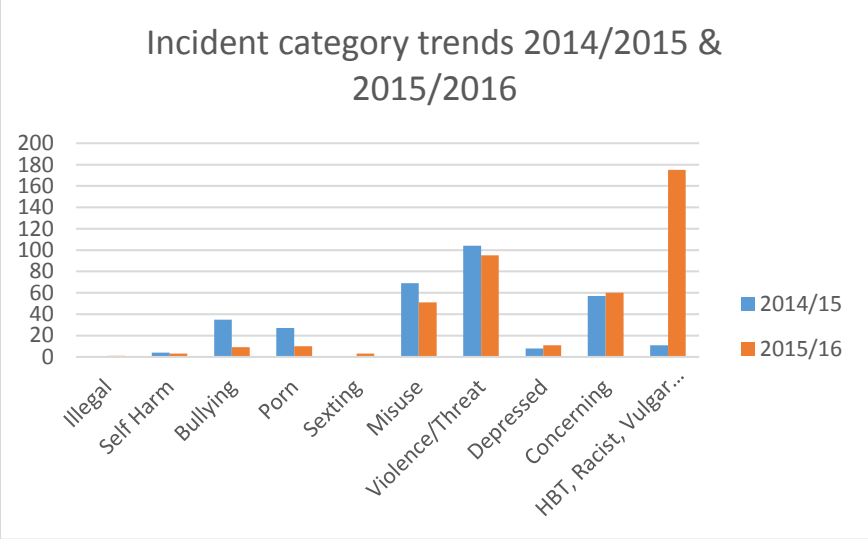
Total: 418

8 serious incidents per average sized English primary school (200 pupils) per year

Table 3: Percentage increase in reported incidents by behaviour category over the last two years

2014 -2016	Illegal	Self Harm	Bullying	Porn	Sexting	Misuse	Violence/ Threat	Depressed	Concerning	HBT, Racist, Vulgar Comment
% Increase	0%	75%	26%	37%	300%	74%	91%	138%	105%	1591%

Table 4: Graph illustrating incidents by category between 2014 & 2016



3.4. Core observations:

3.4.1. Although the sample size of primary students is one third of the secondary sample, the ratio of serious incidents per school is far lower at primary level. The more limited access to computer equipment in primary schools compared to secondary schools is likely to be the main contributing factor as the behaviour categories are all represented but in reduced volume

3.4.2. As with secondary level students the overall trend in behaviour is upward with a 125% increase in incidents per primary student year on year but this is solely due to the increase in HBT, Racist & Vulgar comment

3.4.3. The underlying reduction in incidents excluding HBT, Racist & Vulgarity may indicate that the opportunity to modify behaviour via intervention at primary level is greater than with older students in secondary schools

3.4.4. The relationship between each behaviour category is broadly comparable across secondary and primary school students with the exception of HBT, Racist & Vulgar comment which shows a significant increase at primary level in 2015/16 to exceed all other behaviour categories

3.4.5. Further detailed analysis reveals that the percentage of incidents occurring as a result of benign activity and keystroke errors at primary level is higher than in secondary education. This leads to exposure to inappropriate and potential harmful material, particularly pornography. All UK schools are 'protected' by sophisticated filtering and blocking firewalls/proxy devices, but it is technically impossible to filter out all inappropriate or illegal content with over 1 billion sites on the web today.

3.5. General evidence of behaviour trends in uses of technology

A granular review of the evidence collected by e-Safe in its monitoring of IT/ICT use reveals:

3.6.1. an increasing rise in incidents involving webcam activity

3.6.2. serious incidents occurring on encrypted applications such as Skype

3.6.3. regular attempts to circumvent security and blocking measures e.g. to access the 'Dark Web' using such as Tor browser; and proxy avoidance techniques which are not picked up by edge of network filtering systems

3.6.4. high volume of incidents across most behaviour categories arising from use of social media

3.6.5. chat roulette continues to present some of the most disturbing incidents

3.6.6. an increase in searches and comment related to violence

4. Specific responses to questions raised by the enquiry

4.1. Education (questions 5 through 8)

HM Government policy continually focuses on the risk of online, Internet activity, yet our evidence consistently shows that nearly 1/3rd of the genuine risk is not online. Offline behaviour often reveals the more serious risk - imagery and written content viewed on pen drives; imagery and other material downloaded from mobile phones to school computers; harmful and threatening behaviour reflected in comments on MS Word etc.

Monitoring provides a mechanism to manage the identification of risk and harmful behaviour, and the means by which to measure the effectiveness of interventions to modify behaviour and encourage responsible digital use. The DfE is to be applauded in recommending 'appropriate monitoring' - Statutory Guidance for Schools & Colleges (Sept 2016) but neither the DfE nor its inspectorate appear to understand the latent potential of effective monitoring. All schools and colleges have a legitimate, statutory obligation to safeguard and protect students and staff, and the digital environment and its use by students (and staff) is a rich seam of safeguarding markers.

4.2. Legislation (questions 6 through 12)

e-Safe provides a natural research base for early warning and identification of actual risk. Our window on behaviour affords a unique opportunity to assist policy makers and the inspectorate to understand and anticipate the trends in harmful behaviour as they develop. We capture the behaviour in context as it happens and the growth of our monitored users across the UK education sector ensures an ever increasing data sample of early warning evidence of digital behaviour by young people.

e-Safe's threat libraries enable the production of a powerful set of harm prevalence indicators and harm trend predictors which could be made available as a (confidential) public good to those charged with public policy formulation.

23 August 2016

e-Safe Systems Ltd and Professor Derek McAuley - oral evidence (QQ 37-43)

Tuesday 11 October 2016

Watch the meeting

Members present: Lord Best (The Chairman); Lord Allen of Kensington; Baroness Benjamin; Baroness Bonham-Carter of Yarnbury; Earl of Caithness; Lord Gilbert of Panteg; Baroness Kidron; Baroness McIntosh of Hudnall; Baroness Quin; Lord Sheikh; Lord Sherbourne of Didsbury

Evidence Session No. 3 Heard in Public Questions 37 - 51

Examination of witnesses

Mark Donkersley, Managing Director, e-Safe Systems Limited, and Professor Derek McAuley, Professor of Digital Economy, University of Nottingham.

Q79 **The Chairman:** Welcome to you both. Thank you very much for joining us. As you know, we are deep into our inquiry into children and the internet. You are billed as our technical experts today and we are very grateful to you for coming and being just that. I am going to ask you, if you would, to briefly introduce yourselves. Perhaps, Professor McAuley, you could explain the main aims and the methodology you use at Horizon, in particular the work that you do with youth juries. When I come to you, Mark Donkersley, if you could explain a bit more to the Committee about your company and the system it provides, how the systems work, how your company is funded and so on, that would be helpful too. Introductory statements, if you would, starting, Derek, with you.

Professor Derek McAuley: I am a professor of digital economy at the University of Nottingham and for the last seven years there I have been running a research institute into the digital economy. Within that context, which is quite broad, we have been looking at the opportunities and challenges in the use of personal information. That is the context for Horizon. Obviously, to build an inclusive society, we have to deal with the digital economy for all age groups, so we are interested in not just the compos mentis 25 year-old single adult, which a lot of the technologies are targeted at, but children and disabilities, all sorts of things, to build an inclusive society. To that end, we had a particular project looking at social media analytics, something I gave evidence on to the House of Commons Select Committee.

In that context, we used youth juries as a way to elicit from children and young adults what they thought of social media. The methodology is to present vignettes, so you presented them with short dramas enacted sometimes in front of them, sometimes with a video, which presented some form of dilemma; for example, personal data tracking, issues of concern around removal of embarrassing or inconvenient content. These were presented as vignettes, and the jury, composed of 10 to 15 of the children, mostly aged between 12 and 17, were then asked to pass judgment. They did not sit quietly at the back of the room; they had to discuss it. It was an experimental methodology to try this, rather than to have what would normally be a focus group based on a vignette. Calling them juries and having them making decisions was an important part of that process.

There were three in each of three cities, so there were nine juries all together, in London, Leeds and Nottingham, and in fact they were focused around the 5Rights, which Baroness Kidron has been championing and leading. We partnered with the then iRights group to do this work. From that, this is the evidence we have, we have presented it in written form, and I will answer questions in detail as we go along.

The Chairman: Excellent. Thank you very much. Mark Donkersley.

Mark Donkersley: Good afternoon. I am Mark Donkersley, managing director of a company called e-Safe. I have had some 30 years in the IT sector and since 2009 have been working to develop an operation currently based in Salford, Greater Manchester. Our task is to deliver early warning and safeguarding risk, predominantly into the education sector. We monitor approximately half a million students and staff in the UK from Salford. We also have a much smaller but nonetheless important group of school and college customers in Australia.

Our service is basically a combination of technology which is deployed to the school or college devices; the school environment. That technology is effectively watching the material coming to the device screen—so your laptop, what images are appearing there, whether they are moving or static; it is looking for pornographic material in that sense. It is watching the words and phrases coming to the screen, it is looking at the keystrokes entered into the device, and it is looking at material and activity conducted from connecting devices, so pen drives, downloads from mobile phones, that sort of thing.

When the technology detects material it feels is inappropriate or it matches what we call our threat libraries—these are literally tens of thousands of terms, phrases, euphemisms, slang, in multiple languages associated with a range of behaviours, whether it be paedophile grooming, child abuse, FGM, bullying, self-harm risk and so on and so forth—if something triggers, we receive a screenshot of what the user was looking at on the screen at that moment. That screenshot is reviewed by a team of multilingual behaviour specialists, as I say, based in Salford, and they will review that incident in context and, depending on what they believe is going on, they will escalate that incident if necessary to the school or college, going through to nominated contacts—it could be a head teacher. If it is illegal or life-threatening, the

incident is rung through in real time, so something detected now, at half past three in the afternoon, is going through to the school at half past three in the afternoon. There is then a protocol that is tiered down so that you have still serious but not life-threatening or illegal incidents sent through the same day on encrypted reports, and down to lower level material which goes through weekly and monthly.

We perform that function also for a number of UK police forces. With regard to the police, we are monitoring sex offenders who have been released back into the community where the courts have determined that they should be monitored. Clearly, there we are exposed sometimes to grooming activity, certainly child abuse imagery, and I suppose the differentiator, the reason why the police and schools use us for the service I have described is that we apply specialisation; we remove the burden of a school or police officer attempting to look through this material and identify whether there is a risk that needs escalating. We are performing that function for them.

We are a private company, funded privately with the exception of additional funding from Greater Manchester, which wishes us to grow our international monitoring unit within the confines of Greater Manchester. That is e-Safe.

Baroness McIntosh of Hudnall: What I struggled with a bit, Mr Donkersley, when I was looking at your evidence was that I could not immediately—this, incidentally, is not the question that is written down in front of me, so forgive me if I pick up on something else. Could you say something about consent in relation to the monitoring that is going on, and also, where the content that you are viewing or monitoring is evidently self-generated, that is to say, the child or young person is creating it themselves, do you have a different view of that from the view that you would take if it were material coming in from outside? Can you also talk a bit about what happens once you have notified a school that something that your protocols regard as untoward has occurred? Do you advise the school about how to take that forward? What do you expect them to do with the information that you provide to them? What, if any, redress or appeal system might there be for a young person who feels they have been, for example, unfairly targeted?

Mark Donkersley: First of all, with regard to the education sector, we are monitoring behaviour on school devices and in the school environment. A student in the UK will have signed up to a code of conduct, an acceptable use policy, which determines what they should and should not be doing, what is allowed and what is not allowed on school equipment, in the school environment. At that level, we are not monitoring a personal device per se, unless it has been brought into school and is now being used in the school environment. We are delivering a service which is addressing or helping to address the school leaders' and chair of governors' statutory duty of care regarding safeguarding and protection.

Baroness McIntosh of Hudnall: Can I stop you for one moment, just to fill in one particular blank? Is it purely voluntary that the people who access your service choose to avail themselves of it and, if they do,

presumably they pay for it and that is a discretionary choice that they make from their school budgets, is it?

Mark Donkersley: Correct. There is now statutory guidance from the DfE which in theory compels schools and colleges to provide appropriate monitoring, without really being too clear about what appropriate monitoring is. You are correct: a school determines that the early warning safeguarding service that we can provide is something that they require; they see value in it; they purchase that from e-Safe.

Regarding the material we are looking at, to some degree the individual is anonymous. What we see is a user ID, so not "John Smith" but a user ID. We see that user ID has worked on a particular device—Laptop 01—and at a particular time and date they have viewed a pornographic image, bullied somebody, whatever. Often we will not know whether it is male or female. That degree of anonymity also gives us objectivity in the review process. One of the challenges for schools, if they were attempting to do this internally, is to say, "Oh, it's John Smith again. He's always doing this—ignore it." We review absolutely every incident. What we are looking for is not necessarily the obvious material; it is what we call the ones and twos. What I mean by that is, if you look at the behaviours we detect, invariably the markers are incredibly subtle. FGM does not take place in school but young people on occasion will leave a marker, albeit subtle, about a concern they may have which is one or two steps removed from FGM, but with our specialist review we can say, "Right, OK, there's a potential risk here. This looks wrong", and escalate it through. We have that objective approach.

When we find something, we basically inform the nominated individual at the school. As I said earlier, if it is illegal or life-threatening, invariably a head teacher will be on the escalation list. Bearing in mind we are doing this throughout the year, the behaviours we detect are not confined to the school bell starting in the morning and ringing in the afternoon, clearly; it is 24/7 and it is every day of the year. Lots of our incidents are escalated through activity on evenings, weekends and school holidays. Invariably, although the volume decreases, for example, during the six-week school holiday in the UK, the proportion of incidents which are very serious during that period is much higher. We are currently probably looking at 12,000 serious incidents a month across all our schools. When you look at the school holidays just gone, we were probably averaging something like 200 serious incidents a week. A high proportion of those were illegal, life-threatening, and therefore, again, we are filling a gap that a school would find very difficult to meet regarding attempting to monitor behaviour, and what has happened there is the devices have travelled home with the student or the staff member—because we are monitoring staff as well.

Q80 **Baroness Quin:** The question really is about trends and changes recently. I think we would like more information about what kind of harmful or potentially harmful behaviours you have encountered during the monitoring and if there has been an increase in different, specific types recently, and if there has been such an increase, to what do you attribute that?

Mark Donkersley: In the written evidence we submitted, we illustrated that at secondary level there has been almost a doubling of the volume of incidents that we have been reporting and escalating back in, and it is an across-the-board increase, across all behaviours. The areas which probably give us most concern regarding increase are products such as Chatroulette. I am not sure if the Committee is wholly familiar with Chatroulette, but in very simplistic terms, these are applications—I am sure Derek can explain it technically as well—where a user basically goes online and says, "Hi, I'm Mark. Is there anybody out there who wants to talk to me?" You can imagine that you end up anywhere in the world talking to anybody. You might find yourself in the middle of some online sex act or, as we have detected, directing child abuse behaviour in some other country from your position on your laptop. The Chatroulette sites are figuring highly in the more serious behaviours around sexting and abuse. They are also the more difficult ones to trace. Clearly, we know that a staff member or a student was on this end of the chat sequence, viewing whatever or conducting whatever. It is very difficult for the authorities to trace the other party, which can literally be anywhere in the world.

Are there reasons for the increase? We see a lot of circumvention of security. What we are looking for, the behaviours that we identify, are not new; they have always been around. Clearly, the digital environment today offers, maybe with some of the behaviours, a vehicle to make it easier to conduct them or whatever, but we work on the basis that at technology level it is impossible to protect completely: no matter how high the wall is, whether you have barbed wire on the top, people find ways through it, under it, over it, whatever. Our expectation is that someone will circumvent this, and because of social media in particular, when circumvention occurs—and here another term is very prevalent, proxy avoidance—with proxy avoidance, you are basically going to a very benign website, which becomes a launch pad for anywhere on the internet. Every school in the UK and many schools abroad put in what we call edge-of-network filtering systems. These are looking at the broadband feed and they are looking out for things such as proxy avoidance, as well as blocking material from *Playboy* or whatever it happens to be.

With regard to proxy avoidance, there are certain standards that these sites conform to and usually they are picked up, but these things are being created daily all over the world. What we find is, for instance, on Monday this week we picked up proxy avoidance sites we had never seen before. They could have been created at the other side of the world but the social media engine has got through—people have identified this and said, "I'll go and try it out in school today". Basically, what it allows you to do is completely bypass all the security, and once you are on the proxy avoidance site you can do literally anything and nobody can, in theory, see what you are doing. We can, because we are looking at the device, so we can see that the person has put a bet on the 2.30 at Kempton even though betting is not allowed in school; we can see that they have looked up pornographic material, or whatever it happens to be.

We are seeing an increase in proxy avoidance sites which the edge-of-network filtering systems are not trapping. We will report it to the school—so we report, "Someone has looked at pornography and they have been on a proxy avoidance site. It is called XYZ"—and the technicians in school will no doubt run off and put that in to block that site, but then another one pops up. It is a viral network through social media; people very quickly hear about these, they know which ones beat the system, and they start using them, and then they are looking for the next one.

Baroness Quin: I understand that obviously you report back to the school or college or to the police force, but if in the course of your work you have general concerns because of the rise in a particular kind of activity, do you report that to anyone? What do you do, apart from coming to speak to us, with your overall concerns rather than your relationship with particular schools and police forces?

Mark Donkersley: Our service is confidential to the target customer, the school, so we do not divulge and discuss the detail of what has been going on there. Yes, we do generate analysis of behaviour, our experience of monitoring currently half a million students and staff, and we are incredibly keen to share that material with policymakers and whoever else feels it is worthwhile for them. Our aim is to safeguard and protect, that is what we are passionate about, and that is what we are doing for our customers but, as in sessions like this, we believe there is information that we can provide that can assist whether it be policymakers or just the general understanding of what is really going on out there, because we have this unique window. We are not inviting people to tell us what they think is going on and fill out a questionnaire; we can see it. We know it is happening and we know it is happening to that volume.

Baroness Quin: I also ought to ask the second part of my question, which was: do you see any evidence that harmful behaviour associated with the internet disproportionately affects girls?

Professor Derek McAuley: We have not engaged in this sort of monitoring. The scale of what we have done is qualitative data, which I would not like to go on record as saying definitely shows one way or the other; it would all be anecdotal. We simply have not done that.

The things that one can do legally and that Mark is talking about I would not be able to get through a research ethics committee at my university. I would not be permitted to do that research.

Mark Donkersley: Unfortunately, for the reason I mentioned earlier, in the main we do not know whether it is male or female, unless we can see through the evidence of the actual incident, or it is reported back to us, "That was a female student" or "That was a male member of staff."

Baroness Quin: Do you have any anecdotal feeling about it?

Mark Donkersley: Anecdotally, we would say that the gender which is on the receiving end of a lot of the sexting-type behaviour is definitely female. It is female images we are seeing being passed around. That is

not to say there are not male images as well but it is predominantly female.

Q81 **Baroness Benjamin:** I would like to move to age groups. It has been stated that children and young people have significantly different capabilities and expectations. In the course of your work and the research you have done, do you see notable differences among the various age groups, and is there adequate knowledge and expertise within the industry to address the needs of children of different age groups, between, let us say, zero and 18?

Professor Derek McAuley: Seven minutes before I came into this room there was a Twitter message: 67% of under twos in Sweden are online, which was announced at a workshop today. That is a fairly spectacular number. I think, having watched some of the evidence previously. This is where the issue of trying to draw a very hard line and saying there is a certain age at which suddenly everything is understood by a certain child is—and I am a technologist—socially not sensible. Children develop at different rates. What they are sensitive to is highly context-dependent. We have an example of a six year-old girl becoming very upset simply by seeing an advert about Ashley Madison, the dating website for married people, because her parents had gone through a divorce. The thing that will actually upset very small children does not have to be illegal and it does not even have to be something that you might view as something that should be banned, but it is something that upsets that child.

The industry has done nothing to address tools that would allow much more subtle voluntary filtering. Most of the work we have done goes down only to five year-olds—again, we would have a real challenge if we tried to research younger than that—but five to 10 year-olds are mostly concerned about not seeing things they do not want to see. They are not out there trying to find things. One of the challenges they have is that if something happens to them, they do not know where to go; they do not have a safe place to go and ask about it, for fear that it would be seen that they have done something wrong. That in one sense also extends to the parents; they have a fear of discussing these things with parents. As a technologist, in my village I happen to receive lots of requests: "Can you come and clean up this PC because my son won't show it to me?" I will go and do what is needed and explain to them why they have all this malware. Most of it is because they were trying to download free games but there is a lot of other content they do not want, and they do not feel they have somewhere safe to go for advice.

There are a number of things here. There is obviously illegal content, and you have heard evidence about how to deal with that. There is content that is inappropriate in different contexts. I think we have done very little to deal with children being online, all the way from the tiniest, the 67% of under two year-olds. People are giving them tablets and just saying, "Here you go."

One of the comments I would make which calls back to the previous question about harms is that the advice used to be to keep the computer in a public space, but those computers did not have cameras in them, and there tended to be one in a house, whereas now every

smartphone—and the kids are demanding smartphones earlier and earlier—has a camera. It has two cameras: one so you can see the screen and one that points at you. The technology we are putting into kids' hands that they take to their bedrooms is one of the things leading to a wave of these new apps that have this particular behaviour. All the common-sense advice we have about using technologies in a public area so that people can see what is going on and there can be discussion is just not happening. The danger is that, without some action by the industry to put in place mechanisms that protect the youngest children from things they really do not want to see—not that they are illegal or anything else, and that includes issues such as safe search. Age-appropriate search would be a revolution, and it is not beyond the wit of great scientists in those search companies to figure out.

Baroness Benjamin: In the light of your work with children, do the different age groups understand their rights, and in some cases realise that they are breaking the law by sending inappropriate imagery?

Professor Derek McAuley: I fear that most adults do not understand their rights when it comes to online platforms. How many of you read the terms and conditions? The basis of informed consent as the basis for all data processing is somewhat flawed, to say the least. There is a fundamental problem in that certainly in terms and conditions—and you saw in some of our evidence children talking quite eloquently on terms and conditions—the reading age is often 21 or 22. It requires undergraduate if not postgraduate education to read the text—not to understand the law and the legal implications. I do not think the kids understand it. They sort of know something they are not supposed to do at 13 because it says something about 13 in there but also I think a lot of them do not even think about their behaviours. The classic one that comes from the Chatroulette would be young girls dancing in front of a camera in their bedroom, semi-clothed. That would be something they might not even think about but it is harming themselves long term, and who knows who is at the other side of that conversation?

There is a real lack of understanding around these issues, and the repeated dangers of the internet. One of the lessons that came out very strongly and one of the reasons kids liked our youth juries was that they were a different way of getting the message across, an entertaining way. The way I would put it is we have a world-class creative industry; it should be doing something about communicating this at every age group. There should be a plot line in "East Enders" or something, or whatever kids watch. It is that sort of thing that I think is important, to get age-specific information to people, but also through channels that they will enjoy.

Mark Donkersley: I would certainly concur with Derek's comments there. I think the point I would make across all of certainly the primary and secondary sector in the UK is that the issue we have seen for many years now is mental health. We put in the evidence that that has massively increased but it has always been there. When you look at the various independent reports that have been done for NHS England saying that 50% of mental health issues are established by the age of 14 and 75% of mental health issues are established by the age of 24, that is

squarely within that primary, secondary and further education group. The volume of markers that individuals will leave in the IT environment is incredible to us. They are subtle; they are not the in-the-face pornography or anything like that; these are either cries for help or the very low-level things going a bit awry at home, "I don't feel comfortable", the depression indicators, that sort of thing. We would say it is in that area. If you look at primary, across all behaviours, you see much more change over time. We genuinely believe that is because of the age group and because of the early warning of the risk, and the fact that teachers are then able to intervene, they can modify the behaviour. They have a much greater struggle doing that at secondary level because of the age of the individuals.

We also see that the age group is lowering regarding skill set and use. You used to think it was the elder siblings at secondary telling their primary school siblings new ideas and ways and things that maybe they should not be doing on the internet and with digital equipment; now it is almost the other way round, that primary age is informing secondary. They are coming up with the ideas, which is incredibly dangerous, obviously.

Baroness Benjamin: You mentioned protection. What are the key technical challenges about protecting, when we talk about protection, especially with age verification? A lot of people say it cannot be done, you cannot do this, you cannot do that, but what challenges do you think we face in trying to protect children through age verification?

Professor Derek McAuley: Mark has already pointed out that there is no technology that someone smart cannot get around. It is always a bit of an arms race. The other side of this is that I would be deeply concerned that most of the systems proposed—and there was a report very recently—involve convincing people to hand over personal information to a random website in the hope that it verifies their age, when in fact that is one of the things we should be teaching people not to do, to go to a random website and hand over credit card details or something else. The various mechanisms proposed are somewhat dubious.

I would look at something such as UK Verify, which was set up by the UK Government as the way to do identity for all government services. It has been rolled out already for universal credit, and asked of that group. It was not designed for age verification but that was co-designed with the civil society organisations, which have a concern for privacy, and it passed their test for identification. I would start from something such as that as a way forward. Many of the, let us say, commercially proposed ones, are deeply worrying—and I say that as someone who spends most of their life trying to avoid these people tracking me, and that is what I have taught my children, because being tracked is just as bad. The age verification mechanism becomes very difficult in a world where one also wants some privacy, not necessarily for dubious reasons, but just because I do not want them tracking me all the time. I think there is a challenge there. I have yet to see a solution that is satisfactory but, as I always say to my research students, until you have proved it is impossible, it is still possible, so you should keep looking.

Baroness Benjamin: They can track you if you want to gamble or you buy things on the internet, so what is the difference?

Professor Derek McAuley: Okay. I use a different identity for every service I use, so I have hundreds of email accounts. I also take measures in my browsers to stop them tracking me. It is perfectly doable. In fact, Microsoft nearly made it the default but the advertising industry went after them and shut them down. Tracking is something that one can avoid, but as soon as you say it will become a legal requirement for people to track, then those of us who value privacy over the convenience—which is all it is, because I am perfectly capable of using these services individually but I refuse to be profiled across everything I do.

Q82 **Baroness Bonham-Carter of Yarnbury:** From tracking to filtering, please. Does the present regime of filtering protect children adequately at school and at home? We had some written evidence that when parents decide to use a child-safe filter service from their ISP, the filter will only apply to the smartphone if the child is connecting to internet at the home, not when the child is connecting via the mobile network. It does not sound as if filtering is a very satisfactory way of protecting children from content.

Mark Donkersley: It has a place, definitely. It has an ability to effectively close the tap, but it cannot close it completely. We have talked already about circumvention and proxy avoidance, for example, as a way of circumventing filtering. The challenge with filtering is obviously to have the balance there to allow the user to exploit the power of the internet and at the same time protect them from the risks and dangers.

Baroness Bonham-Carter of Yarnbury: I am sorry. There is something I did not understand there. Is the child trying to overcome the filter? Is that what you are saying?

Mark Donkersley: Oh, yes.

Baroness Bonham-Carter of Yarnbury: The child knows that his parents have put a filter on?

Mark Donkersley: Potentially, yes, but this is where monitoring at the device provides the belt-and-braces approach, because even if it is circumvented, or, as you said, you step into a different environment and the filtering is no longer there, the fact that the device is being monitored allows you to identify that that individual is now looking at "Call of Duty" and they are only six, whatever it happens to be. It goes back to the earlier point as well, I think, that age verification itself is not the biggest challenge in the world, as Derek says; there are ways and means but people will find a way round it, but if you are monitoring as well, that is what is telling you someone is gambling at the age of 10 or someone is going on to Facebook when they are three. The evidence is there. The challenge then, I would argue, is to inform the parents and make the parents appreciate the challenge.

Baroness Bonham-Carter of Yarnbury: That was going to be my next question, exactly that. Are the parents alerted to the fact that the child is using these sites?

Professor Derek McAuley: BT—I have never used one of these services myself; I would rather have a conversation with my children about it—would flag up sites visited and things such as that. There is a real danger with that, though, as a general mechanism, of showing too much detail directly to parents, and that is one interpretation, because you go to a website today and content is pulled from hundreds of machines. The adverts are coming from a completely different company, and who knows what the advert is? That is easily misinterpreted. It is one thing to have a company with experts who will disambiguate that but, again, we have not yet been able to figure out ways in which to represent the topics that the child is looking at; so rather than say, "These are the websites they went to", and leave it to a parent to try to interpret that, saying, "Your child is showing an increasing frequency of attendance at these sorts of sites" and prompting a discussion. Again, the social development is different for all children. Anyone who has more than one child will know that they have two different children, they develop socially differently, and the content that a parent lets a child have access to in the home will vary depending on whether you believe your child is ready for it.

There is a different point from the very first question. You had the Internet Watch Foundation in here, and for illegal content, and for clearly specified adult content, most public wi-fi providers and the cell phone companies implement the same sorts of filters by default that, for example, Sky do, so it is true that in many places they take the phone it will still have the same sort of filtering going on, but at that point it is strictly filtering; it is not reporting, because there is no parental-house relationship to report it to if it is a pay-as-you-go mobile.

Baroness Bonham-Carter of Yarnbury: A quick supplementary, which I think you were touching on, which is that of course you do not want the filters to filter information that is of help to young people, on sexually transmitted diseases or whatever. That is another problem, presumably.

Mark Donkersley: It is, and certainly within schools, again, this presents a challenge, because you have on the one hand probably a vast swathe of material suggesting that individuals have been on these health sites, whatever, which at first glance may be indicating some sort of health risk, but it is all very genuine and not an issue. That is what we are saying: at the beginning the challenge that school leaders have is that they do not have the resources with the specialisation and the time, and they certainly do not have the budgets available to just sit there poring over this material, whereas we do.

Lord Sheikh: I wanted to refer to FGM. Mark, you touched on that very briefly in your introduction. It is a subject which concerns me greatly. I have spoken on this matter in the House of Lords and, more importantly, I am the co-chair of the All-Party Group on Sudan. I led a delegation to Sudan recently and we looked at issues concerning women. Following that, I am sending a group of British parliamentarians to Sudan. What is happening on FGM is, of course, this is still going on with regard to young girls in this country but also girls are being sent from this country abroad for this horrible action to be taken. You mentioned FGM. What work have you done and what degree of success have you achieved?

Mark Donkersley: We collaborate with many organisations which are specialists in the different types of behaviour. In this particular area the challenge is that it is not very obvious. Someone is not going to say, "I am worried because I am being lined up for FGM." They are not even going to use the phrase, the terminology. It is going to be a subtle, young person's way of describing a concern that they have an inkling they are actually being sent away from the UK and they think, "This is going to happen to me. This is why I'm going", and that concern is being expressed. We work internally to almost create that youth-speak, so we understand the nature of the issue, we appreciate the marker that we are looking for, and we said, "Okay, how is a young girl going to articulate a concern around this, given that they are probably not going to mention FGM?" We come up with all these different markers, terms, phrases, and that is what we look for, and when we tease them out, great.

We are also made aware by various organisations of, shall we say, the code that is being used at parent level to disguise FGM, and we incorporate those markers as well. I will not quote one here in open forum, but sometimes we might have a young person saying, "I've heard my parents reference this and I think that is code for circumcision of some description." We will find that incident, review it, and in the particular way I have described, that would be escalated to the school to intervene.

Lord Sheikh: My own feeling is that of course we have to change the culture, although of course it is a criminal offence, not only here but in overseas countries. Therefore, if a role can be played in changing the culture, I think we would have a better chance of success.

Mark Donkersley: Sure. I would also point out that we have over a million students at primary and secondary who do not speak English as a first language, and you can flick a computer now and change that keyboard to Urdu, Farsi, Polish, whatever, at the touch of a button. Often, the more serious behaviours, again, are being articulated in a foreign language, maybe Urdu script or Arabic script. We are fortunate that we can detect that. We have to make sure we have the markers in there and that we understand the cultural emphasis, and it is a major challenge for us to be completely on top of that.

Q83 **Lord Sherbourne of Didsbury:** Can I ask about the role of Government? As I understand it, the Government produced some proposals at the end of last year requiring schools to put in measures to protect children from harm online, if I am correct, and there are some proposals in the Digital Economy Bill. What further things do you think the Government should be thinking of doing? What would you like to see them doing?

Mark Donkersley: A number of different things at different levels. It is our evidence and experience that nearly a third of all serious behaviours we escalate are the result of offline activity—nowhere near the internet, no online activity at all. There is very little, if any, mention of offline behaviour and how you should be trying to interpret and monitor that in

any of the guidance being put forward by Her Majesty's Government. That is an issue. Nearly a third is a big hole.

Lord Sherbourne of Didsbury: What would you like them to do exactly?

Mark Donkersley: First of all, educate the inspectorate and the school leaders that this is not just an online issue. It focuses the mind in an area; okay, it is where the majority is happening, i.e. two-thirds, but one-third is a big amount to be missing, to have invisible.

Lord Sherbourne of Didsbury: The Government should be doing what? Educating?

Mark Donkersley: Yes. In statutory guidance that has been provided there needs to be more understanding of the reality of how the digital environment is being used. Offline activity is a significant proportion of activity and there are a lot of markers there which are of value to school leaders.

I would say the second point around this is that we see what we do as a public health issue. We regard the evidence of what we see as a public health issue. We have talked about mental health, about the fact that the emphasis is on young people where mental health issues are established. The NHS is spending huge sums of money on mental health, and there are all sorts of reports out there saying that intervention at an early stage is not just going to help the individual, it will have this wider benefit and value to the NHS and other government departments. We feel that, alone, purely the issue of mental health is more than adequate justification for the Government to be mandating monitoring across schools.

Lord Sherbourne of Didsbury: You want to have mandatory monitoring in schools?

Mark Donkersley: Absolutely.

Lord Sherbourne of Didsbury: Can I ask Professor McAuley what your thoughts are on what the Government could do?

Professor Derek McAuley: The one thing that came very clearly from the youth juries was this comment that people did not know where to go when they had a problem. We have listed all these problems that people have, "Don't do this, don't do that." It is a bit like saying, "Don't fall over and break your leg" and then fail to provide an accident and emergency service. They need somewhere to go. This applies to parents as well; the parents often do not know how to react. From all age groups, we need children to be able to feel they can go and talk to someone safely about something that has happened.

Lord Sherbourne of Didsbury: What kind of people would those be?

Professor Derek McAuley: I would hope it would be within the school system. It would be a function that would be defined, that would say, "This is the amnesty. Come here and tell us what happened and let's get this mess cleared up." Monitoring is one thing but without sitting down and doing a lot of research into what he has done—which I might find hard, getting to the heart of how much of it has started off in a small

way and escalated over time; was there a point at which we could have intervened? As with mental health issues, the question is whether there is a point at which you could intervene much earlier with assistance and more engaging education. The internet is a great thing; it is not all bad. We have to be careful.

Q84 **Earl of Caithness:** Can I take you on to data protection? Does increased monitoring of online activity have implications for the data protection of children? Is that going to change with the EU regulation due to come into force imminently?

Professor Derek McAuley: Absolutely; it is a data protection issue. The GDPR brings in tighter constraints on consent and the types of information that are considered personally identifiable information. If I look at the industry in general, they get away with it on data protection. In some countries they are quite hot on enforcing it. I think, to be honest, how the GDPR is going to play out will depend on the next two years of implementation. How harsh are we going to be with the interpretation of those rules? We could decide to take strong interpretations of them, which would include significantly increasing the requirements vis-à-vis children and making sure they understand what they are doing. Continual, ongoing consent; repositories. One of the things that children said was, "I can't even find out where all the information about me is." There is no obligation for someone who holds data about me to tell me they have it. There is a legal obligation to make sure it is up to date but they do not have to contact me about that. There are many mechanisms there where we, not just in the UK but generally across Europe, should be taking a much stricter interpretation of data protection law. The GDPR gives us this opportunity—two years to try to clean up our act and get a bit more responsibility into these businesses.

It absolutely applies to children. The companies that have the under-13 rule—which of course is not a UK law but US federal law; we do not have to have anything; the UK has not stipulated anything about age—know that kids under 13 are using the site and they are not doing anything about it. There is not even an attempt to do age verification. Much as we say it is difficult, the fact that they know, blatantly, that they have kids on there means they are not complying with the data protection law. All we need are a few serious court cases for that £2 billion or whatever—2% of maximum global revenues; it might wake some of them up.

Earl of Caithness: Given what you have said, do you think there is enough protection under the existing law, and is it just that the whole thing is so spread out that nobody has brought it all together, or there is no group that is bringing it all together? How does this affect 18 year-olds? I was thinking of the subject access request. Should a child have to pay £10 for that? Does that not put a child off, if they even knew about it?

Professor Derek McAuley: Indeed, and given how many people hold data about me, at £10 per subject access request, I would be bankrupt. Under GDPR—I might have to bring a legal colleague in here—I believe it is supposed to be online and free, to be able to ask at a reasonable

frequency. Given that all of this content is digital these days, it is all ready to be made available if someone can authenticate themselves. In that sense, it should be free, so one of the things we might work on are the tools that would allow children to be able to access that and to understand what it means, and then to start to educate them about their digital footprint.

The Chairman: Our legal experts in the next session may help us with this one as well.

Q85 **Baroness Kidron:** You have segued into what I was interested in, which is this question about industry responsibility. I think it is palpable to us as we take evidence that people talk about schools' responsibility and parental responsibility, but when we try to get to the nub of what a parent or a school could do, the tools are not really available for them to make change. It seems that maybe industry has to help make change. I wonder whether each of you, from your own point of view, could say. You have mentioned things such as UK Verify—why does industry not do something around that?—and terms and conditions, in your report—why does industry not do something about that? I would really like to hear from you what industry could do that is a little bit more radical and a little bit more user-friendly when we are talking not simply about protection but about the normative use of "children being children" in this digital sphere.

Professor Derek McAuley: Stop trying to monetise every piece of data. The assumption that there is a pot of gold at the end of the data rainbow drives industry at the moment. Many of the dreaded internet-of-things devices, in which the next generation of devices will have embedded technology—they may not even have a screen by which you can give consent—will be streaming data somewhere and people will be processing it. Internet Barbie dolls are already on the market. There is no point at which anyone is perceiving they are giving consent to having their audio or video streamed to the far side of the planet. This thing would stream my audio if I pressed the button to servers in America. That will be embedded in our world.

This is only because there is a belief that somehow after you have bought the product they will be able to monetise the data somehow, so they must grab all this data. It is irresponsible business models that are driving this. It is people thinking that, instead of just selling a product that has technology in it, they must sell a service and track you for all time. I think in industry there is this mind set which is driving everyone at the moment because they think that is what is making Google a lot of money. It is foolishness and in the long term will cause harm, in the sense that in the long term people will not adopt these products if they are constantly reporting on them. It is in industry's own long-term interest, which of course is one of the challenges industry has, that it does not tend to think long term. It would be better if they were much more attuned to the privacy issues and not sharing data when they do not need to. It could do a lot itself.

Mark Donkersley: We are clearly coming from a different angle on this, in that where we are receiving and where we are viewing behaviour, the

digital environment is the vehicle; it is not the cause of the behaviour in the vast majority of instances.

I would say, going back to Chatroulette, that yes, there are examples—there is anecdotal evidence where we could see that an individual has inadvertently stepped into something and that environment has then led to harmful behaviour and risk, but in the main they are the vehicle as opposed to the actual instigator of the issue. It is very difficult for me to offer a panacea for a fix for the technology industry.

Baroness Kidron: Is it not the case that most of the big companies are very well aware of the sorts of markers you are talking about and of the lack of offering of the safe space that Professor McAuley talked about? Is it not true that most of them would have—what did you call it—depression indicators? They would have at scale, for billions of incidents, what you are doing in a very small way in schools; and rather than being monetised, that could be put to social use for the under-18s.

Mark Donkersley: Yes. I would say that they are not applying those markers to any degree. It is veneer-thin. There is no way that some of the Leviathans that Derek mentioned, with their population of users, could handle all the material that would come back the other way if they had sensible markers in their system to identify risk and misuse, and so on and so forth. I think it is wrong to expect them to be able to do it. Yes, they could always do more than they currently do. As I say, we have evidence, experience, where we see some horrible situations. We have managed to alert somebody to intervene and protect, help and support an individual here, but there is probably something far worse that has happened at the other side of the world that nobody is able to trace.

The Chairman: I have to call matters to a halt as we have gone miles over time, but that is a sign that we have been absolutely absorbed by your evidence. We are extremely grateful. Thank you both very much indeed.

If you have views on the role of the education system, whether PSHE education should become a statutory subject, for example, please drop us a note. That is the outstanding area we were here to explore with you but everything else we have covered very fully indeed and we are very grateful to you. Thank you for coming.

Facebook – written evidence (CHI0044)

Inquiry: Children and the Internet

Facebook is pleased to be able to provide our contribution to the committee to this important inquiry.

Risks and benefits

The Committee is right to consider both the risks and benefits of Internet use for children. This continues a public policy precedent in the UK which the Byron Report created in 2008 for considering this topic in the round. Professor Byron summarized the available evidence at the time showing the considerable benefits of online services and technology for child and especially adolescent development, whilst also proposing ways to mitigate emerging risks.

In a similar vein, Facebook seeks to ensure that all its services maximize the benefits for everyone using them, and aims to minimize the risks. We provide special protections to under-18s and provide them with particular support and specific tools to manage their experience. Some of the content rules we have in place for the whole Facebook community are particularly relevant to under-18s – including that we don't allow most forms of nudity and pornography in any form.

Some 1.71bn people use Facebook each month (most of them every day) and over 500m use Instagram. This obviously includes many millions of young people who become eligible to join these communities on their 13th birthday.

There is significant evidence that with the right tools and good advice, young people can have a positive experience online including being able to manage the inevitable risks they may encounter around content, conduct and contact. Like the Committee, we look to academic and safety organisation experts to inform our work to keep young people safe.

One example of this is the work of a dedicated engineering team who cooperated with experts from Berkley and Yale universities to find ways to encourage more compassion and empathy in situations where a young person feels upset or harassed and needs help to resolve the situation.

As adults, most of us have learnt to find the right language to express our disquiet in order to resolve awkward situations within personal relationships. In adolescence, not having the right words and some confidence to use them are often the cause of unhappiness and event depression among teens. Our team found a way – which they called social reporting – to give people the words and the tools to resolve such problems. It allows someone, for example, to manage a situation in which a friend has posted a photo of them they don't like. Our reporting flow asks a set of questions, then provides suggested language to ask the person to take that photo down, and evidence shows that this works and leads to more empathy between the individuals concerned.

We are constantly looking to improve our work in this area – understanding both the risks and the benefits of social media for young people. So we believe expanded partnerships with NGOs, Government, parents, young people and the experts will be vital to getting that right.

Education

The Committee will hopefully get responses to their questions on the role of the education system from practitioners and organisations with direct responsibilities in this area. We see our role as being supportive of educators and establishing the best possible partnerships. There are many examples of tools and support that we provide to young people, parents, teachers and others to make sure that they are able to access good advice, and to control their online experience.

For example we have created a guide for educators in relation to bullying https://www.facebook.com/safety/bullying/educators/ and a Bullying prevention hub, https://www.facebook.com/safety/bullying/

Our Help Center and Safety Center offer detailed, audience-specific resources for families and teachers, with information tailored to specific contexts. And our privacy basics is a simple guide to managing your data on Facebook (https://www.facebook.com/about/basics).

We agree with the view implicit in the Committee's questions that trusted advocates, peers and educators are far better placed than companies to convey effective training and education. So we support the work of experts and organisations who deliver training directly, including Childnet and the Diana Award Anti-Bullying Ambassadors in the UK, to reach as many schools and young people as possible. We also look to take what we learn in one country with a partner and export it to other countries. In May 2016, we launched a new resource 'Anti-Bullying Activism on Facebook' - a guide for schools who would like to set up their own anti-bullying initiatives on Facebook, which was developed in partnership with the Diana Award.

Governance

Facebook's services broadly look and feel the same for under 18s and adults. There is no 'Facebook for kids' unlike some other services. However, since everyone's Facebook experience is unique - depending on who they are friends with, what Pages they like and what they are interested in – in reality a typical teenager's Facebook experience will be very different compared with a typical adult.

There are some features regarding under 18s which are designed in:

- Under 18s do not see commercial content for age-related products such as alcohol, gambling or dating services. This means they will not see ads for such products or content from relevant branded Pages. This is an example of how young people are better protected from adult commercial content on our services compared with other media such as broadcasting, printed or outdoor media.

- We make sure it is not possible to search young people by the name of their school.
- We can age-gate an individual piece of content once it is reported to us, on the basis that although the content is allowed on Facebook, we judge that it might be disturbing for a young person. This could include gory news footage after a terrorist attack. Age-gating means that no-one under 18 will be able to see the content.

In doing this we keep in mind that we aren't always the experts. This was the thinking behind the establishment of our Safety Advisory Board. This comprises a diverse set of experts and organizations (including Childnet) devoted to online safety to advise us on safety issues and the design of our products.

Legislation and Regulation

With some exceptions, Facebook's approach to providing products which serve young people well, including around safety, is not framed by regulation. We provide services which are accessible for free to anyone in the world who can access the Internet. We take safety seriously because we know that people using our services care about it, and it's a foundation for growth, rather than because we are required to by legislation. The features to protect young people described above – eg age-gating disturbing content, prohibiting nudity – apply globally, even though most countries don't have laws in this area. Our Help Center, Family Safety Center and other relevant resources are available to young people, parents and educators around the world.

One notable exception to this environment is the impact on our approach to young people conditioned by the US Children's Online Privacy Protection Act (COPPA). This law stipulates that organisations can only collect the data of under 13s with express parental permission. Like most online services that collect personal data, we consequently decided that we would apply a rule that a person has to be 13 in order to join Facebook. This rule applies globally though in a couple of countries we set the entry bar at 14 because of local data protection laws.

Overall globally we have found our industry-leading safety processes, partnerships and policies to be highly effective in safeguarding our young users, and this informs our view about the relative merit of specific national legal and regulatory requirements.

Our view has been largely aligned with the views of UK Ministers and policy makers. Tanya Byron's report in 2008 led to the creation of the UK Council for Child Internet Safety rather than new legislation. Facebook has been a leading member of UKCCIS since its formation and we've seen firsthand the value of Ministers convening a collaborative, multi-stakeholder approach to tackle problems and share best practice. CEOP and the Internet Watch Foundation are other examples of where the UK has led the way in expertise, joined up working and partnership including industry.

We therefore counsel the Committee against making radical recommendations to change this cooperative approach. That said, the issues facing young people online are constantly evolving as technology and their habits change, so it is

helpful for the scope and range of this work to be reviewed and where necessary extended. The UK should strive to remain ahead of the curve.

August 2016

Facebook and Google – oral evidence (QQ 108-121)

Tuesday 22 November 2016

Watch the meeting

Members present: Lord Best (The Chairman); Lord Allen of Kensington; Baroness Benjamin; Baroness Bonham-Carter of Yarnbury; Earl of Caithness; Bishop of Chelmsford; Lord Gilbert of Panteg; Baroness Kidron; Baroness McIntosh of Hudnall; Baroness Quin; Lord Sheikh; Lord Sherbourne of Didsbury.

Evidence Session No. 8 Heard in Public Questions 108 - 128

Examination of witnesses

Simon Milner, Policy Director, UK & Ireland, Middle East, Africa and Turkey, Facebook and Katie O'Donovan, Public Policy and Government Relations Manager, Google.

Q108 **The Chairman:** I rise to welcome you, Katie O'Donovan and Simon Milner. Thank you very much for joining us. We are very appreciative of you giving up time to be with us. Our inquiry is concerned with children and the internet. It is a big subject for us. You are very much in our thoughts as we get deep into this world. Could I ask you if you would be very kind and introduce yourselves, say where you come from, and make any opening remarks you would like to make? Katie, perhaps we will start with you.

Katie O'Donovan: Thank you for having me here today. It is good to join you all and to follow your inquiry as it has been going. My name is Katie O'Donovan. I work for Google UK in the public policy team, and I am responsible for our child safety work. Prior to that I worked at Mumsnet, a parenting website, where I was responsible for our policy and campaigning work there. Currently, I sit on the board of the Internet Watch Foundation and am a member of the governance board of UKCISS on online child safety.

Simon Milner: My name is Simon Milner. I am a policy director for Facebook, based in the UK but covering a number of countries, including the Middle East and Africa. I have similar credentials, in the sense of having sat on the UKCISS board and on IWF, and I am very much looking forward to our discussion today.

The Chairman: Thank you both very much.

Baroness Benjamin: I am sure both of you agree that in order for us to keep our children safe, protected and informed we all need to act and play our part in a responsible way with integrity. What do you see as the

role of your platform in helping to safeguard children online and inform children, parents, schools and others about the safe usage of your services?

Katie O'Donovan: We take our responsibility very seriously. Google as a company is 18 years old, which in internet terms is quite old. That gives us the ability to evolve as a company and develop our understanding of the significance of this issue. It is a matter we take very seriously. It is probably helpful to describe the approach we take in three ways. We have very strict terms and conditions for our platforms and where we host content. We ensure that those conditions are adhered to, so where people notify us that those conditions are not being met we will review those and, if necessary, take action.

We also believe that technology is really important. As a technology company, we feel it is within our gift to help on this issue. For example, we have tools like SafeSearch and restricted mode search for YouTube, which parents can lock on so there is a safer environment for their children in relation to those products.

We also have flagging mechanisms on YouTube where we can use technology to help us to respond quickly. We are also able to build bespoke products. Last year, we built and launched a product called YouTube for Kids. That is a safer and more collated environment for kids to enjoy and experience YouTube.

The final part of our approach is to recognise that technology cannot be the only answer. Some of these are societal issues that we have all been grappling with for many years and generations. Certainly, the internet makes them different and can complicate issues, but often they are not uniquely a technological issue. Therefore, part of our response is also to invest and work in partnership on education to help young people develop skills, resilience and intelligence and to be empowered so they can act more safely online. We ourselves run projects like Internet Legends, but we also work in partnership with many other safety organisations in the UK.

Simon Milner: Facebook is a bit younger than Google. We are just over 12 years old. I have been at the company for almost five years. During that time, I have probably spent more time on the issue of safety, particularly associated with young people, than on any other issue. To me, that is a demonstration that nothing is more important to us than the safety of people on Facebook, particularly vulnerable groups like the under-18s.

Like Google, we have a multifaceted approach, including what our policies are, the employment of hundreds of safety experts, our partnerships with safety organisation, which I am happy to talk about more, and with law enforcement. Some things go beyond safety organisations and need to involve law enforcement. Above all, it is about constant learning. In what I am talking to you about today I will demonstrate just how much the company has progressed over the past five years in what we have learned as to the best role we can play in helping to keep young people safe.

We are very much part of a safety chain, if you like, which involves young people themselves—there is an awful lot that young people do to help one another—their teachers, parents, other technology organisations, from whom we learn as well, safety organisations, academics and government. A whole group of us are involved in doing this, and we absolutely recognise that we have a central responsibility, given that this is about the use of our platforms.

Baroness Benjamin: How do you get to them?

Simon Milner: How do we get to whom?

Baroness Benjamin: To the people you want to know about your services and what is out there for them.

Simon Milner: It is a combination of things. It is principally through the service itself. When people first sign up to Facebook there are a number of steps to go through. We also make sure there are regular reminders about things like the privacy settings people have on their accounts, because we want to ensure that if people are sharing publicly they are reminded of that and understand what it means.

Baroness Benjamin: How are they reminded?

Simon Milner: They are reminded through a little pop-up that may come up. When people first join Facebook their default setting is friends only. This is for everyone, those under as well as over 18. If somebody decides to change that and wants to share publicly, we will notice that. Maybe after two or three times we may say, "Do you know you are posting publicly? Are you sure you want to be posting publicly?" We do that through the service itself and our help centre. We have just relaunched our safety centre as well, which is focused particularly on families.

There is also the very important role safety organisations play, because they reach directly to young people in their schools and can directly interact with parents and teachers. We do not rely just on communicating online; we communicate offline, often via these safety partners.

Baroness Benjamin: Do you have measures to ensure that children cannot search for certain items, such as suicide, self-harm, pornography and so on? What happens if children do come across that content, whether it is inadvertent or deliberate?

Simon Milner: Facebook does have a search feature, but we are not a search engine for the wider internet. I am sure Katie can talk about the role of search and Google in that. When it comes to the issues you have raised, particularly around suicide and self-harm, our focus is much more on how we can ensure that, if somebody is showing signs of such distress on Facebook, there are very straightforward ways they can get help through Facebook, or that their friends can get help for them. To give you an example, if someone you know is showing signs of distress, at worst is saying, "I am about to kill myself", or, "I am going to take these pills", there are very good tools on Facebook for you to get help for that person. If it is really serious and you alert us to it, we can contact the local police, who can physically help that person in distress. More

often, it is a case of intervening in their Facebook experience and saying, "Hey, somebody you know is worried about you. Here is where you can get help". In the UK, that would mean giving them details of the Samaritans so they can reach out and get that kind of help for themselves. That is the area we focus on. It is not about search for us; it is much more around when somebody is showing signs of distress.

Baroness Benjamin: What sort of response do you get if you tell somebody you are concerned about their behaviour and you give them guidance? Are they susceptible to this? Do they appreciate the fact that you have done so, or do they think you are interfering?

Simon Milner: Typically, we get a positive response. The best experts in this are the suicide prevention agencies. They have told us that they find this an incredibly valuable way to reach people at the most acute times of distress. That is the hardest thing. When you are walking down the street and see an advert for the Samaritans you may be feeling fine. It is only in those dark moments when you will not be and you do not necessarily see that advert. Because we can provide that content to you directly at that time, often, it can be exactly when you need it.

Q109 **Baroness Benjamin:** What policies do you have, Katie O'Donovan?

Katie O'Donovan: We have a number of different measures. Google as a search engine absolutely seeks to deliver the world's information to everyone and make it universally accessible. That is a wonderful opportunity for so much of the information, but, as you rightly pointed out, there are certain areas that can be quite difficult and challenging, particularly where content is not illegal but might not be appropriate for everyone, for example those who are more vulnerable. SafeSearch, which is a product we developed, can be turned on for any Google user. It can be locked on and password-protected, so a parent can do that for a child. That means it delivers only safe research results, so, particularly for pornographic images, it will restrict the corpus of the search results that you see. An Ofcom study released last week showed about 50% knowledge of that among parents. Therefore, it has quite a high knowledge base, but we could absolutely do more on that. It is of real interest to us to think about that and work with partners on it.

We also have a system called autocomplete. Often, when typing something into Google we want to make it easier for you to get the information you want faster. For example, if the question is about what time a film is being shown at a cinema, we can also complete that for you, but we realise there are particular topics that are very sensitive and you do not want autocomplete for that. We do not do autocomplete for terms to do with suicide or swearing, for people seeking pornographic material and for people seeking extremely violent material. People are still free to type those queries into the search engine, but it gives a bit of friction; it does not make it as easy as it is to find other things.

We work very closely with organisations on some of the controversial search terms. If people are looking for information around suicide, we have worked with the Samaritans to develop what we call OneBox. That is a noticeable block that comes up at the top of your page. If you search in the UK for terms around there, you will be pointed straight to the

Samaritans and their helpline number. The Samaritans have told us that that works very well for them. They often get phone calls where people have seen that number, and they are able to provide the expertise and support they do. Similarly, we do that for people who are looking for online child sex abuse material. We work with the Lucy Faithfull Foundation and the Stop it Now Coalition. They present information that is relevant to those people. We have a wider grants programme to enable charities to advertise on all our search terms for this.

Baroness Benjamin: Do you ever take anything down?

Katie O'Donovan: Google is a search engine. We do not host the sites that are linked through. Those are hosted by private companies, individuals or charities themselves. It is difficult for us. We do not have the ability to take down content from the internet, but we can de-list content that is notified to us as being illegal. If there is illegal material in the UK or in different jurisdictions, we will not link through to that once we are made aware of that information.

Baroness Kidron: Is there a public list of things where you do not autocomplete?

Katie O'Donovan: Our policy is public. I am not sure whether it is an exhaustive list.

Baroness Kidron: We could see if it included radicalisation terms or pro-ana sites.

Katie O'Donovan: Yes.

Baroness Kidron: Therefore, we could get an idea of the big picture.

Katie O'Donovan: Yes. Radicalisation sites is one of the issues in there, and I can certainly give you details.

Baroness Kidron: We would be really interested to see what that list looks like.

Katie O'Donovan: We have no problem in doing that.

Q110 **Lord Sheikh:** With regard to self-harm and suicide, I am quite encouraged by what both of you have said, particularly working in conjunction with the Samaritans, the police and the authorities. How is it monitored? For example, if somebody puts an item on Facebook or Google and is in a state of distress at that moment, quite often, that is the opportunity, when that person is down. How do you monitor that? How do you keep that under review to make sure that we render help at the right time?

Simon Milner: We do not monitor what people are doing on Facebook. However, when somebody shares, they are doing it for a reason. Typically, they are not sharing so that anybody on Facebook can see it; they are sharing so their friends can see it. I expect we are going to talk a bit later about the internet being always on, but that is one of the advantages. If you are in distress, usually one of your friends is awake and looking at their Facebook news feed at that time and will see it. That is what people are doing; they are reaching out to their friends. The key

thing we want to ensure is that when that happens, if their friend spots it, there is readily accessible help.

Lord Sheikh: Could the friend get in touch with you, for example?

Simon Milner: Yes; they can report it to Facebook. We can give them some language to communicate with their friend. We will say they might want to send a message to their friend saying such and such, which will include information about phoning the Samaritans. Therefore, we can help. Typically, these are young people; it is peer to peer. We want to ensure that, if a young person sees another friend in distress, there is material readily available for them to be able to help. We know that this works. In extreme cases, we also know that when they report it to us we will then absolutely look at that person's account. We have people who are expert in self-harm and suicide. If they are experienced, they can spot when somebody is joking. You do get people who joke about killing themselves because of the latest pop band splitting up.

Lord Sheikh: What about their football team?

Simon Milner: Or their football team losing. They are very good at being able to spot the signal from the noise. When they spot something that is really serious, it is not about getting that person to phone up the Samaritans; it is about getting the police involved. We have a network of relationships with law enforcement around the world, although not in every country. Certainly, we have very extensive ones with every single police force in the UK so that we can and do let them know. It is one of the few times when we will provide somebody's data to the police or third party without their permission, saying, "We know about this young person. It appears they are at home. It looks like they have taken lots of pills", and there are occasions when those people are rescued.

Lord Sheikh: It is a cry for help basically. They want to share it with somebody else.

Simon Milner: Yes.

Lord Gilbert of Panteg: That means that, when something is reported to you, a person has to sit down and review it. What is the triage system? How quickly in those most urgent cases can you deal with that issue, and how does it get to the top of the queue?

Simon Milner: It feels like that is a question for me, given we are hosting content. To give you a sense of the scale we are dealing with, we have about 1.8 billion people regularly using Facebook. Most of them use it every day. That is about 40 million people in the UK and, therefore, it includes lots of young people. That is a lot of people. We have billions of things happening on the site every day and millions of reports. We use technology to prioritise the most serious cases that may involve real-world harm, but we also ask good questions. We do not have just a big red button that says "Report". If we do that, how do we know what the issue is? If you are not on Facebook, I would encourage you to join. Try using the reporting function. You will see that, depending on the nature of the content, we will ask you certain questions. The one that people typically might press is, "I do not think this should be on Facebook".

Then we will ask you why you think it should not be on Facebook. That will enable us to get that report to the right person quickly.

We have also found over years of experience that often a problem is not about our policies; it is about relationships. It is about a young person, or indeed someone of our age, who does not like a photo of them. It is not against our policy to post a bad photo of someone. We can provide tools particularly to give young people a form of words to ask their friend in an empathetic way, "I do not like that photo of me. Can you please take it down?" That means we do not look at it; it is not against our policies, but we have provided a way for those people to solve their problem, and then those kinds of reports do not clog up our systems.

Lord Gilbert of Panteg: How many times last year did you report to the police a very serious incident where you thought somebody might be suicidal?

Simon Milner: I am afraid that I do not have that number to hand. I am happy to check with my colleagues who work in that part of our business to see whether it is something we are able to disclose to the Committee. It will be no more than a handful.

Q111 **Lord Sherbourne of Didsbury:** Mr Milner, you talked about your policies and processes in place to protect the safety of young people and children. You say in your evidence that you are not disposed towards regulation because you find that your policies and processes are highly effective in safeguarding young users. What is the evidence for knowing that it is effective?

Simon Milner: It is principally from the reaction we get from our users. When people report to us, typically, we will ask them, "How was your experience?" in the way that many companies and organisations do, but it is also through our partnerships. I know that recently Tony Close and a colleague from Google, whose name, I think, was Ms Fussell, gave evidence to you. They talked about the different platforms and their experience of them. I think they were very positive about Facebook. I know Tony Close. I have not talked to him recently about Facebook, but to me that is a good vindication that the things we are doing are working.

We look to studies like the big EU safety work that Sonia Livingstone has led in understanding young people and their approach to safety. We look for independent sources of evidence as to how well we are doing, but, to be clear, we do not rest on our laurels; we do not think we have sorted out all the problems and can sit back. Far from it. We continue to invest, grow our expertise and look at whether we have got things right. For example, in the past year a number of our partners have said they think our safety centre is out of date; it is not accessible and does not work on a mobile phone. That may sound strange given how many things work on a mobile. Our safety team worked hard to revamp it, relaunch it and make it accessible, and change some of the language there and some of the advice to recognise changing technologies and the changing use of our service. We are always looking for ways to improve it, based on the feedback we get from both the people on Facebook but also the experts we work with outside.

Lord Sherbourne of Didsbury: If you do not get feedback where children have been badly affected by content, how do you know whether they have seen it?

Simon Milner: I do not quite understand the question.

Lord Sherbourne of Didsbury: Clearly, you are not complacent because certain things are not going right in particular cases. How do you know they are not going right? What evidence do you have for it? How would it be reported to you?

Simon Milner: Principally, it would be reported through our safety partners. We do not just ask our safety partners how we are doing; we also give them direct access to experts in our community operations team to let us know when they think we have made the wrong decision.

Lord Sherbourne of Didsbury: Are you talking about policies or outcomes?

Simon Milner: Actual outcomes.

Lord Sherbourne of Didsbury: Under your system, when children see content they should not be seeing, that is not always notified to you, is it?

Simon Milner: Let me give you a related example where something may be going on in a particular school. Often, waves of bad behaviour happen around an individual school community. It is something we have not seen before. People are reporting it, but we do not quite understand what the problem is because we do not understand the local context. That is when somebody like ChildNet or the NSPCC reach out to us and say, "This school has contacted us. A problem is happening in the school, but it is also on Facebook", and they are not getting the right kind of outcomes they would expect from their reports. That can lead us to learn from that and realise—a ha!—that this is a new phenomenon we have not seen before. We now understand why we have been getting a number of reports like that. You are right that, if people do not report to us, we are not going to be able to take action. Therefore, it does need that young person or their friend to report it. You are right. Sometimes, we make a mistake; we have not reached the right judgment, and that is where the direct access that the safety partners have to our community operations team can help rectify the problem.

Q112 **Lord Sherbourne of Didsbury:** Can I pursue with Katie O'Donovan the Digital Economy Bill that is coming to our House very shortly? We had evidence last week from the BBFC. They told us that what is not in the Bill but might be is a clear legal requirement, which ISPs would like, for those providers to withdraw their services when publishers have not agreed to withdraw material. What is your view on that?

Katie O'Donovan: Obviously, the Bill is still in the House of Commons at the moment and has come under a lot of scrutiny. There has been a Committee in the Commons on it, and over the week the Government said they were now minded to request that ISPs block content. The Bill is a very good example of a straightforward ambition to address the issue of the availability of pornography, which has changed significantly since the advent of the internet. That is a sentiment we absolutely understand.

One of our concerns is that the BBFC, the regulator, is very competent in understanding what pornographic material is and identifying that. You then have sites that are hosting pornographic material, which may be perfectly legal but are not meeting the requirement of age verification. The difficulty is that you have a regulator encouraging what are described in the Bill as ancillary service providers, perhaps payment providers or advertisers, to withdraw their services, but they are not legally compelled to do so. One of the things the Government have sought to do by including ISPs is to give a very clear legal direction to ISPs that it is for them to block access to that content.

Google is not involved in the value chain of pornography. We do not host pornography on our main platforms; we do not allow pornographers to advertise with Google products; and we do not host advertisements on pornographic websites. Therefore, it is not something in which we are directly involved in terms of the value chain, but it is a very good example of ensuring that, where there is legislation and regulation around the digital industries, it seeks to have a very clear purpose that is defined and discussed by the country, essentially. In this case, it is a parliamentary process. It is absolutely right that Parliament can ask ISPs to block content, but it is very helpful to have a clear distinction and direction of what content is legal and illegal, because it is very difficult for us in some instances as a content host or search engine to decide where a line should be drawn on content that remains legal.

Lord Sherbourne of Didsbury: But the BBFC could do that, could it not?

Katie O'Donovan: I think the Government are seeking to table an amendment, as they indicated at the weekend. At the moment, the BBFC can request ancillary services—those who support the functioning of the pornographic websites—to withdraw their services.

Lord Sherbourne of Didsbury: They can define what is legal, illegal, acceptable or unacceptable. They are well placed to do that, are they not?

Katie O'Donovan: They are very well placed to identify what is pornographic material, and that is very helpful. What is more difficult—I hope that the Government will bring clarity with their amendment—is whether content is illegal or legal. If it is adult pornographic material, which might not be suitable for a general audience but is still legal, it is very difficult to ask ancillary services voluntarily to do something. That is what the Government have sought to do where they have directed ISPs more firmly.

Q113 **Lord Sheikh:** Regarding the removal of content from Google and Facebook, it has been said that not all platforms are quick to take down offensive content. We have heard from children who have said that, in particular, Facebook does not respond adequately or quickly with regard to any complaints these people have made. How do you monitor and moderate content that may be unsuitable for children? That is my first question. My second question follows on from what I said a minute ago. How do you respond to complaints from children asking for content about themselves to be deleted? If you are going to do this effectively—

in other words, to look at complaints concerning content—do you have enough resources? What are the benefits? What are the minuses regarding this approach in regard to responses?

Simon Milner: There are quite a number of elements to your question. I want to make it clear that we do not moderate content. That is principally for privacy reasons, but if you think about the scale of Facebook and the fact that most of what happens on Facebook is perfectly benign and in general is very positive, it would be completely inappropriate for us to be monitoring and moderating that.

Lord Sheikh: It may be benign to you but not to the person who has been offended.

Simon Milner: We do have very clear policies about what is and is not allowed on Facebook. One of them, which you raise, is that you cannot post an image of someone else without their permission. To that end, given that most people will not necessarily ask for permission, if somebody comes to us and says, "There is a photo of me that I do not want to be on Facebook", we will take that off. As long as we are hearing directly from the person in the photo we will do that.

Lord Sheikh: Do you have adequate resources to do that?

Simon Milner: We certainly have an adequate process for doing it. For example, I complained this morning that my internet was completely cut off. I am hoping that by the time I get home it will be restored. If it is not, of course I will be upset about that. As with any organisation, you have to prioritise. We prioritise on the basis of real-world harm. We absolutely prioritise reports that come in from younger people on Facebook, but if it is an image they want to have removed that is not going to be as high a priority as, say, somebody reporting a suicide risk, or that they are concerned for their safety in some way. Therefore, there is a prioritisation based on that, but we try to get to these reports as quickly as possible. Every piece of content reported to us is looked at by a human being, and that takes some time. You have to ensure that the right expert who understands the language, our policies and so on is looking at that, but I want to be clear that not only young people but the parents of somebody under 13 can report an image and we will take it off Facebook.

We endeavour to try to get to things quickly and to be accurate in our decisions, but we are dealing with millions of reports every day. It is hard to satisfy everyone all of the time, but I do encourage you to try it. Try it and see what you feel about the response time, but also what you think about the message we give you. When you report something to Facebook, we let you know we have got your report. In some more complicated things we might tell you how long we think it will take, and then we will let you know our decision and why. We try to keep people, as per best practice across all service sectors, at least informed about how we are getting on with their report. I am not sure whether that adequately answers your question, but I hope I have addressed some of the points.

Lord Sheikh: Yes. I have one supplementary after Katie answers what I have put.

Katie O'Donovan: In a similar way to Facebook, if on YouTube there is a video that shows a child or somebody of any age and you do not want that video to be on there, you can request that it be taken down. You flag it and say, "This is my image and I am not happy with it. I do not give consent for it to be on YouTube". We will remove it after we have reviewed it.

We also use the right to be forgotten for search listings. That was a ruling by the European Court of Justice in 2014 when it asked Google to de-list and not return results for particular search queries of particular individuals who felt that the search queries being returned were outdated. If we agreed that they were not in the public interest, we removed them. Young people can use that as well. If those links to stories are no longer relevant and it is not in the public interest, we can remove those lists. Similarly, if there are websites that contain personally identifiable information, whether it is name and address or bank details, you can request that those results are not returned in search, which we will not do, and we do not do it for extortion sites either.

Lord Sheikh: If something is put on Facebook or Google that has a possible criminal element, because there are instances where these things do happen, are you proactive on that issue, or if something slanderous or libellous is said will you be involved in issues like that?

Simon Milner: With defamation-type issues, you absolutely have to rely on the individual who feels they are being defamed to get in touch with us. We have a special process for that, and we will act in accordance with legal advice in respect of any referral like that. There is one particular category of criminal content that we endeavour to ensure never reaches Facebook: child exploitation images. Those images tend to be illegal everywhere. Facebook, like most parts of the internet industry, uses technology to prevent known child sexual exploitation content to be shared via its servers. We are under an obligation as a US company to report instances of that to authorities in the US. We will not only close someone's account; we will also report their details to the US authorities, which then share it with law enforcement elsewhere in the world to catch the perpetrators.

Q114 **Baroness McIntosh of Hudnall:** This is probably a question for Google entirely. When the European regulations that led to the right to be forgotten came in, what position did Google take corporately in advance of those regulations? Did you get behind them and push them along, or did you try to stop them?

Katie O'Donovan: We were very concerned when those regulations were first raised. The principal reason for our concern was that it gave us a responsibility that might be better served in a democratic or open process. The way that the legislation works is that, for example, if there is a news story about me and a petty offence I may have committed 10 years ago, I can make a request to Google for that search result not to be returned against my name. It is for our legal process and teams to decide whether that is in the public interest. That is quite a heavy

responsibility for a private company to have, and it is one that we take very seriously. We were concerned about the precedent that set.

Since the legislation has come into place, we have been applying it as a European-wide piece of legislation, and we adhere to it. I think that in the UK there were about 100,000 requests last year. We granted 40% of those; in 60% of cases we said there was a public interest. This was primarily for adults rather than young people.

The systems we have in place are working well. We have a good system of legal review, and we have an annual report that makes clear all of the information we review in these circumstances, but it was definitely a concern to us when it was raised and, while it is working well at the moment, we keep it under ongoing review.

Baroness McIntosh of Hudnall: In relation to other requirements that might be placed on ISPs or other providers, do you still feel, in the light of your experience, that you would rather not have that kind of responsibility? Where would you look for those responsibilities to be taken up?

Katie O'Donovan: It has worked at a practical level, and we have additional policies. For example, we have a self-regulation policy on revenge porn. If you have been subjected to a former partner, or somebody else, sharing images of you on the internet and the internet host will not remove them, we de-list those and remove them from our search results. It is important that those conversations are had. They are real issues of great concern to people, particularly the more vulnerable in society. We now have a generation of people who have grown up online, which gives you a different set of challenges. It is absolutely right that policymakers across Europe and in the UK seek to find the best solutions to those issues. At the moment, the process is working, and we will continue to be part of that process, but we will also look for our own self-regulatory resolution as well—for example, policies on revenge porn.

Q115 **Baroness Bonham-Carter of Yarnbury:** My question for Kate is quite a niche one and is about journalism. I am interested in and have been concerned about content embedded in news items apparently from trusted outlets but somehow a bit of video has got in that is seriously unpleasant. What is your approach to managing that content? You might be a child who has Googled Iraq or something. It is a perfectly legitimate bit of wording and then there is something very nasty in the middle.

Katie O'Donovan: Is that on YouTube or on a third-party website?

Baroness Bonham-Carter of Yarnbury: It would be a Google search.

Katie O'Donovan: You are looking for a news story on Iraq and it is taking you to something else.

Baroness Bonham-Carter of Yarnbury: It is in the middle of the content, and I would be surprised if it had anything to do with whoever has posted it. Is that possible?

Katie O'Donovan: You can have scenarios where you are looking up Iraq, Syria or ISIS and you are looking for news-based results. You might go to a mainstream news organisation. You might go to slightly

different editorially guided news organisations. Sometimes, within that footage, you can see content that can be absolutely distressing. It can have valid news value but would none the less not be suitable for a general audience. If you have opted for Google SafeSearch, which you can do from the home page very easily, those are de-prioritised in your search results, so it would be much more unlikely that you would have those results, but the content on third-party websites, whether it is a mainstream news organisation or a kind of citizen journalist website, is not something we have the ability to control. It is not within our gift to set the parameters of what that content should be. YouTube is our own platform and, therefore, we have strict terms and conditions about the content that is allowed. Graphic violence is not allowed on that. The exception is that, if there is news value to it and it is within context, we may allow that to remain, but often we will age-gate that content, so you have to be signed in and be over 18 to access it.

Baroness Bonham-Carter of Yarnbury: I see. You are using a kind of editorial function.

Katie O'Donovan: We do not editorialise search results. We give users what they are looking for. If you were to Google something like Iraq, it is more likely that you would get geographical information, information about population and that kind of thing. We will give the most relevant information to your search query, and that will be from a variety of websites.

Baroness Bonham-Carter of Yarnbury: Admittedly, I was not using safe mode, but I went straight to this page. It concerned me that young people, who might be given a project or whatever, could access it.

Katie O'Donovan: That goes back to the fundamentals that we are discussing here. Online, you have fantastic opportunities to read, experience and learn about different cultures and historical events, but there is also content that is absolutely not suitable for a general audience, so SafeSearch would be our technological response to that. We also feel that there has to be an educational and support response, so that when young people are using the internet they do it safely and understand that some things will not be what they expect to see. Some things will be unpleasant to see. They have to think about how they are searching and where they are looking for information and using trusted sources as well.

Baroness Bonham-Carter of Yarnbury: I obviously need that lesson too.

Katie O'Donovan: I think we all do at certain times.

Baroness Kidron: Do you operate the right to be forgotten in non-EU countries?

Katie O'Donovan: No.

Baroness Kidron: Therefore, there is a possible role for regulation. We had a brief conversation earlier about fake news on Facebook. What has come up a lot in our inquiry is the whole question of critical literacy, especially with regard to young people. We would love Simon to say something about that particular incident.

Simon Milner: What would you like me to say, Baroness Kidron? Do you want to ask me a question about it, or shall I just give you a general response?

Q116 **Baroness Kidron:** I think the question is: are you comfortable as an organisation with what has just happened with the fake news and the potential outcome of, and effect upon, the American election? Do you think it has further implications for other sorts of information that young people might be seeing and not judging clearly? Is that a sufficient question?

Simon Milner: That is perfect. Thank you very much. Our chief executive, Mark Zuckerberg, has spoken quite extensively about this issue since the events of 8 November, including at the weekend when he put a lengthy post on his Facebook page. I am happy to provide a link to the Committee for that so you can see the detail. I think there are three main points here. One is that our analysis shows that much less than 1% of the content on Facebook may be inauthentic, a hoax, fake or whatever words you use. We see no evidence to suggest that the sharing of fake news in relation to the US election made a significant difference to the outcome of it. Many other commentators have come out and said that as well since 9 November.

However, it is not a good user experience, particularly if people are sharing stories that are untrue. Therefore, we want to try to find ways to diminish the extent of that content on Facebook and reduce its prominence on people's news feed, but we also do not want to be the arbiters of truth. There are many more experienced people in this room than me, but certainly during the years I worked at the BBC I rarely read a story about the BBC that I thought was wholly accurate when I knew the issue very well. That is not to do with the quality of journalism; it is just the nature of one's understanding of an issue. You very rarely read something that is 100% accurate. Where do you draw the line if you are an organisation that is trying to depress the extent of that content, albeit it is already less than 1%, without making editorial judgments that people would think stray over the line, particularly for a platform that is used by 1.8 billion people globally?

It is an issue where we are determined to try to improve user experience, but also one where we are very mindful of the need to work very closely with publishers and those much more experienced than people in Facebook on these issues, and to learn from others about how best to tackle this. It is not an issue just about Facebook; it is a wider issue, and something where there needs to be a concerted and well-informed public dialogue about those matters.

Baroness Kidron: Does the 1% relate to the amount of news carried by Facebook or 1% of all the things posted on Facebook?

Simon Milner: That is a broad-brush number. It is less than 1%, which is anything from .99% to 0.001%. It is somewhere in that range, but we are not quite sure where—indeed, how would you measure it?—but it is about all content on Facebook.

Baroness McIntosh of Hudnall: Your point about things not being 100% accurate as reported is a perfectly legitimate one. We used to be

told we should not believe everything we read in the newspapers. A lot of us were brought up in that way. Does it seem to you that part of your responsibility as providers as opportunities for these stories, whether they are wholly true, wholly untrue or partly true, is possibly to say to people, "You should not believe everything you read on Facebook"?

Simon Milner: I think this is one way where our community can be very powerful. Just because somebody has shared a story suggesting that the Pope was endorsing Donald Trump does not mean they were saying it was true. Quite often, people would share things and say, "Look at this utter nonsense".

Baroness McIntosh of Hudnall: That is a very sophisticated nuance, if you will forgive my saying so, particularly for younger people.

Simon Milner: I am not sure I completely agree. There is a lot of evidence that young people are very good at identifying when something is wildly inaccurate. I agree with you when it comes to things that are plausible. It is plausible that Nigel Farage might be the next UK ambassador to the US. Who knows? When you have things that are not true but plausible, it is incredibly hard for anyone to judge. I agree there are some interesting questions about how you provide alternative perspectives, including fact checking. Katie may want to talk about the role of fact checking when it comes to news on Google, and we may need to learn from that.

Baroness McIntosh of Hudnall: I am sorry to press this, but I am asking you about something else. It is not about Facebook mediating whether things are or are not true; it is simply pointing out to people, as part of the normal way that you present what you do, that not everything that pops up and appears to have the authority of a particular brand, or even a particular design behind it, is necessarily information that should be trusted. It should at least be open to question. That is where the issue about critical thinking is surely most at risk, is it not?

Simon Milner: I absolutely understand what you are saying. One of the things that we do, for instance, is ensure that we verify certain pages on Facebook. If something purports to be from the BBC and it has a blue tick, it is from the BBC; it is not from somebody else pretending to be the BBC. That is one of the ways in which you can help people understand it. Generally, we look for brands that we trust. The verification tick that we, Twitter and other services use can be very helpful in guiding people about authoritative sources of information.

Katie O'Donovan: I think the critical thinking point is clear. In the past year we started a programme called Internet Legends, which goes into schools and works with eight to 11 year-olds. We were very pleased to have some Members of the Committee visit a school in Brixton last week. It is a general programme for eight to 11 year-olds, so those just beginning their online journeys. It sets out some very basic tenets and principles that we think it is good to encourage when people are online. One of the four is to check something is for real and ask whether, if you see something online, it is too good to be true. Is the source trusted? Think about it critically. That is a small way in which we are involved in starting that conversation. I know that there are many others active in

the States. It is important for all of us—this goes for adults as well—that, if you can easily be duped by things online, you apply critical thinking, and we do have a role as a platform to support that.

Q117 **Bishop of Chelmsford:** Before I ask my question, I dive briefly into this debate. It is very important for the way young people, in particular, access the internet. Katie, a little while back in the conversation I thought I heard you say that Google does not edit material; it is just the pure noble provider of all of it. Am I not right in saying—correct me if I have got it wrong—that, when I put something into Google, the material it presents to me is not necessarily the same for somebody sitting next to me who puts the same thing into Google? What Google delivers to me is shaped very much by all the previous things I have been putting in as Google builds up its profile about the sorts of things I am interested in. First, is that true? Secondly, I do not think young people are sufficiently aware of that. That is editorial control. It is not the sort of editorial control newspapers provide, but it is editorial control, and we should be more open about that. I am not suggesting it is necessarily very sinister, but it is a fact, is it not?

Katie O'Donovan: That is a good and important question, and the answer to that probably has two very meaty sections. If you and your neighbour are not logged into Google accounts and using Google Search, you would get the same results. Those results would be based on a number of different indicators that our algorithms use to understand what would be the most relevant search. If you are looking for a news story, some of that would be indicators of the quality of the news site that we return. We use indicators like how many people link to this site. Is it linked to by other reputable sites? If you are a website that links you by the BBC, for example, that is understood by our algorithms to be probably quite a legitimate site.

Therefore, we have ways that are not editorial in the classic way newspapers behave in maintaining quality in the results we return, because that is absolutely what our consumers are using.

We do have ways of making sure that the search results that you look for are particularly relevant to you if you are signed into your Google account while you are doing the search. We do that because it is helpful, by and large, for consumers, but you are absolutely right that the trust and transparency that goes with that is key. For example, if you wanted to buy some wellington boots and searched for that, and you were signed into your Google account and that account was happy to have location features switched on, we might offer you wellington boot shops in London. If you wanted a take-away pizza, it might be in your local neighbourhood, but transparency is absolutely key in this.

We have a website called My Account and privacy settings within that, which we encourage people to review. You can personalise all the information we collect on you and how we use that information. Data enables us to give good personalised responses, which is usually what consumers want, but, if you would like advertisements that are not personal to you and not based in any way on your search history, you can turn that off. If you want to mute particular adverts, you can turn

that off. It may be you were very interested in buying a car and have now bought one, so you want to mute adverts about buying a car. You can do that. It may be that you do not want us to keep a record of your search history at all because you do not want us to learn from that and improve and nuance your results. It is always confidential, but you do not want us to log that. Therefore, we have the ability to give personalised responses and usually that is helpful to the consumer, but we absolutely give the opportunity for consumers to turn off those elements.

Bishop of Chelmsford: I would love to pursue this further, but I do not suppose Lord Best thinks we have time for that. I just note that now we have become consumers, whereas the discussion was about how it affects other content that is not about being a consumer, but I will leave that one hanging.

Katie O'Donovan: "User" would have worked just as well.

Bishop of Chelmsford: Yes, but it is an interesting shift. What do you think is an appropriate age threshold for someone to use a social media platform?

Simon Milner: Shall I take this, given Facebook is a social media platform? We have a policy that for legal and operational reasons you have to be 13 to be on Facebook. That applies globally, with the exception of a couple of countries where it is 14 because of local law.

Bishop of Chelmsford: What do you do about eight year-olds on Facebook?

Simon Milner: There is nobody who will have their age set at eight on Facebook because they would not be allowed to have an account. I understand what you are saying.

Bishop of Chelmsford: We know that there is a barrier.

Simon Milner: The research done by Professor Livingstone and colleagues suggests there are not many eight year-olds on Facebook, but there may be quite a lot of 10 to 12 year-olds who are lying about their age to be on Facebook, which is of concern to us.

Bishop of Chelmsford: The Ofcom research suggests that there are quite a number of eight year-olds.

Simon Milner: The main things we do is ask people their age when they join Facebook. If somebody puts in their real age and finds they cannot open an account, we put a little cookie on their machine that means they cannot go back in and try again with a different age. That is one piece of technology that does it. We make this very clear in all the training in our safety centre and take every opportunity we can, including in front of this Committee, to remind people that you have to be 13 to be on Facebook, and indeed to use many online services. However, we have a fundamental issue in the UK—I know this was also evidence Tony Close and his colleague Lindsey Fussell presented to the Committee—whereby many parents choose, for whatever reason, to allow their children to go on Facebook. Often, they have helped their children get on to Facebook.

When that happens, it is very hard for us to be able to know that that person is not the age they say they are.

However, we have special reporting processes. Whenever a teacher in a primary school says to me, "I have a real problem. All the 11 year-olds in my class are on Facebook", I say, "You can report all of them to us". Particularly when it is coming from a teacher I say, "Tell us about the accounts and we will act on all of them, because we know you are a trustworthy source". They do not often do that because they think they might incur the wrath of the parents. It is a fundamental problem to which we have not found a ready-made solution. When millions of parents are making that decision, how can we enforce our policy? I do not like it; I do not condone it, but as a parent, all of whose children are now teenagers, I can understand why people might have made that decision. It makes it much harder.

Bishop of Chelmsford: Made what decision?

Simon Milner: The decision to help their child lie about their age.

Bishop of Chelmsford: We will not ask you whether you did with yours.

Simon Milner: I am very happy to say I never did.

Bishop of Chelmsford: Surprise, surprise: children lie about their age. I certainly did when I was younger. Whose responsibility is it to do something about this in your view? It sounds like there is a gap between your policy and what is happening. Should there be some regulation?

Simon Milner: There is regulation in the US and regulation is coming in Europe with general data protection regulation, which will be implemented by April 2018. Obviously, that will apply in the UK until we exit the European Union. Indeed, it may apply after that depending on the decisions the Government and Parliament take. It is not clear to me that that will fundamentally change the behaviour of parents, but it might. It creates another moment for the industry, together with government, safety organisations and so on, to remind people that these are the rules and why they are there. As per the guidance we have provided in our safety centre, that moment when your child becomes 13 is a great learning moment to say, "You can now come into a world that gives you incredible opportunities but also responsibilities".

Bishop of Chelmsford: To turn the question on its head, why 13? I know that is not your decision, but, out of interest, why is that? You seem to be very committed to it.

Simon Milner: It is the law in the US. The Children's Online Privacy Protection Rule has been there for quite a long time. I do not know the history of it and why the US authorities fixed upon 13 as the age. I expect Professor Livingstone knows better than I why they went for that particular age, but I am happy to look into it and provide anything further that I can.

Baroness Kidron: Simon, has Facebook put any money, thought or creativity into some sort of public service campaign—I cannot think of a good way of saying it—to parents saying, "Do not do this"? Is that something you could or might consider?

Simon Milner: We certainly have supported safety organisations who make it an important part of their work to ensure parents know this rule.

Baroness Kidron: But not within the Facebook ecosystem itself.

Simon Milner: If you think about it, once people have made that decision they are allowing their children to be there. It is not obvious that it is going to make much difference. We feel it is a situation when perhaps parents are all together getting that talk on internet safety. For those of you who have had children, nine, 10 or 11 is often the time when schools are doing quite regular internet safety training with the likes of ChildNet, NSPCC and so on. When all parents are in the room together, that is a great moment; that is a good learning opportunity. We provide both financial and other support to those organisations when they are making those kinds of interventions.

Lord Sheikh: May I put a very brief supplementary?

The Chairman: Lord Sheikh, we have finished our hour of conversation and are just coming up to the halfway mark, so I am not going to have any more supplementary questions, sadly. We have to move at a bit of a pace. Could colleagues ask their questions briefly, and could our two witnesses, very kindly, give pretty clipped, tight responses?

Q118 **Baroness McIntosh of Hudnall:** These are questions about privacy settings and your attitude to how rigorous you should be about this. The UKCISS guide states that the company should offer privacy setting options, including privacy by default, to give control to its users. Do you comply with this? Do you offer default-on privacy settings and, if not, why not? I have already asked you about the right to be forgotten. This is a matter more for Google than Facebook, but, in the event that those regulations do not apply because we are no longer part of the European Union, would you cease to apply them?

Katie O'Donovan: I can start with that question and work backwards. We have not made a decision about that yet.

Baroness McIntosh of Hudnall: Therefore, it is not necessarily "yes".

Katie O'Donovan: It is an honest answer: we have not considered that and, like everybody else, we are looking to see what happens as the UK prepares to leave the European Union. Obviously, the Government have said they will transpose GDPR and lots of other legislation. From what we have gathered so far, it looks like the right to be forgotten would still apply, and we would happily concur with that. If the UK Parliament decides something else, we will engage with and work with it to ensure that the alternative is helpful and productive and does what Parliament wants it to do.

As to our privacy settings—I mentioned some of this in my previous answer—we believe they work for our users to enable them to have a personalised and effective use of our services. That means some of them are on by default, and we give people access, and the opportunity, to change those very easily. We make sure that our terms and conditions are easily understandable. We work as a cross-functional team to make sure they are not legalese jargon and not too long. We were very

pleased to win an award from *Time* magazine for clear terms and conditions.

We also make sure that we respect people's data related to different age groups. We have different priorities for people aged 13 to 18 who use our services and a different approach to advertisement in the way their data is held. We make sure that all data, whatever the age of the user, is never sold or passed to third parties; it always stays within Google.

Simon Milner: We comply with the UKCISS guidelines. As I mentioned earlier, whenever anyone joins Facebook their privacy settings are set to the tightest level, which is friends only. That will not change unless and until they change them, and that is true for all age groups.

Q119 **Lord Gilbert of Panteg:** Can we move on to the issue of privacy of data that you collect from your users, particularly children? This came to public attention when Facebook and WhatsApp were proposing to share data, but it is a wider issue. Can children, or any user, decline permission for you to share data with third parties and still use your services?

Simon Milner: Yes. We do not share people's data with third parties without their permission. That is true of everyone, however old they are, with the one exception of law enforcement requests. When we get such requests we can and do share data. We make public the number of times we do this. We report this every six months. That is the one time when we will share people's data without their permission, if there is proper legal process and evidence of a crime and so on.

Lord Gilbert of Panteg: Do third parties include other companies within your group?

Simon Milner: No. They are part of the Facebook group. Depending on the actual data policies of those companies, we can and do share data between the companies within the group.

Lord Gilbert of Panteg: Could a child, or somebody else, decline permission for you to do that and still use your services?

Simon Milner: It depends on which particular services we are talking about in terms of those within the group. Rather than go into it now, I am happy to write to the Committee afterwards to explain the details of that.

Lord Gilbert of Panteg: Is it the same for Google?

Katie O'Donovan: We do not share the data of anyone of any age with third parties. We do not share personal identifiable information with third parties. You can choose to decline to share any of your data or usage with Google and still use all our services in exactly the same way as if you were fully sharing it.

Lord Gilbert of Panteg: Do you think children understand the extent to which you analyse data about them in creating your profile of the user?

Katie O'Donovan: We are very keen to ensure that more and more people do understand the way that we use data to make sure our services deliver effectively for them. We launched Privacy Checkup on My

Account. We regularly advertise that to our users and encourage them to have a look at their activity. I think we have had about 1 billion visits since we launched it. Every year, on Safer Internet Day, we have home page promotions on Google to direct people to that section of the website. We have offered free data to people to have those check-ups. It is a very easy to understand and intuitive guide to what you want to share with Google and how, and that is available to anyone who is 13-plus and has a Google account.

Lord Gilbert of Panteg: Do you think children understand how Facebook uses their data?

Simon Milner: We are endeavouring to help them to do that. I rather look to third parties to give you hard-and-fast data on it, but we try to make our data policy more accessible to everyone. Last year, we relaunched it. It is about a third of its previous length. We changed some of the language to make it more accessible and had clearer sections in it. We do not have a separate version for children. However, we do work with organisations like ChildNet, a long-term partner of ours. They have produced their own guidance on how services like Facebook and how advertising work on Facebook and so on. That is probably the best way to try to help young people understand how services like ours work.

Q120 **Baroness Kidron:** One of the things we have been trying to look at is the idea of well-being rather than safety and expanding this conversation, because safety is not enough. Simon, I think you have already referred to it. One thing we have taken a lot of evidence on is that the always-on culture is a problem for kids, particularly at the developmental stage when they are not entirely in control of their own feelings. Maybe you could give us a response to some of the evidence you must have seen about screen time and the compulsion to respond and share.

Simon Milner: It is certainly something we are aware of. We talk about it a lot with our safety partners. One thing we are very clear about is that what is right for each family can be quite different in terms of screen time. What is right for each member of the family when growing up can be quite different. What worked for my 19 year-old daughter when she was 14 does not work for my currently 14 year-old boy.

However, we also say it is important for parents to set a good example. If they say there should be no phones at the dinner table that includes parents. That is part of the guidance. Often, young people will copy what they see from their parents in terms of use of technology, so setting a good example can be very important, but try not to preach. Who are we to tell parents how to bring up their children?

We would also say that when it comes to well-being—I am very pleased to hear this is an important part of what the Committee is looking at—we know from experts that social media can become incredibly important to people when they are under stress. When they are mentally challenged, it helps to bring people together who are suffering from the same condition, if you like. Not all young people have happy home lives. Unfortunately, we hear all the time about young people who are in the most stressful situations at home, not when at school. Therefore, having

the ability to access secret groups on Facebook, where their parents do not see what they are doing, can be very important for those young people. Like all these things, it is not linear and it is not a one-size-fits-all approach. It is about ensuring that we try to provide the best general advice we can to the great majority of young people and parents who live the same chaotic lives most of the rest of us do but generally are getting on with it and finding a way through. We also work with specialist experts, whether it is CEOP, the NSCPP, Lucy Faithfull Foundation and others, who deal with the most vulnerable children and those under most distress, for whom social media can be a lifeline. Getting that balance right can be incredibly hard, but we try.

Baroness Kidron: I acknowledge that what you have just said is absolutely true. It provides a huge resource for young people, but most platforms, however, are designed to extend use. One thing that has come up again and again is young people's feeling of being overwhelmed by alerts and notifications. Should some of these things be off by default? Should some of them give them a break? Are you comfortable with the design of your services with regard to the developmental stage of the people who are using them?

Simon Milner: I can tell that Katie wants to come in. I am happy to come in if there is time.

Katie O'Donovan: I am also conscious of time. We would echo a lot of the points Simon made. The LSE and Sonia did some very interesting research recently on the differentiation of different types of screen time and how we cannot lump it all together as bad, which is the point you are making.

Your point about technology and whether we can build some of that into products is something we are very interested in as well. When we launched YouTube for Kids, we developed a time limit so parents can choose how long they would like their children to use that for. As users of technology get more and more sophisticated, obviously they have the ability to override those as well, but the elements we can build in by design are really important. That is something we think carefully about as a company.

Q121 **Earl of Caithness:** Notwithstanding everything you have said, the problem for young children is getting worse because of offline and online access. There is a real problem here. You can help to control that by the design of your platforms, so could both of you give an example of what you can do to your platforms to make it safer for children?

Simon Milner: That is a very general question. What have we learned to do? We have learned to put help where it is most needed. We have a very extensive help centre and very much encourage people to go there with their problems, but the key thing we have learned is that nothing is as good as inline help. When you are experiencing Facebook on your mobile device or computer and see something that distresses you, there is help right there when you need it, or, when we start to see behaviour like public sharing, which is an unusual pattern for you, we intervene at that time to say, "Are you sure you want to be posting publicly?" I think that the more we can provide inline, real-time help, that is very

effective, in the same way that, when you talk to teachers and parents, it is all about, "I really wish I had been there at that moment, because that was the teaching moment". We are always looking for teaching moments as part of young people's experience on our platform.

Katie O'Donovan: The answer I would give is that most specifically for younger people it is, first, SafeSearch and restricted mode, which is restricted search on YouTube as well. That enables people to experience the full possibilities and opportunities of the internet but in a more restricted and safer way. Secondly, with YouTube for Kids, we took the decision to invest a lot of time and engineering effort—it was much more complicated than we thought it would be when we set out—into building a product specifically for younger people that does not collect their data or personal information and does not allow them to communicate. It has a very in-depth onboard inflow for parents that enables them to learn about how to report and flag content on YouTube, which is really important.

Earl of Caithness: Let me turn it around to you, Katie, and then Simon. Why do you not have on Google an automatic stop after you have done a YouTube search instead of continual running of the next YouTube video that you do not want? Think about that one. Simon, why do you not have a device, or alarm system, which says, "You have been on Facebook for an hour. Is this good for your health?" Those are two things you could do easily. Why do you not do them?

Katie O'Donovan: On YouTube, we are trying to serve content that is relevant to the viewer. If they have watched a video and we offer one that is similar and they do not want to watch it, they can very easily click pause or come out of the app and stop watching.

Simon Milner: It is extremely unusual for anybody to spend that length of time on Facebook. The average amount of time over a whole day might be an hour, and that will always be in fits and starts. It is an interesting idea. I will happily pass it back to our safety team to see what they think.

Earl of Caithness: Cut it down to half an hour.

The Chairman: There are two good ideas. The fact we have overrun by miles is a tribute to how much we have learned from you. Thank you very much indeed for all of that. I am afraid we did not get round to asking you about advertising on which we would be very interested to hear you. I am afraid we must do that by correspondence. Email would be just right here. Thank you both very much indeed for joining us.

Family Online Safety Institute – written evidence (CHI0033)

1. The Family Online Safety Institute (FOSI)[176] is an international, non-profit, membership organisation[177] working to make the online world a safer place for children and their families. We achieve this by identifying and promoting the best practices, tools and methods in the field of online safety. FOSI convenes leaders in industry, government and the non-profit sectors to collaborate and innovate new solutions and policies in the field of online safety. Through research, resources, events and special projects, FOSI promotes a culture of responsibility online and encourages a sense of digital citizenship for all. With roundtables, forums and conferences around the globe, FOSI plays an important role in driving the international debate.

2. FOSI is a registered charity in the United Kingdom, [178] and is headquartered in Washington, DC, but works globally. In order to achieve our aim of ensuring that children access the best of the Internet in the safest way possible, we focus our efforts in three key areas. We promote enlightened public policy, based on research and preventing actual harms. We advocate for industry best practice, believing that technology companies are often best placed to respond quickly and effectively to online safety challenges, and finally we advise parents on how to be good digital parents, raising their children to be informed and confident digital citizens.

3. In the United Kingdom, FOSI has been an active member of the UK Council on Child Internet Safety (UKCCIS)[179] for many years, and also continues to work closely with the European Commission on their online safety efforts.[180] While in the United States, Canada, and Australia, FOSI regularly engages at the federal and state level to provide resources and raise awareness about online safety efforts. Enlightened public policy requires a foundation of understanding on how children are using the Internet and the risks that they are facing, and thus FOSI conducts regular quantitative and qualitative research studies into parents' and children's online use.

4. FOSI's 2015 research on "Parents, Privacy and Technology Use,"[181] found that that majority of parents have rules about their child's technology use, and 75% of parents have specific rules about what their children can or cannot post publically online.[182] Furthermore, parents who often use technology with their child are more confident that they can manage their

176 Family Online Safety Institute. *Online at* https://www.fosi.org

177 FOSI members include: Amazon, AOL, AT&T, AVG, Comcast, Crisp Thinking, CTIA, Disney, ESA, Facebook, Google, GSMA, Kaspersky Labs, LinkedIn, Microsoft, MPAA, NCTA, Netflix, Nominum, Photobox, RSA, Skout, Symantec, Telstra, Telecom Italia, T-Mobile, Twitter, Verizon, Yahoo!

178 UK Registered Charity no. 1095258

179 *Online at* https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis

180 *Online at* https://ec.europa.eu/digital-single-market/en/news/commission-broker-new-alliance-better-protect-minors-online

181 Family Online Safety Institute. November 2015. *Parents, Privacy & Technology Use*. *Online at* https://www.fosi.org/policy-research/parents-privacy-technology-use/

182 Family Online Safety Institute. November 2015. *Parents, Privacy & Technology Use*. p. 19.

child's technology use.[183] FOSI strongly suggests that parents and children go online together from an early age to help develop ongoing conversations about appropriate use of technology.

5. Parents also need to be educated about keeping their children safe online and how to be good online role models. Frequently parents are sharing more information about their children than they should be, or than their children are comfortable with. According to our recent survey, 19% of parents who have social networking accounts, acknowledge having posted something online that their child may find embarrassing in the future. 13% of parents say that their child has already been embarrassed by something they have posted, and 10% say their child has asked them to remove an online post that relates to them.[184] We also heard anecdotes in our 2015 focus groups from parents who felt they may have shared too much about their children. The responsibility for protecting children's safety and privacy belongs to all.

6. Previous research studies conducted by FOSI include "Parenting in the Digital Age"[185], "Teen Identity Theft"[186], "The Online Generation Gap"[187], and "Teens, Kindness and Cruelty on Social Network Sites"[188]. We encourage the Committee to consult the research from previous years to inform their knowledge of trends in Internet use amongst children.

7. To complete the research foundation for informed public policy, FOSI has created comprehensive, user-friendly resources for professionals and consumers. For professionals and policymakers, we provide the Global Resource and Information Directory (GRID.)[189] In partnership with UNICEF, GRID was completely overhauled and updated in 2016, and now captures the challenges and responses to online safety around the world. It aggregates online safety laws, education initiatives, research and active organizations in over 100 countries to date, with a particular emphasis on efforts to combat online child sexual exploitation.

8. The importance of encouraging industry to work together to develop solutions to online safety challenges is a responsibility that FOSI takes seriously. Through private consultation and public events, we work with all sectors of the Internet industry to recognise patterns in Internet use amongst young people, and to identify problems and emerging issues to create responses before children are impacted. As an example, FOSI's

183 Family Online Safety Institute. November 2015. Parents, Privacy & Technology Use. p. 23.
184 Family Online Safety Institute. November 2015. Parents, Privacy & Technology Use. p. 22.
185 Family Online Safety Institute, November 2014. *Parenting in the Digital Age*. *Online at* https://www.fosi.org/policy-research/parenting-digital-age/
186 Family Online Safety Institute, November 2013. *Teen Identity Theft*. *Online at* https://www.fosi.org/policy-research/teen-identity-theft/
187 Family Online Safety Institute, November 2012. *Online Generation Gap*. *Online at* https://www.fosi.org/policy-research/online-generation-gap/
188 Family Online Safety Institute, November 2011. *Teens, Kindness and Cruelty on Social Network Sites*. *Online at* https://www.fosi.org/policy-research/teens-kindness-cruelty-social-network-sites/
189 Family Online Safety Institute. *The Global Resource and Information Directory*. *Online at* https://www.fosigrid.org

Annual Conference this year will focus on "Online Safety in Transition"[190] and will look at the future of policymaking on Internet safety and privacy. This is an opportunity for industry to share best practices and for policymakers, charities and teachers to identify areas where more work is needed by industry and increase awareness around existing resources.

9. Furthermore, FOSI has developed a program to provide advice, tips and tools to empower parents to confidently navigate the online world with their children[191]. The Good Digital Parenting initiative (GDP) informs parents as to the technologies, sites, apps and services that their children may be using with ways to talk to their kids about how to stay safe online. The initiative includes blogs, videos, and resources to help parents start conversations with their children about their online activities, as well as the rights and responsibilities that accompany growing up online.

10. It is essential to have an understanding of the environment in which children operate in order to create new initiatives and policies to enhance online safety and privacy. For now, it is hoped that the research findings, in conjunction with FOSI's international expertise and policy knowledge, will provide the Committee with a constructive context to their inquiry.

11. The Internet enhances the educational and social lives of children in the United Kingdom and around the world. Their use of media permits them to gain knowledge in a variety of new and engaging ways. Children are able to create and share their own content and express their ideas, thoughts and experiences on a worldwide platform. The Internet allows experiences that go far beyond their homes and communities; they are able to explore the world, immerse themselves in different cultures, geographies and periods in history instantaneously. The skills children learn through their online exploration in early life prepare them for their future and provide knowledge as well as the digital abilities that are vital for functioning in the modern technology-driven world.

12. There are harms that come with living in an online world, and they should not be discounted. Often, the skills and knowledge children have about new media far exceeds that of their parents. There is illegal activity online, just as there is offline, and there is a possibility that children can be exposed to content and actions that are harmful to their development and well-being.

13. Consequently, at FOSI, we believe the key to keeping children safe and ensuring that they have safe, productive and private experiences on the Internet, is to build a culture of responsibility online. This can only be accomplished if six separate entities work together to create a safer Internet. The key components are: 1) government; 2) industry; 3) parents; 4) law enforcement; 5) teachers; and 6) children, themselves.

14. Reasonable government support and oversight are essential components of this approach. An atmosphere of cooperation needs to be created amongst

190 *Online at* https://www.fosi.org/events/2016-annual-conference/

191 Family Online Safety Institute. *Good Digital Parenting*. *Online at* https://www.fosi.org/good-digital-parenting/

stakeholders, and cross-sector bodies, such as UKCCIS, are a great example of this. Government funding for research into online behaviours and educational efforts that promote digital literacy and parental engagement, is vital.

15. Effective oversight of industry self-regulatory efforts allows for maximum innovation and development of creative solutions, whilst ensuring that industry continues to raise the bar in the field of online safety. As part of this, FOSI encourages robust and comprehensive industry self-regulation. As a membership organisation, FOSI brings together leading technology companies, who often compete with one another on other issues or for market share, to discuss emerging trends and create best practices and new solutions to increase safety and privacy measures for children and adults alike.

16. There has never been a time when so many resources have been available for parents, grandparents, teachers, and care givers to provide protection from online risks. All of the major operating systems and search engines provide family safety settings. Mobile operators, social networks, and Internet Service Providers offer tools and settings to help protect families. Technological parental controls cannot replace involved and empowered parents, but they do continue to be a part of the solution in keeping children as safe as possible online when used to the best of their capacity. Technology develops at a rapid pace, and with each new development companies are working to stay current by creating new and innovative safety tools for parents and teachers.

17. Engaged and knowledgeable parents are vital to ensuring that children have a safe online experience. Providing and encouraging the use of online safety tools is a community-wide effort and each player in the online safety eco-system can play a role in helping parents to learn about and embrace the tools available to them. Parents can be reached through education campaigns through schools or the media, website safety blogs, and government outreach campaigns.

18. Law enforcement must be fully resourced and given the tools and training to combat the rise in cybercrime. Cross-border and cross-industry cooperation is vital to allow law enforcement officials to apprehend and prosecute those involved in illegal online activity, including the creation, sharing and downloading of child abuse material. Similar to the challenges of industry regarding the development of updated parental control software, the ever-evolving nature of criminal activity via the Internet means that providing law enforcement with proper support and training is essential for the success of their efforts.

19. Superior technology training must be provided to all teachers. This will enable them to incorporate digital citizenship teaching across the curriculum, helping children navigate the online world safely and providing them with the skills to operate in an increasingly technical world.

20. Ideally resilient children would make wise personal choices about the content they access and post online, the people they choose to engage

with, and how they conduct themselves overall online. Additionally, as part of the culture of responsibility it is vital to teach children to be media and digital literate.

21. Children must be educated on how to operate as good digital citizens. It is essential for children to know about the rights and responsibilities that come with being online, to understand the consequences of sharing of information and online behaviour and to empower them to make the right decisions when they see upsetting content or inappropriate behaviour. Through teaching children to make good choices on the Internet, they can be better protected from the risks that exist online. The skills that they learn through this process will assist them throughout their digital lives, teaching them to be informed and resilient.

22. There are numerous programs and resources offered to respond to existing online challenges such as cyberbullying, sexting, radicalisation, and concerns about screen time. However, the Committee has specifically requested input on the harms and benefits of emerging technologies. These developments may require slightly adapted responses, in order to ensure that children are able to access the benefits, whilst remaining as safe as possible.

23. The Internet of Things provides substantial opportunities for all families. Fitness monitoring devices can increase activity. Systems to monitor the vital signs of newborn babies can regulate health and smart toys can interact with children to build speech, social, and learning skills. Connected clothing, toothbrushes, and dolls can provide parents with peace of mind allowing them to better understand and improve the wellbeing of their family.[192]

24. The 'always on' nature of these devices may cause privacy concerns, whilst the fact that children are talking to a toy which responds to them raises additional data security issues. But at this early stage the exact harms are unclear. The UK Government should consider funding research into actual harms around the Internet of Things so as to provide a basis to develop solutions, including educational resources for parents and children.

25. Consumer education is essential to ensure public safety, whilst allowing innovation to flourish. All stakeholders should work together to ensure that information about how to stay safe whilst using these new technologies is easily accessible, especially to parents who may have the most concerns about their children.

26. Building on the culture of responsibility and engaging with all stakeholders can help futureproof efforts to keep children safe on the Internet as it currently exists and is accessed, as well as devices and means of access that have yet to be developed. New companies should work to ensure that they have the tools and resources needed to address potential harms and should adopt the best practices that have already been established.

---

192 For more information "*Kids & the Connected Home*" event https://www.fosi.org/events/kids-connected-home/#media

27. The government can best assist children through working as one part of the joined-up, engaged ecosystem. Their potential to raise awareness, direct funds to education and research, and to convene parties through multi-stakeholder bodies like UKCCIS is unrivalled. An open and productive dialogue between government and technology companies is often the best way to counteract many of the issues that arise online.

28. Ultimately, FOSI strongly encourages the Committee to recall the many opportunities for education, enlightenment, and exploration that the Internet offers to children in the UK. The responsibility of government to emphasise the positive aspects of the Internet and the opportunities that it provides must not be forgotten, nor diminished, in well-intentioned attempts to pursue the near impossible goal of keeping all children completely safe online at all times.

26 August 2016

Girlguiding - written evidence (CHI0026)

About Girlguiding

1. Girlguiding is the leading charity for girls and young women in the UK, with over 500,000 members. Thanks to the dedication and support of 100,000 amazing volunteers, we are active in every part of the UK, giving girls and young women a space where they can be themselves, have fun, build brilliant friendships, gain valuable life skills and make a positive difference to their lives and their communities. We build girls' confidence and raise their aspirations. We give them the chance to discover their full potential and encourage them to be a powerful force for good. We give them a space to have fun. We run Rainbows (5–7 years), Brownies (7–10 years), Guides (10–14 years) and The Senior Section (14–25 years). Registered Charity No 306016. www.girlguiding.org.uk

About Girlguiding's Evidence

2. Girlguiding's submission focuses on evidence from the Girls' Attitudes Surveys – our annual research into the opinions of girls and young women throughout the UK aged 7 to 21 and the personal testimony of young members. We also reference other research where outlined. Our young members would be keen to give oral evidence directly to the committee if invited.

3. The Girls' Attitudes Survey canvasses the opinions of over 1,500 girls and young women, inside and outside guiding across the UK each year. We commission expert child research agency ChildWise to conduct this survey. For more information and data see www.girlguiding.org.uk/girlsattitudes. Girlguiding's response is also influenced by the Girls Matter campaign – Girlguiding's member-led campaign that profiles girls' and young women's calls for change http://new.girlguiding.org.uk/report

Risks and benefits: 1. What risks and benefits does increased internet usage present to children

Benefits – Voice

4. Girls and young women are using the internet to have their voices heard and as a medium to express their opinions and take part in conversations in a way that wasn't possible in the past. Girls harness the power of the internet to take action to make a positive impact on their communities and raise awareness of campaigns that matter to them. Girls express themselves through blogs, social media, video blogs and sharing websites like Youtube, and petition websites. Campaigning has moved online, with the growth of websites such as Change.org, young people can join online communities to support many different causes. Girls and young women have joined campaigns such as No More Page Three, and a major factor in being socially active involves some aspect of online activity.

5. The 2015 Girls' Attitudes Survey found that, of girls aged 11 to 21, 25% say they share campaigns they care about on social media and 30% sign online petitions. Girls become more active as they get older, with 49% of 17 to 21 year olds saying they sign online petitions and 30% saying they share campaigns on social media. Forthcoming research from the 2016 Girls' Attitudes Survey has found that 46% of girls aged 13 to 21 agree social media empowers them to speak out about things they care about.

Information

6. Young people use the internet as a source of information and research. The 2015 Girls' Attitudes Survey found that, of girls aged 11 to 16, 33% chose online as their top choice for where they'd like to get help and support, for example around their mental health. For girls aged 17 to 21, this number rises to 66% who browse the web for mental health information.

"I'd like to see more information online for those supporting someone else with mental health problems, or who may be struggling as a result of caring for someone with them."
Girl's response to Girls' Attitudes Survey 2014

7. The 2013 Girls' Attitudes Survey found that, while the majority of girls and young women aged 11 to 21 still got get information about relationships and sex from talking to friends (63%) and from sex education lessons at school, 35% turned to the internet as a source of information and advice. For older girls aged 16 to 21 the internet was even more important, with 49% getting information about sex and relationships online.

Social Networking and Support

8. Girls and young women are increasingly using the internet to find help and support from each other. Some girls and young women find support groups online that they don't have access to otherwise which can be a vital resource. Forthcoming research in our 2016 Girls' Attitudes Survey shows that 14% of girls aged 11 to 21 use online support groups.

Risks – Cyberbullying

9. Girlguiding research from 2015 found girls are impacted by online bullying - 45% of those aged 11 to 16 report experiencing bullying through social media. 28% say they have experienced bullying by someone via their mobile phone (such as abusive texts or calls); and 24% say they have been bullied on websites or chat forums.

10. The impact of cyberbullying can be severe, with 69% of girls aged 11 to 21 saying bullying made them less interested in their school/college work, and 49% say bullying led to them taking more risks than they usually would. Around two in three girls aged 11 to 21 say the bullying stopped them from speaking out about their views (69%), made them less interested in their school/college work (69%), or stopped them from going out with their friends (66%). For a significant minority, cyberbullying had more serious

consequences. 44% of girls aged 13 plus say that the cyberbullying led them to self-harm.

11. Although it is less common among younger girls, a third of girls aged 7 to 10 have also experienced cyberbullying despite social media platforms requiring users to be 13 or older. Girlguiding research has found that 13% have been bullied on social media, 12% have been bullied by mobile phone and 8% have been bullied on a website.

Sexism and Sexual Harassment

12. The majority of girls and young women have experienced sexual harassment in the last year and the nature of the internet means this harassment no longer stops at the school gates or even the front door of home. Research from our 2013 Girls' Attitudes Survey found that 54% of all those aged 11 to 21 say they have had negative experiences online, including sexual harassment. For older girls, aged 16 to 21, 26% say this negative experience includes having had sexist comments and 25% say this includes threatening things said about or to them.

13. The 2014 Girls' Attitudes Survey found that 66% of girls and young women aged 11 to 21 say that they often or sometimes see/experience sexism online. The survey also found that, of girls aged 13 to 21, 59% had faced some form of sexual harassment at school or college, and 15% had experienced sexual abuse on social media.

14. Girlguiding's 2013 Care Versus Control Healthy Relationships report found that most girls that took part in the research (aged 11 to 17), have experienced the darker side to social media of unwanted intimate pictures and videos. Often these images came from others outside of their immediate circle, such as people in other year groups or at different schools, and the content is more likely to be material found online. Girls that do end up participating in this behaviour are often left isolated, stigmatised and unable to ask for help.

Gender Stereotyping and the Representation of Women in online Media

15. The majority of girls and young women tell us that gender inequality - including stereotyped and sexist representations of girls and women in the media and public life – negatively affects how women are treated in society. With the increased use of online forums, advertising and videos, young people are constantly accessing such media.

16. The 2014 Girls' Attitudes Survey found that 45% of those aged 13 to 21 say that they have heard about sexist abuse of women in the media on social media channels and 49% say that this restricts what they do or aspire to in some way. Girlguiding also found that 27% of girls say that this abuse makes them scared that they could also receive abuse online just for being a girl or young woman, and 26% have been put off wanting to be featured in the media themselves. Others self-censor messages to lessen the risk of sexist abuse (18%) while a 14% use social media less to avoid the risk of being targeted.

'We don't want to be objectified. It has a negative impact not only on women but also on men and young boys, and changing this could lead to a decrease in gender-based violence and rape.' Haley, Carrickfergus, former Girlguiding Advocate

Pornography

17. Girls worry that as an increasing number of young people are left to learn about sex and relationships through online pornography, this is negatively reflected in their lives and relationships. Research for the 2015 Girls' Attitudes Survey found that 53% of young women aged 17 to 21 think that girls are coerced into sex acts because boys are copying what they see in pornography and 71% of those aged 17 to 21 think that pornography gives out confusing messages about sexual consent. 73% of girls and young women aged 13 to 21 think that online pornography is damaging young people's views of what sexual relationships are like and 66% of young women agree that pornography puts pressure on girls to have sex before they are ready. Of the 60% of girls that say that they see boys their age viewing pornography on mobile devices such as phones or tablets 15% of girls report seeing boys looking at pornography most days and a further 13% see this happen most weeks.

18. Girls worry that the proliferation of pornography is having a negative effect on women in society more generally. Girlguiding research shows that 71% of girls aged 17 to 21 agree online pornography makes aggressive and violent behaviour towards women seem normal, 65% agree online pornography increases hateful language used about/to women, and 80% of 17 to 21-year-olds feel that pornography encourages society to view women as sex objects. 70% of girls aged 13 to 21 feel the increase in online pornography contribute to women being treated less fairly than men.

'Boys are expecting sexual relationships to be like in pornographic films. They "learn" from them and think girls would want to be treated how they are in them type of films.'
Girlguiding member

2. Which platforms and sites are most popular among children and how do young people use them? Many of the online services used by children are not specifically designed for children. What problems does this present?

19. Social media is extremely popular for young women and girls. In 2013 Girlguiding found that nearly three quarters of girls and young women use at least one of the main social networking sites (73% of 7 to 21 year-olds), with 96% doing so from the age of 11 upwards. For girls of primary school age (7 to 11), 25% claim to use Facebook despite the fact that these girls are clearly below the minimum age limit of 13. One in ten uses Twitter (11%) and 9% use Instagram. Among those aged 11 to 21, 90% use Facebook, 57% use Twitter and 38% are now on Instagram, which is especially popular among those of secondary school age (46% of 11 to 16 year-olds, 31% of 16 to 21 year-olds).

20. Research from research firm ChildWise found that 95% of girls aged between 5 and 16 have a computer at home and 82% have their own computer (tablet, laptop / netbook, desktop). For Girls aged 7 to 10 when asked to name their favourite websites and apps, responses are YouTube (24%), Minecraft (11%) and FRIV, an online gaming website (7%). For Girls aged 11 to 16 the most popular are Snapchat (29%), Instagram (25%), Facebook (21%) and YouTube (19%).[193]

3. What are the technical challenges for introducing greater controls on internet usage by children?

21. When asked about content controls in the 2014 Girls' Attitudes Survey the majority of those aged 11 to 21 agree that children can access too much content online that should be for adults only (71%), yet only half agree that parents should be able to control what their children can view on the internet at home (50%). Fewer than half agree this parental control should extend to what their children can view on their mobile devices (46%). Among girls aged 11 to 16, more disagree with these sorts of parental controls than agree with them.

Education: 5. What roles can schools play in educating and supporting children in relation to the internet? What guidance is provided about the internet to schools and teachers? Is guidance consistently adopted and are there any gaps?

22. Education is a key preventative mechanism to enable all young people to develop the skills to negotiate using online forums and to address issues they face. The 2015 Girls' Attitudes Survey found that 90% of girls aged 11 to 16 say they have been taught about staying safe online at school and the 2014 survey found among those aged 7 to 10, 78% have learned at school about personal safety on the internet. There are some areas of being online that young people still want to learn more about, particularly how to deal with online harassment.

23. Quality statutory Personal, Social and Health Education (PSHE) and Sex and Relationships Education (SRE) that is modern and relevant can help teach young people about the benefits and risks of using the internet and how to stay safe online. Girlguiding's Girls Matter campaign called for the government to introduce statutory and modernised sex and relationships education so that lessons included online safety among a number of topics. Schools are in a unique opportunity to engage with all young people around the use and impact of pornography and provide a space to discuss how this affects young people's understanding of sex, relationships and consent, statutory SRE is an ideal space in which to do this.

24. Girlguiding produces a guide on web safety for its members[194] and the Girlguiding programme contains resources on how to use the internet and stay safe online.[195] These resources, along with material produced by

193 http://www.childwise.co.uk/reports.html#monitorreport Section three; p.15
194 http://girlguiding.org.uk/Guides/assets/pdfs/GuidesWebSafety.pdf
195 http://girlguiding.org.uk/Guides/websafecode.html

partners, such as Three[196], help young people learn about the positive and negative potential of the internet and to approach anything they see online critically.

25. The British Board of Film Classification (BBFC) has done some excellent work in recent years in working towards limiting young people's exposure to sexualised imagery, particularly in age ratings for music videos and age verification for pornography to make it less accessible to children and in challenging the normalisation of access to pornography.

26. It is also important to provide education to adults so they have the skills to talk to young people about these issues.

"By introducing quality, compulsory PSHE schools can play a key role in educating and supporting children in relation to the internet. Young people should not only be taught about strangers online and cyberbullying, but how to deal with harassment from strangers and how to be polite while sharing opinions online. It is also important that we demonstrate to children that not everything they see online is true, and teach them how to determine how reliable a source is. Easy access to pornography is also very dangerous for young people as it creates unrealistic expectations of sex. It is impossible to censor the internet, so instead we need to educate teenagers about sex, porn and what's real and what's not." Katie, Girlguiding Advocate, 16

"We can't and shouldn't keep young people from having full access to the internet; it is our right to be able to make full use of it. However, I think more needs to be done to educate young people about using the internet so that they can utilise it confidently and safely." Katie, Girlguiding Advocate, 16

Legislation and Regulation: 9. What are the regulatory frameworks in different media? Is current legislation adequate in the area of child protection online? Is the law routinely enforced across different media? What, if any, are the gaps? What impact does the legislation and regulation have on the way children and young people experience and use the internet? Should there be a more consistent approach?

27. Girlguiding would like to see the introduction of greater protections for young people, and a consistent approach across all media, bringing online media in line with the principles of the broadcast watershed. We also look forward to working with the Government as they work towards the implementing provisions in the Digital Economy Bill to introduce age verification checks on potentially harmful adult content websites, which includes an effective regulator.

28. Girlguiding research from 2014 found 85% of young women aged 17 to 21 agree that the government has a role to play in making sure the media represent women fairly and 55% of those aged 13 to 21 think that social media companies should take more responsibility for making sure users are safe.

196 http://digital.girlguiding.org.uk/how-staying-safe-online-can-help-you-with-your-next-badge

'We need tighter controls on access to internet porn, changes in advertising and the media to stop sexualising women, and more about consent covered from a younger age.' Girlguiding member responding to 2014 Girls' Attitudes Survey

10. What challenges face the development and application of effective legislation? In particular in relation to the use of national laws in an international/cross-national context and the constantly changing nature and availability of internet sites and digital technologies? To what extent can legislation anticipate and manage future risks?

29. International collaboration is vital to tackle these issues and for legislation to be effective and not simply bypassed.

11. Does the upcoming General Data Protection Regulation take sufficient account of the needs of children? As the UK leaves the EU, what provisions of the Regulation or other Directives should it seek to retain, or continue to implement, with specific regard to children? Should any other legislation should be introduced?

30. Girlguiding is concerned that the legislation does not take into consideration sufficiently at what point a young person owns and has access rights to their own data. The Information Commissioners Office refers to ages 12 and up as the age of responsibility although legislation states from when a child is cognitive. Some greater clarity on age would be welcomed.

12. What more could be done by the Government? Could there be a more joined-up approach involving the collaboration of the Government with research, civil society and commerce?

31. The government should listen to children and young people and actively seek their views to inform the next steps they take on this issue.

32. The Government should introduce statutory PSHE and SRE that includes information on staying safe online. The Government should update the Sex and Relationship Education Guidance that has not been modernised since 2000 and fails to reflect the rise of the internet and social media since that time, and the integral part it now plays in children's lives.

33. The Government should continue with its plans to implement age verification checks on websites that contain adult content and create and effective regulator that has the powers to properly enforce its will and fulfil its functions.

34. There should be an expectation on platforms that provide internet services to address violations of their own community standards. These companies should have a responsibility, embedded in their cultures and adhered to, to take responsibility for how their platforms are used, especially when it comes to misogynistic and sexist content, that while might not break community standards do not reflect the spirit of the rules.

Girlguiding - written evidence (CHI0026)

August 2016

Adam Glass and ICO – oral evidence (QQ 44-51)

Tuesday 11 October 2016

Watch the meeting

Members present: Lord Best (The Chairman); Lord Allen of Kensington; Baroness Benjamin; Baroness Bonham-Carter of Yarnbury; Earl of Caithness; Lord Gilbert of Panteg; Baroness Kidron; Baroness McIntosh of Hudnall; Baroness Quin; Lord Sheikh; Lord Sherbourne of Didsbury

Evidence Session No. 3 Heard in Public Questions 37 - 51

Examination of witnesses

Adam Glass, Partner, Lewis Silkin Solicitors, and Steve Wood, Interim Deputy Commissioner, Information Commissioner's Office.

Q86 **The Chairman:** Welcome, Adam Glass and Steve Wood. Thank you very much for waiting patiently to join us. As you can tell, we were deeply embedded in the previous session but we are delighted to have you with us as our legal experts today. Thank you for joining us. I am going to ask you both to introduce yourselves. If you could do that and if from the Information Commissioner's perspective we could hear about your current role and whether that might be strengthened, you might just throw that in in your introductory remarks, and whether the ICO has a specific policy or approach regarding children, and children of different age groups indeed, that would be a helpful opener for us to get us cracking. Steve Wood, would you lead away with those themes in mind?

Steve Wood: Thank you very much, and thank you for the invitation to come and speak to you today. My role is deputy commissioner at the Information Commissioner's Office. We are the UK's independent regulator of the Data Protection Act and the Freedom of Information Act and another piece of legislation called the Privacy and Electronic Communications Regulations, which covers areas such as direct marketing.

Regarding the ICO's role focused on data protection, we have a range of powers and functions under the Data Protection Act. We can hear and adjudicate on complaints from members of the public; we have enforcement powers, so we can take action against organisations called data controllers under the Data Protection Act—we can take enforcement action to force an organisation to stop using personal data, for example. We also have the power to fine data controllers under the Data Protection Act. We have had those powers since 2010. You may have seen the latest fine we issued in the media last week, which was the £400,000 against the internet service provider TalkTalk. We also have a

role and a function in disseminating good practice to organisations. That is really about education and guidance.

We also have a role in promoting guidance and awareness—

The Chairman: Sadly, we need to interrupt you, and you have only just started. Profuse apologies; we need to vote on this amendment.

The Committee suspended for a Division in the House.

The Chairman: I was asking you about the ICO's policies and whether there was a particular approach regarding children, and indeed children of different age groups. Steve, I am afraid we cut you off in full flow on that theme.

Steve Wood: Thank you very much, Chair. Yes, I will continue. I gave a general overview of what the ICO does earlier but I will talk a bit more about our activities in the area of children, and particularly relating to the internet.

The first thing is I think increasingly, particularly over the last five years, the ICO has recognised the importance of the issues that have emerged, and has started to develop further strategies to look at the issue. The first area where we have done a considerable amount of work is in the area of education. Originally, going back over five years, the ICO had a specialist section on its website aimed at young people and children, which was not particularly well used. We took further advice from experts, which said that for the key messages the ICO had about children and young people becoming more aware of how to control and manage their own personal data, we were going to have to do more to embed this in teaching in schools. We invested a considerable amount of money in a project working with education consultants from the University of Edinburgh to develop a programme of developing teaching materials for primary and secondary schools, which we have promoted to teachers. We also responded to Department for Education consultations on the national curriculum to try to have these issues better embedded in the national curriculum.

The approach we have taken, and the reason we try to embed the information in the curriculum, was particularly trying to understand the difference between e-safety, which was starting to be taught more in schools, and the concept of individuals learning how to control and manage their personal data and feel empowered, which is a slightly more nuanced topic. We wanted to add something from that perspective, so we have continued that work and will continue to promote the use of those materials.

We are also aware of and interested in the possibilities of greater partnerships with organisations, as certainly the Data Protection Act and the ICO do not have all the solutions in this area. We have a relevant and useful role to play, so the more we can work with other regulators and develop partnerships, the more we can tackle that, which is another area.

On our approach to guidance to organisations about issues relating to children, we have not developed a lot of specific guidance, labelled as guidance, about processing personal data about children. We have more

taken the approach to embed children's issues in lots of different pieces of guidance, so we have guidance about processing personal data in mobile applications; we published a new piece of guidance last Friday about privacy notices, which is obviously an important issue relating to transparency on the internet, and we had a section relating to children in that. We are very much focused in the guidance we are producing always to highlight to organisations the importance of the particular issues relating to children. Because the Data Protection Act does not have any particular reference to processing children's personal data, we developed what we called a risk-based approach in our guidance, which stresses the importance of organisations assessing for the type of processing they are doing, the types of uses of personal data and the types of personal data they are collecting, what types of safeguards they should put in place relating to that context to make sure they can understand the particular situation that they are processing the personal data in. In some situations that could include parental consent but we have not taken a blanket approach to that; we have taken a risk-based approach. I will leave it there.

The Chairman: Thank you very much. Please introduce yourself, if you would, and Lewis Silkin as well.

Adam Glass: My name is Adam Glass. I am a partner at the law firm Lewis Silkin. My area of expertise is media and IP litigation, so I have a lot of experience in representing clients who have problems, often online, whether that is defamation or misuse of private information or that kind of aspect. I have a lot of experience of the practicalities of trying to obtain remedies for them, and using social media platforms to obtain information from them on which to bring a cause of action or obtain a remedy for clients.

The Chairman: Thank you very much.

Lord Gilbert of Panteg: Can I pursue the discussion the Chairman started about how you view children and young people in different age groups, and in particular the balance between intrusion, which is necessary to protect them—schools have a duty to protect children but it is quite intrusive—and their rights to privacy, and whether that balance changes as children and young people get older?

Steve Wood: I am happy to answer that. The Data Protection Act has a number of principles embedded in it, including the concept of fairness and transparency, and also the concept of legitimate interest, which should allow a school or an organisation which wants to use personal data in those situations to assess the type of data they are collecting and to make sure it is fair, transparent, and proportionate. Transparency might either need to go to the parent, depending on the age of the child, or to the child. The Data Protection Act has these principles, which we believe are flexible, which will allow an organisation to act in the best interests of a child in particular situations but also to consider the intrusion into privacy that might take place.

The Data Protection Act sets out a number of areas where organisations always have to focus on proportionality as the key principle, making sure

they are only collecting the information they need. That is a duty on all organisations under the Data Protection Act.

Lord Gilbert of Panteg: You have no specific view or guidance as to how that balance changes for different age groups?

Steve Wood: We have not gone down the route of saying it changes at age 13. Our approach is to look at the particular situation. It may be in certain situations a child of 13 could understand what was being explained to them and it might be fair in that situation to provide some information for the child and for them to be able to interact with it. In other situations it might not be appropriate.

The stress and emphasis we want is to put it back on the organisation. There is not an easy slide rule to go to in guidance to say the child is age X, therefore you need to do X, Y and Z. The responsibility is on them to assess the particular context of what they are doing. The key tool we promote for this, which is not specifically focused on children, is a concept called a privacy impact assessment. If an organisation was doing something unusual or extensive with personal data, we would say they need to complete a privacy impact assessment, which has a series of questions to guide them through the right balancing exercise which perhaps you are alluding to. The General Data Protection Regulation, which will come into force possibly in 2018, will contain stronger provisions on data protection impact assessments, explicitly promoting them on the face of the law, which we think is a positive development.

Q87 **Lord Sheikh:** I want to ask you about the amount and volume of work you do on data collection and legal sharing of data. Are we doing enough? Should we increase it? If we were to increase it, what would the benefits be? The second part of my question relates to what the ICO told the Committee: "In reality there may be little that can be done to prevent unscrupulous third parties from harvesting a child's data and using it for inappropriate purposes." How can this situation be improved or mitigated, for example through making data collection more transparent and understandable for children?

Steve Wood: I will answer both of those questions in turn. The issues which often emerge around the benefits of increased data collection and data sharing will depend on different sectors and different uses of data. Certainly in the commercial internet sector, better use of personal data can lead to better products for individuals. It can lead to more personalised services that individuals like using, and for a child that can mean that a cookie is set on the computer which means they can go back to carry on the game they are playing. Those are the sorts of benefits that can come from personalised services, which sometimes need unique identifiers or more information about individuals.

There are certainly benefits which can come from the use of data, particularly when it is aggregated for research purposes and social benefits in those areas. Where we would stand on all those issues as the ICO is making sure it goes back into that process I talked about earlier, still making sure the uses of the data are necessary and proportionate, and how they are balanced against the harms and the issues for the individuals. The heart of it must be that we need to do better on

transparency, making sure people understand how the data is used in those situations.

Turning to your second question, about what can be done to prevent the harvesting of personal data of children, we made that statement to highlight the importance of getting things right first time. That goes back to the importance of transparency and better user controls for children and young people on the internet, because once a picture or a piece of information is publicly available on a website, as it stands, it is quite easy for that information to be harvested and re-used. Our emphasis is on much better prominent and clear controls for individuals, so it is only one click away or it is very accessible. Equally, it does not just have to be one notice on a website that does this. The document I referred to earlier that we launched last Friday, the new *Privacy notices code of practice*, has tried to get away from the concept of a big, monolithic document—we have all seen them; the statements about them being longer than "Hamlet", et cetera—very much privacy information can be embedded and can pop up in lots of different places in a website to build someone's knowledge as they understand what the service is doing with their information. Organisations have to redouble their efforts in transparency and better controls.

There probably also needs to be more innovation around technology. Is there more that can be done around standards and ways that data can degrade or automatically expire and can easily be re-used? We do not have all the answers to those questions at the ICO but under the new Information Commissioner, Elizabeth Denham, who took up post in July, we are in the process of establishing a more significant technology function at the ICO, and a grants and contribution programme; we would hope to actually fund innovation in this area to see if there are better privacy-by-design solutions, to try to work with industry to get that type of work developed.

Lord Sheikh: A very quick supplementary: how safe is your data? With all these people breaking into the data, how secure is your collection?

Steve Wood: It is a question which was obviously at the top of the news last week, when we issued that fine against TalkTalk. TalkTalk is a large internet provider, but the attack on TalkTalk involved a technique which is relatively simple, because it was undertaken by some teenage hackers. Data can be secure; organisations can secure data completely or absolutely, but they must constantly redouble their efforts to secure the data. We are saying security and data protection should be a boardroom issue; it should be recognised at a high level of organisations so that the messages go down from the top.

Baroness Kidron: Can I just ask something very precise about what you are saying? The work you are doing around terms and conditions is fantastic but there is one fatal flaw: if you do not tick "Yes", it does not work. Not only in building up a profile but in little pieces and learning to say "Yes" to specific things, is there something you can do with industry that allows people to use services? Young people in particular have a real problem: if the service does not work unless they say "Yes", what kind of choice is that?

Steve Wood: I guess the point you are making is sometimes it is a take-it-or-leave-it approach.

Baroness Kidron: Almost always.

Steve Wood: We are aware of the pressure on young people to use certain types of services. We are interested in whether sometimes there should also be a granularity of consent. The case where we took action on that involved a public sector body. UCAS, the university admissions organisation, had a mechanism where third parties could direct-market to individuals on the UCAS database, and the consent for that was wrapped up with individuals wanting to receive the marketing and also information about careers and health. Perhaps the child would want the information about careers and health but not the marketing. In that situation we made them sign an undertaking to separate out the consent. I cannot say too much about it, but we are also investigating the current case involving WhatsApp and the sharing going from WhatsApp to Facebook in the new terms and conditions. That is pretty much a take-it-or-leave-it situation, with not a great deal of control about the data. That has triggered our interest.

Baroness Kidron: That is a policy issue, not a technological issue.

Steve Wood: Yes. The solution is in a range of areas. I would not say we have cracked all those problems but I was trying to say we are aware of it and we are trying to do more to promote that approach.

Baroness Benjamin: On the subject of personal data, at what age can someone be said to be able to understand an agreement they are making regarding their data and its usage, as well as other terms and conditions? What evidence is there to suggest that 13 is the appropriate age at which parental consent is not needed?

Steve Wood: It is a difficult question. The evidence for age 13, particularly in the online context, is mixed on how appropriate a very broad cut-off date is. In the European data protection regulation which has been negotiated in Brussels over the last five years there was extensive debate about what the age should be in that legislation. In the end EU member states could not agree, and they put in the age of 16 but gave the member states the choice to decide to lower it to 13 if they wished. To have a broad, blanket provision in law which can link into a particular age indicated perhaps the lack of strong evidence. There probably is a need for more research to understand what the particular issues are online. Age is often quoted in other contexts, and perhaps learning could come from other sectors about where young people are consenting and that has become the rule of thumb.

Certainly the experience, and the evidence I am sure you have heard as well, is obviously that 11 and 12 is a crucial age, because it is when children start secondary school. In the year before they start secondary school there is a lot of pressure and a lot of interest in starting to use online services. The age issue probably needs to reflect the current circumstances, which is why we were quite cautious in our support for the age level set in the General Data Protection Regulation, because we were worried it was a broad cut-off and might give a false sense of security once that consent is given in that situation, because once the

consent is given, in any case the young person is still using the service, and it is how the service protects them as well. It is only one solution in the whole situation.

We are supportive of a risk-based approach to using age verification in certain situations. It might be a blunt-edged tool if it is used very broadly, and will it have the intended effect?

Adam Glass: The answer to the question is it seems to be that somewhere between 13 and 18 is where people think a child or young person can understand an agreement. Obviously, generally UK law is that under 18 you cannot enter into a contract, with a couple of exceptions. In some ways it is arbitrary. I think 13 is probably very much following the lead from America and American legislation. A lot of social platforms are US-based and have legislation that says 13 or under in relation to data protection collection.

Obviously, the GDPR that may be coming in in a couple of years sets that arbitrariness at 16. I am not sure the ICO is being cautious, because member states cannot go lower than 13, so between 13 and 16. The ICO I think is plumping for 13, so the lowest age range. I am not sure if that is cautious. Basically, between 13 and 16 seems to be the fluidity. Of course, some children are more mature than others, some are more vulnerable than others. There is no science to this. I am sure there have been lots of social studies done by academics or whatever as to when and how, but I cannot see how anyone can positively say that you would definitely understand something at age 13, 14, 15 or 16. Obviously, someone has to take an informed decision, and it seems that between 13 and 16 in the next couple of years is where it will be.

Baroness Benjamin: Is there a role for parents to play here then?

Adam Glass: There is always a role for parents to play.

Baroness Benjamin: Some parents do not literally understand the rights and what their children are exposed to and what they are doing.

Adam Glass: I think that is absolutely right. I am not sure children and young people understand their rights—almost certainly not in relation to what their data may be used for. I am sure if you took a straw poll outside the school gate, most parents will certainly not have heard of the GDPR and probably do not know the rules around data protection in the sense that lawyers do, or people involved in using the Data Protection Act to further a means, for example a legal remedy. I am sure parents do not understand.

Baroness Benjamin: If children understood how their online material and data was being used, do you think they would be horrified? Should they be educated about this?

Adam Glass: Of course, and I think the education is going on, and even younger than the age when at the moment they can give consent. I have a daughter of nine and she is already interested and wants to explore the internet. She is not getting that opportunity yet from me but it is way younger than 13. The duty or obligation is of course across the remit of schools and parents. At my kid's school quite a lot is done: they have a lot of classes and whole-school discussions about online, the dangers of

being online rather than necessarily how their data is being used; the dangers of chatting to people you do not know or may have only met once, and things like that. Absolutely, if we can educate parents more, it has to be a good thing. I am not sure how you can enforce that or make it better [as relates to parental involvement with their children].

Q88 **Baroness McIntosh of Hudnall:** From the point of view of legislation, or of us as legislators, there is quite a lot in the ICO evidence that you submitted to us, Mr Wood, where you stress that age verification, for example, is not an altogether useful tool, that it has drawbacks, and that anyway, as you put it, a resourceful child can almost invariably get round it. Why are we spending so much time arguing? It feels like an angels on a pinhead kind of argument whether it is 13 or 16 or 15 or something in between, because who is going to be in a position to enforce it? I am overstating that but is there an answer?

Steve Wood: The way I would answer is that it always has to be the responsibility of the organisation processing the personal data; they have the responsibility to assess the risk of the type and the nature of personal data that they are using.

Baroness McIntosh of Hudnall: But how are they to verify the source of that personal data or those personal details? If you say you are not competent to enter into an agreement to supply that data unless you are—fill in the blank—but you, the agent in this, the child, are perfectly capable of submitting a completely false prospectus to the internet provider, which will absolve them of any responsibility for not having done their bit of it, what are we to do about this?

Steve Wood: To go back to the responsibility of the organisation, they have a responsibility to assess the risk in that situation, and, depending on the risk, they should put in place more robust solutions to verify the age and the identity of the individual and the parental consent. That is the approach taken by the Federal Trade Commission in the US. It is still not a perfect solution—you played the evidence back to us in that a resourceful child can sometimes get round it in these situations, which is why I think it is quite important to come back to the basics, that organisations should only be collecting the information they really need in that situation, because that reduces the risk as well. It will be a combination of factors which tackles this tricky problem you have rightly highlighted.

Adam Glass: I was just going to say something about the robustness of the process: if a child says "I want to go online", "I want to receive some data" or whatever, and clicks, the process can be that they put in their parent's email, that email is pinged to the parent, who can look at the privacy notice, et-cetera. With the better platforms, they will then go through, for example, a ghost payment on a credit card information, so the parent will get a phantom transaction, will have had to click on that, provide their credit card details, so they will know that their kid has given their information, wants to be set up on an account, and the parent will have gone through that whole system for that, and they will not be able to be registered until the parent clicks and says, "I have

given my credit card and I can see it has gone through." The better platforms do that well. That is one way of having good verification.

The other method of enforcement of course is lawyers occasionally holding people to task if they do not. There was a case last year, which has been settled, confidentially settled, against one of the social platforms, where a father brought a case on behalf of his vulnerable child, who was 11 at the time. The child had set up multiple accounts and was posting and receiving information from men, and posting inappropriate sexual pictures. He brought a case, and basically accused the platform, held them to a duty of care, and said, "This is a negligence case. You have a duty of care to my child. You should have ensured the verification process was tougher." That did not go the whole way, but there is a way. Of course, we have better law sometimes by taking some cases and obtaining judgments, whether statutory or common law.

Baroness Benjamin: I was going to touch on the law. As there is currently no specific provision regarding children's data in UK law, do you think there needs to be some sort of law and would it be workable in practice?

Adam Glass: I do not think we do. I think there is enough. We generally have good data protection laws, the Data Protection Act. The GDPR, as you have heard from various commentators, will specifically probably strengthen and clarify certain aspects of that, in relation to lawful processing, transparency, legible, plain English.

Baroness Benjamin: But does it focus on children?

Adam Glass: Yes, Articles 6(a), 12 and 17 specifically relate to and mention children, for example 12 being transparency and plain language. It specifically says "if aimed at children", that needs to be intelligible, transparent, clear, but also plain and clear for them to understand. Article 17, the right to be forgotten, will again specifically relate to data that was processed when you were a child, even perhaps if you are now an adult, that should be able to be deleted, and for further onward dissemination to be stopped.

Baroness Benjamin: Is it working?

Adam Glass: The GDPR is not in yet, but what I am saying is there are those specific references to children in those Articles [to the legislation]. It will depend on member states how widely or narrowly they interpret the general framework, and of course, with guidance from the ICO as to where they think we should be heading.

Baroness Kidron: Just on that last point: however, we are leaving the European Union.

Moving swiftly on, you said something, Mr Glass, about companies responding more quickly to copyright issues because they carry financial penalties rather than questions of harmful behaviour. I am interested in your position on that. Do you feel strongly about that? You seemed to be suggesting the law was in place and maybe if there were financial penalties—

Adam Glass: My experience is, certainly in the past—and things have changed quite a lot over the last couple of years—that social media platforms were more worried about an IP complaint, so to take down a picture, for example, and that would come down pretty quickly if you could show you were the owner of the copyright. They did not seem as worried about defamation, bullying, harassment. As I say, I think the tide has gone the other way regarding bullying and harassment, partly because of the terribly sad cases that we see in the press of children taking their own lives because of online bullying, and the social platforms have changed their game and upped it in the way that they respond quite quickly to those kinds of issues now.

Defamation has always been a tricky one. I have some sympathy for the platforms, because they do not want to be the arbiter or the judge on the balancing act between freedom of expression and defamatory material. There is no doubt in the past they would keep that up and take off the IP stuff pretty quickly. Whether or not there should be tougher financial penalties—I am not sure that would make a lot of difference to the big players, for which it is a pinprick to be fined anything.

Q89 **Baroness Kidron:** In this area of enforcement, I was also going to ask about this personal family and household exemption that the ICO have taken exception to. I do not think we understand it 100%. Maybe you could unpick the problem for us.

Steve Wood: There is an exemption in Section 36 of the Data Protection Act which essentially provides an exemption when an individual uses personal data for their own household, personal or family use. If individuals set up a group on the internet to share photographs after a holiday or to interact with each other in that situation, the Data Protection Act is essentially saying that those individuals are removed from any responsibility as being data controllers themselves, as individuals, under the Data Protection Act, so we cannot take action against them as the ICO if that use is for purely household, personal, family use.

It does not absolve the internet company hosting the photographs. The issues obviously come in particularly how they would react and must have the take-down systems, et cetera, to be able to take down the content quickly if an individual complained about a certain type of information that was posted.

The Data Protection Act in its construction is probably more focused on making organisations accountable rather than on an individual to individual situation, which is obviously a different step for a regulator such as the ICO to take when there are other legal remedies, prosecutions, et cetera, for defamation which can be taken in a certain situation. Members of the public understandably can be very confused, and will come to us in certain situations where they have had an upsetting experience online, and perhaps will complain about an individual to us. We are trying to improve the signposting of where individuals can go if we think we cannot help because of the way the Data Protection Act is constructed. We are not necessarily criticising the Data Protection Act, because it is a big step for a regulator to step into

that individual's space, which is important for freedom of expression reasons. It is quite welcome that yesterday, for example, the CPS published new guidelines about prosecutions for hate-speak online in relation to social media. That gives us a better place to signpost to give people when they are in an upsetting and difficult situation and there may be a remedy available to them in another area of the law.

That is how that particular exemption works. We would probably more target our enforcement action against a data controller, to make sure they take their responsibility seriously, particularly if there were repeated or systemic problems, perhaps repeatedly not reacting to take-down requests from individuals in genuine situations where they should be looking and considering those carefully.

On the point about what we can do under the GDPR, where the step change is, at the highest level it is possible to fine 4% of global turnover, which is what is called a competition-level fine. It is more serious. We wanted to have that really big stick in the cupboard. It would be for the most serious cases and will probably be used rarely, but it does up the game in getting organisations to take it seriously, so more of our efforts will always be focused on organisations rather than that individual to individual interaction, which is exempted under the Data Protection Act.

Baroness Kidron: Very briefly, I would like to ask this, as so many young people complain about non-response. They do not understand how they can work out their takeaway is two minutes, one minute, 30 seconds, at the front door, but when they make a complaint they find it very difficult to know whether it has been opened, responded to, what the status is, and so on. I wonder whether you think that the culture, and the law or regulation, are in the right place regarding complaints.

Steve Wood: I think organisations have to continue to up their game in that area. If the number of complaints increases, they have to think about the reasons why that is happening. In the situation you described, that quite a few years ago perhaps they were more responsive to copyright infringements probably was true. As Adam said, I would agree it is improving, there is a better prominence and availability of those services.

Also, the individual should be able to do it themselves; self-service is the best option; to easily press a button to delete or remove your data in a clearly useable service is probably the best situation. The position can improve.

We also have better case law now. We had the Google Spain judgment a few years ago about the so-called right to be forgotten, which enabled individuals in that situation to request that search results against their name be removed from Google. Initially Google resisted that, and were not interested in that type of area, given how that would interact with their business model. Once the judgment came in, they had to comply with it, and in fairness to them, they have invested in improving that service. Google are also fairly transparent. They have published quite a lot of data about when the take-down requests are coming, and they are removing things such as social media results from search engine results. Lots of those cases are probably young people who did something

embarrassing when they were 14, are now applying for university and they want that information removed from the search engine result. It is a step in the right direction that the case law is helping in that situation.

Q90 **Lord Sherbourne of Didsbury:** A very simple question: in your evidence, talking about taking down content, you said, "Perhaps service providers should be encouraged – or required – to do more to clean up problematic content from their networks." Just give me one or two specific ideas that you have in mind for what you would like them to be required to do.

Steve Wood: I think it comes down to when they need to be proactive and when they should be monitoring the information they hold, to understand that information, particularly—it goes back to the answer I gave before—about when an individual has information that they want to have forgotten. The organisations which hold that information should be responsive to that request.

Lord Sherbourne of Didsbury: When you say they should be required, do you mean by legislation? How would you require them to do it?

Steve Wood: With the legislation, if the GDPR comes in, to some extent, Article 17 of the GDPR will give the right to be forgotten, which is the right to request to have information deleted. There is the possibility that that will come in and that will provide some of that remedy. Some of it may come down as well not just to legislation but making sure that particularly the major providers all understand the good practice of having a very responsive system to take-down requests.

Lord Sherbourne of Didsbury: How would you make sure they did?

Steve Wood: There are different ways we can do it. We could do things such as proactive audits, where we can go and look at how the different providers are responding. We did what we call an international sweep a few years ago, working with other international data protection authorities. We went and looked at the websites of different organisations providing services to children online, and we then publicised the findings. So there are different ways we can do it.

Lord Sherbourne of Didsbury: That is encouragement really.

Steve Wood: Yes. Probably a mixture of hard and soft measures will be needed.

Baroness Quin: I have a question but I just wanted to pick up on something else. You referred on a number of occasions to the right to be forgotten. I may be wrong in this but I had a feeling that the Government's view was not very much in favour of the right to be forgotten. From what you have said, you sound more favourable towards it. Can you explain what the current thinking is about this?

Steve Wood: Yes. We are an independent regulator, so our view can be different from the Government's view. I gave evidence to this House after the Google Spain judgment in 2014, so I am quite aware of what the issues are. When the judgment first came out, the term "right to be forgotten" was quite emotive; people thought it was about censorship, deleting information; quite strong analogies were used about taking

books out of libraries, when actually, if you look at the judgment, it is a more proportionate measure. It is about the right of the individual to have search results which are returned against their name—so you type in someone's name, a certain link appears in that search result, the individual makes the case as to why that search result should not appear against their name. It does not remove the information completely from the internet in that situation, but it was about removing it from Google in that situation, because that can be one of the most personally intrusive things, as the way you look up someone when you first meet them is you put their name into the search engine. It is quite a proportionate step in starting to give an individual some more control over their data.

They could also go to individual websites and ask individual websites to remove the information. It was portrayed quite negatively in the media I think because they saw it as censorship. The reality is that it is a proportionate tool for individuals to control their information. Equally, it is not a magic bullet in solving quite a difficult problem; if you have a mass of information about you on the internet, it is very difficult to get it removed.

Q91 **Baroness Quin:** That is very helpful. Thank you. I was also going to ask, and you have touched on it in answers particularly to Baroness Kidron earlier, regarding industry: is there more that the industry could do to make their data collection practices and other terms and conditions clearer and more understandable for children? I know you touched on this before but have you any further thoughts about it, in particular how companies could be either (a) encouraged or (b) required to adopt such measures?

Steve Wood: I will try not to repeat the answer I gave before. We would say there is more industry can do. Again, to reference the forthcoming GDPR, there is a stronger provision in that for codes of practice, and they specifically say that codes of practice could be drawn up relevant to children's issues. To have some stronger codes of practice for industry might be one way of addressing it, which is a tool we could develop in this country, or industry-wide across Europe, to look at the particular challenges.

I would say it is always the mix of the regulatory tools we will use. We will take on and look at and investigate the worst abuses, and those might be enforcement cases or investigations to make an example of the worst cases. We need to improve the guidance to make sure organisations are getting the basics right. Industry needs to do more of its own codes of practice, to be constantly raising the bar. We want it to be a competitive advantage of a company to sell themselves on their privacy practices. It is starting to happen but it is still probably in its infancy. Why should it not be the case when someone is looking at two competing services that they could think "I want to use that one because it is more privacy-friendly"? In an area with a lot of market domination, and obviously market domination is not our responsibility, that is where the challenge lies.

Earl of Caithness: Does it make any difference to your work whether we are in or out of Europe, and, if we are going to be out, do we need to bother to enforce GDPR?

Steve Wood: This is obviously a question for the Government to decide. We are the regulator and not responsible for what the rules should be. Our view as a data protection regulator would be that the case for a strong, effective, progressive data protection law, whether that is a UK law or a European law, is strong because the challenges of the digital economy and all of the issues we have been talking about today remain the same whether we are in Europe or out of Europe. We will always make the case to Government to make sure we have a strong data protection law, with the right building blocks in place. Lots of those building blocks are in the GDPR, which could come into force in 2018, before we leave the EU in any case.

Businesses are telling us they want guidance, because they do not like the uncertainty. They obviously want to start preparing for the new law, and if that is going to include age verification, obviously it is important for them to invest and plan ahead. That is the feedback from businesses. Multinational businesses operating across Europe in any case will want to think about complying with the GDPR because of their European operations as well. It is still a relatively early stage of these issues being discussed about the future of data protection. That is as helpful as I can be.

Q92 **Baroness McIntosh of Hudnall:** The related question, which I hope you will be able to enlighten us about, is this upcoming issue of net neutrality in relation to European law, which we may or may not, presumably, be obliged to conform to, depending on what happens over the next couple of years. Can you give us some sense of what impact, if we are going to be in the position of implementing the net neutrality rules, that will have on the arrangements the Government already has with ISPs?

Steve Wood: The issue of net neutrality is actually the responsibility of Ofcom. I am cautious about saying very much about that matter because it is not our regulatory responsibility.

Baroness McIntosh of Hudnall: Does either of you have a view? Given that there has been quite a lot of work done, as I understand it, to try to go for an opting in rather than other kinds of arrangements with ISPs, if this were to come in, would it be likely to undermine some of the protocols that we have begun to build up already?

Adam Glass: In what I have read about it, I have not seen anything that would mean it would affect the current protections we might have in relation to this area, but I have to say the pros and cons of net neutrality is a trillion dollar question. I have not quite reached the bottom of what it might all mean.

Baroness McIntosh of Hudnall: And you may never have to.

Adam Glass: Quite. It was recently voted down with the amendments at the European Parliament. Who knows what may or may not now be implemented?

Baroness McIntosh of Hudnall: The recommendation would be to ask Ofcom, would it?

Steve Wood: Yes. There are some parallels between areas such as the importance of transparency, for example, so we will discuss that with Ofcom in trying to make sure we give consistent messages if net neutrality does come in between transparency and the data protection rules and transparency in relation to net neutrality, to make sure these things are reasonably well aligned. That is about as much as I can say.

Q93 **The Chairman:** You may have some final thoughts for us, including any comments on the guidance from the Director of Public Prosecutions that we have been hearing about recently. Please share any final thoughts with us before we break. Adam possibly first.

Adam Glass: From the practitioner's point of view, my frustration when representing clients has been that certainly the civil or criminal route each has its own value. Generally, with the civil route, where, for example, you might have the most success in trying to get something removed straight away from the internet—if there is an emergency you can get an ex parte injunction, for example—whereas with a criminal matter you are in the hands of the state and the investigation, and you may get no interim order from a judge to get anything removed, and he does not have that power effectively. Often I am looking at the civil route, and the difficulties are often that you are going to multiple people—it might be a mobile phone company, it might be an email provider like gmail or Yahoo—trying to get information because I want disclosure of someone who is hiding behind an anonymous IP address. To try to get to the bottom of that can often take multiple attendances on a Master in the Queen's Bench Division to get an order that I then have to serve on the various people to get the information. That will often have to go to the US, because that is where the servers are placed. The difficulties in getting to somewhere where I can actually serve a letter, to find the person that I want, can be time-consuming and very costly for a client.

Certainly in the past the platforms have been difficult, where they have said, "Well, we are not based in the UK, we are based in the US. You have to serve on us in the US…" I can get any order from the UK, and generally judges are very supportive when we need to get that, but I would then have to serve it in the US or other jurisdictions, and certainly outside the EU that can be very difficult. Particularly in the US they have various principles, free speech being just one, where they do not necessarily even want to take notice of a UK order and have it enforced. To do that you would have to go through the state system, et-cetera. Those for me are very practical issues, and you can rack up quite a lot of money before you even have somewhere to serve a letter of complaint on someone.

Baroness Kidron: Can I just say for the record you have to not only have an active parent for that but a rich, active parent, since we are talking about children.

Adam Glass: Absolutely. Absolutely right. Lots of law firms take matters pro bono or reduce fees to try and help but you can easily rack up

thousands of pounds before you even obtain the information by which you can start your claim. That for me is one of the downsides of the civil route, as I say, as against the criminal one, where at least you have the state bearing the costs of the investigation, but you might have a year before you come to trial and the stuff remains on line; you will not get a judge taking it off in a criminal case, and maybe someone goes to prison or is fined, but the stuff can still remain online. It is up to the platforms to take it off.

I would like to see a cheaper, more effective and more expeditious route to obtaining information that can enable lawyers to assist young people, children, and their parents to take speedy action. The cost is a big barrier to that.

The Chairman: Steve, any final words?

Steve Wood: I think just to echo the comments I have already made about there probably being a range of solutions, going from the education and transparency points I made earlier down to the legal points and what we may be able to benefit from if the GDPR comes in and also the mechanisms we can have to enforce, so it will be a range of solutions that help tackle this difficult area.

The other point I had to make in my final comments was similar to Adam's, which is the international dimension to this, which makes it a lot more challenging. This is why it is probably important as well that we are going to have to have a move towards global standards on this, because it will be the way to make it easier to operate for the average citizen in the situations that Adam talked about. At the ICO we have led in the development of a global enforcement network for data protection regulators around the world, which enables us to share information or pass on concerns when a member of the public comes to us in the UK, complaining about a firm which is solely established in the US but perhaps offering services to UK citizens.

One example of that is the case of a company called VTech, a child's toy manufacturer which makes smart tablets and screen-based toys for quite small children. They had a really large data breach, and earlier this year we were able to liaise with the Hong Kong Commissioner at least to try to get some information and answers to be able to feed back to people in the UK and parents who were concerned about this. Ultimately, the solutions have to be global and we need a strategy to really make it work so people do not have to have recourse to a lawyer. It should be possible for a regulator such as the ICO to act on behalf of the public. Even though we cannot take every case forward, we should at least be able to interact in the most serious issues on a global scale.

The Chairman: Thank you both very much indeed. We have had a long afternoon. We are very grateful to you for staying with it. It was all good stuff. Thank you very much indeed for joining us.

Google and Facebook– oral evidence (QQ 108-121)
Transcript to be found under Facebook

Wendy Grossman – written evidence (CHI0046)

About me

1. I am an award-winning freelance journalist who has specialized in the area of the internet and related technology for more than 25 years. In that time, I have written books about the developing internet and been a regular contributor to the *Guardian*, the *Daily Telegraph*, *Scientific American*, *New Scientist*, and *Infosecurity*, among many other leading publications. In 2013, I won the BT Enigma award for lifetime achievement in security journalism. I am also a member of the advisory councils of the Open Rights Group and the Foundation for Information Policy Research, the advisory board of Trust in Digital Life, and the executive board of the Association of British Science Writers.

2. I have been online since 1991, and wrote one of the first two guides on how to use the internet for *Personal Computer World* in 1994 and the earliest articles on encryption policy to appear in British publications. Since 1993, I have called my specialism "the border wars between cyberspace and real life". More accurately, I focus on computers, freedom, and privacy.

The free and open internet

3. In his oral evidence, John Carr talks about the way the internet industry operates: "permissionless innovation", he calls it, and goes on to suggest that, "I think we should try to establish, either through law or culturally, that any and every company has a duty of care to children if it brings out a new product or a new service, just as it does in the physical world." Successive British Prime Ministers have sought to make Britain "the best place in the world for ecommerce". Requiring advance permission for all such experiments, Carr's idea here, would effectively void that long-held policy.

4. While it is reasonable to suggest that companies should not release products that clearly violate established principles and should not act contrary to law or repeat actions that have already been established as harmful or mistaken, it is nearly impossible for anyone inventing and marketing a wholly new technology to predict what that technology's' users will do with it once it's been released. The internet itself is a good example: pioneers such as Vint Cerf (co-author of the protocols on which the internet runs), and Tim Berners-Lee (creator of the World Wide Web) thought with great care about the design of the technologies they were creating, seeking to embed democratic ideals so deeply they could not be controverted. And yet, look at the result: the internet has become, in the words of security expert Bruce Schneier, a "giant surveillance machine"; the World Wide Web has empowered many to publish information but has also created giant players whose control threatens the openness Berners-Lee sought to create to such an extent that Berners-Lee has begun a new project to re-establish it.

5. I think policy makers would struggle to define such a "duty of care" for services and technologies that are still in the research phase. While it would not be unreasonable to apply the concept to technologies whose usage and potential

dangers are well understood, that approach represents little change from the status quo. For example, a "smart" refrigerator that collects and data mines its owner's nutritional habits first must comply with the ordinary laws that regulate the sale of electrical appliances and second must comply with data protection legislation. It would be desirable also to hold the refrigerator's manufacturer liable for violations of known security principles that result in the refrigerator's being hacked, though this particular form of liability has been long resisted by software publishers and is not at present a legal requirement.

Redress

6. A critical issue with respect to blocking and filtering is the problem of overblocking – that is, blocking sites in error. Campaigners in the child safety arena seem to feel that such collateral damage is less important than ensuring that no potentially harmful site is missed. However, filtering systems are often opaque, blunt instruments whose inner workings remain hidden from everyone except those who build them, which are also often non-UK companies. It can be exceedingly difficult for a site owner to find out that their site is blocked, identify the source of the block, find someone who will understand – or even listen to – their complaint, and get the block overturned. The Open Rights Group's Blocked project[197] has found that at least 19% of the top 100,000 sites as determined by Alexa are blocked on at least one network in the UK. Children's interests are particularly vulnerable to blocking systems that implement hidden

7. Filtering has a second problem, less often discussed, although Baroness Kidron touches on it in her oral evidence: filtering does nothing to modify behaviour, and behaviour may be more harmful and troubling than content. As she notes, children are concerned about bullying, both online and offline. Filtering is a shallow fix for the very real problems many children have. Filtering is an attempt to use technology to fix profound social problems. This approach very rarely works.

8. It is essential that filtering systems include provisions for redress for those whose sites have been incorrectly blocked, and to consider whether the extensive filtering already present on the UK's networks has provided the benefits its promoters promised.

Parental responsibility

9. On behalf of the Open Rights Group, I attended two meetings on age verification run by the Digital Policy Alliance (ORG, like other NGOs, could not afford the membership fees to allow further participation).[198] I noted at those meetings a hint that some participants viewed parents who choose not to implement filtering as somehow negligent. It is essential that any moves in this area should recognise that different people have different values and beliefs about educating their children, and there should be no stigma attached to electing a different path than the government of the day would like.

197 http://www.blocked.org.uk
198 My write-up of the first meeting I attended is here: http://www.pelicancrossing.net/netwars/2015/08/running_with_the_devil.html

I0. I believe that the public (both online and offline) behaviour displayed by a minority of adults creates a real difficulty in trying to teach children not to bully, abuse, or personally attack others. No amount of controlling the internet will change the context of the society we live in.

Age verification

11. It is essential that any age verification system that's put in place should be able to verify age as an attribute without accessing or collecting identify information. A shop that sells alcoholic drinks and cigarettes does not need to know your name or address; they merely need to verify that you are the right age. An example of good practice is provided by the US state of California, where medical marijuana is legal provided that you have a government-issued card attesting that you are a patient who requires it. When this law was passed, the US federal government was still opposed to legalisation; to protect its citizens from the possibility of being targeted by federal law enforcement, the state issued photo IDs with no name, address, or other identifying information, and designed a system that when queried using the card's number would respond solely with a "yes" or "no" indicating whether the number was valid.[199] This is the right approach for age verification in order to avoid enabling the many undesirable side effects of creating a database of adults who wish to access material that, if known, they might find embarrassing or fuel for blackmailers.

12. As a final point on this subject, I would like to note that it seems to me wholly inappropriate that a system intended for national scope is being defined by a closed group of industry insiders. Any such system should have input from civil society and others to represent the interests of consumers. This is especially true of the internet, a medium intended to allow individual to be both consumers and publishers. As presently constituted, there is a real risk that the system adopted could be out of the reach of small publishers and site owners, the very people the internet was meant to empower.

Children's rights

13. Children, like everyone else, have fundamental rights: access to information, freedom of expression, privacy. Filtering, blocking, age verification, monitoring, and imposing a duty of care all have consequences for these rights. Contrary to common belief, children are not automatically gifted with a deep understanding of how to make technology do what they want. Some are so gifted; but children are as varied as any other demographic group, and many struggle, particularly those with older devices, limited online access, or limited literacy. These difficulties apply to every age group, and must be taken into consideration when designing systems intended for use across the entire population. It's popular to say that children don't care about privacy, but this is demonstrably not true (see, for example, Danah Boyd's book about teens and social media, *It's Complicated*). Even younger children care greatly about privacy, but their threat model is limited to their parents and teachers. The more control they are placed under, the more children will seek to bypass it; instead, they need support and help in understanding the world they encounter. The loss

199 http://www.cdph.ca.gov/programs/MMP/Pages/MMP%20Top%203%20Questions.aspx

of privacy under monitoring requirements, even with the well-intentioned goal of protecting them, is of particular concern in the case of children, who are still developing their individual relationship with the world and therefore need the freedom to read widely and experiment without fear.

September 2016

Department of Health, Department for Culture, Media and Sport; and Department for Education – oral evidence (QQ 129-137)

Transcript to be found under Department for Culture, Media and Sport

Karl Hopwood, esafety Ltd and Mary McHale – oral evidence (QQ 52-60)

Tuesday 18 October 2016

Watch the meeting
Members present: Lord Best (The Chairman); Baroness Benjamin; Earl of Caithness; Lord Gilbert of Panteg; Baroness Kidron; Baroness McIntosh of Hudnall; Baroness Quin; Lord Sheikh; Lord Sherbourne of Didsbury.

Evidence Session No. 4 Heard in Public Questions 52 - 60

Examination of witnesses

Mary McHale, Teacher, and Karl Hopwood, e-safety consultant, esafety Ltd.

Q94 **The Chairman:** Thank you both very much for coming before the Committee. We are two minutes ahead of time. I am going to ask you, if you would, to tell us a little bit about yourselves. We have your CVs. For the record, and because we are televised—I am not sure how many people watch us—it would be very helpful if you just said a little about your background, where you come from and the particular way in which you are approaching our inquiry on children and the internet. Mary, would you like to go first?

Mary McHale: Thank you. I am Mary McHale. I am the lead tutor of key stage 5 and the e-safety leader at St Peter's Catholic School in Solihull. I have been an integral part of embedding e-safety into our school community. Now, because of the success of e-safety in our school, we are also working with local schools in the community. I have worked towards accreditations, which include ThinkUKnow, the NSPCC's "Keeping Kids Safe Online" and the Ofsted-recommended EPICT accreditation. As part of that now, I have become a facilitator so I can accredit other schools in the locality with EPICT facilitation. We have also been working with the University of Oxford in producing some resources that can go across the UK, and I am delighted to have been invited here today to discuss this matter.

Karl Hopwood: Good afternoon, everybody. I am Karl Hopwood. My background is in education. I was a primary school headteacher for a number of years, but for the last nine, almost 10, I have been working probably 60% of my time in schools with pupils, parents and staff around online safety issues. The other part of my work is for INSAFE, which is the organisation that co-ordinates the Safer Internet Centres around Europe. My role there is primarily working with helplines that just deal with online safety issues. I am very pleased to be here.

The Chairman: Thank you very much. Lord Sherbourne.

Q95 **Lord Sherbourne of Didsbury:** Can I direct a question, first, to Mary

McHale about the work that you have been doing in schools on online safety? So that we are clear, what do you think are the most important aspects of what you are asking schools to do and where is it most successful?

Mary McHale: When I started looking at the e-safety in our school community, the success of what we have done is the cohesion that we have had between the staff, the students and the parents. We have worked cohesively together to ensure that all of us are safeguarding our students because it is an integral part of the safeguarding now in all schools.

We set up an e-safety committee in the first instance. Five members of staff—teachers, IT managers and the headteacher—were involved in that. We also have lots of students involved, so they can communicate with any concerns that are on the ground in the school. We teach the students about their roles and responsibilities in becoming a safe digital citizen. When they come to us with a concern or they recognise that something is going on, we can work together to ensure that we reduce any problems with that.

For many years now we have run a very successful e-safety parents' evening. In fact, we have one on Thursday. This time we have opened our doors to the primary schools in the local areas because some of them are having a little difficulty in trying to attract parents to their e-safety evenings. Because ours is quite successful, we have opened it up to many of them. We have always had a very good turnout, but we hope that this year it will be even more successful. We have an e-safety log in school that we promote to schools, which records any e-safety concerns that go on in our school. We have a look at a solution and we revisit that, because sometimes when we deal with a concern, it might come to a good outcome but it might crop up again four weeks down the line. We can talk about a social media concern where somebody has posted something inappropriate about another student. We would deal with that but we would revisit it. The students know that we are always looking at what goes on and we are revisiting it all the time. We feel that it has been successful.

I am ever so proud of the students in our school because they are really responsible digital citizens. They tell us anything that is going on and we are all trained as staff to recognise any of the associated risks. All the staff have regular training. We have just embraced e-safety in our school. There is a safer internet day in February, when our day becomes a week of events. We make sure that it is embedded throughout the school from year 7 all the way up to year 13. We get all our staff, governors and parents involved in that so that we are taking a cohesive approach.

Lord Sherbourne of Didsbury: As a result of what you call this integrated approach, can you give the Committee one or two practical examples of how the children—the students—have behaved, reacted or done things in a different way, which is obviously a positive outcome of all this work?

Mary McHale: One student recently was online and somebody was trying to get her to send them pictures. She kept asking questions. Our advice to the students is, "If you do not know them, you do not make any connections with them at all. You ignore them or you block them". But all students are inquisitive and so she did pose a couple of questions. She recognised that, even though this person was saying, "I know who you are. I am a friend through a friend", she was able to recognise the risks associated with that. She then told her mum; her mum phoned the school. We could speak to the student about it and she was able to block this person.

When they came and told me this story, we did not have to intervene in any part of that but just make sure that she was happy, safe and there were no emotional aspects of that going on. It was a really proud moment to see that all the work we have been doing in school is having an effect on these students and they are becoming really responsible and recognising the risks, quite clearly. Therefore, that is reducing any further problems down the line.

Lord Sherbourne of Didsbury: So that I am clear, when you say that that work has produced this outcome, what was the school doing so that the girl responded in this way?

Mary McHale: We have been thoroughly educating our students throughout and assuring them that what goes online stays online. It is a meaning that we have throughout the school. Also, it is to ensure that we teach them, as part of our aspects of training them, that, if they do not know this person online and they are being asked to make contact with them, they do not make connections at all and they connect only with people whom they know so that they become safe.

Lord Sherbourne of Didsbury: Mr Hopwood, what do you think are the most successful ways of engaging or undertaking e-safety with children and school students?

Karl Hopwood: In the past, perhaps we have not been using the best messages for online safety in terms of young people. To give you an example, we used to say to children, "Do not talk to strangers online". I completely understand why we used to say that to them, but I am not sure that that message is quite fit for purpose. It is very blunt. If I am in a class of year 5 and year 6 children—so 9 to 11 year-olds—frequently, at least 50% of them will be talking to strangers online every day, normally through the online games that they play.

In the work that I am doing in schools, I say to young people, "If you are having conversations with people you do not know, there are certain warning signs and certain things that might happen that mean you need to go and ask for some help". If the messages are too blunt, and if people are using resources that have been around for an awfully long time that have not been updated, I worry slightly that, perhaps, young people disengage.

The other thing we used to say to people is, "Do not give out any personal information online". We all know that you cannot do anything online without giving out some personal information, so we have to be a bit more nuanced in what we say.

Baroness Quin: I want to follow up on something Mary said. It made it sound as if the teachers are very savvy about what they are doing. Is there a big time commitment given in the school to help teachers themselves to master the awareness and the messages that they want to give to children? Say a new teacher is hired; do they immediately have some kind of induction course into this particular activity?

Mary McHale: They do. We are very good at making sure that our teachers are up to date with what is going on. Through our e-safety committee, we ensure that we are dealing with the apps, the internet sites or the games that are being played in our community. What we train on in our community is not necessarily what would be going on in another community near us—one size does not fit all. Every community has its own problems or issues. You will find that there will be apps or internet sites that are appropriate and will go across all the schools in the UK. However, what we might have been dealing with last term will not be what a school down the road might have been dealing with. We make sure that all the teachers are trained in what is going on.

For example, another thing we do, if we are concerned that something has gone viral quite quickly, is to send out an e-safety alert to our parents on that day to make them aware of it. We will also put some training on for our staff to recognise any signs or to forward any names or anything that they are concerned about. It takes a lot of time. However, digital technology is constantly evolving and it is part of our responsibility to keep up to date with what is going on, because it is an integral part of safeguarding. Therefore, if we are to look after these children, we need to make sure we know what they are accessing online, because, if we do not, we are potentially opening them up to some dangers. We are not saying that everything that comes online has negative effects. However, we need to be very savvy about what is happening and we need to work with the parents to look after these students.

The Chairman: Lord Gilbert, did you want to come in?

Lord Gilbert of Panteg: Thank you. Let me just ask you a little more about working with parents. Your school is, clearly, at the leading edge of protecting children online. You emphasise, however, the importance of an integrated approach and working with parents. How do you reach out to parents who are not participating and who are not coming to your evenings, particularly where you might assess that a child is at risk or at greater risk than other children? Do you have any other way of reaching out to them?

Mary McHale: We do. We send out bespoke emails to them. Last year a group of students were concerned about something, as were we. We invited only those parents to come along. We had a very informal meeting. We do not make it formal. It is just about us working together to ensure that we protect them online. I would not say it is all parents. It is very difficult. However, we have ways of sending out emails if they do not attend, or we can have other meetings at a more convenient time. That is what we have done in the past and it has worked well. I think the parents are really appreciative of the effort that we go to, to make sure

that they are up to date with what is going on in the school community. At the end of the day, it is their children we are looking after. We all want to make sure that they are safe while they are in school and outside school.

Lord Gilbert of Panteg: Do you have any sense of the proportion of parents who are not participating?

Mary McHale: It is difficult to put it as a percentage. When we had a meeting, when some of the parents did not turn up, if it was a few, then we would send an email, we would ask for a meeting, and then, by the time we had taken several approaches, we had pretty much ensured that we had engaged all our parents.

The Chairman: Lord Sheikh, did you want to ask a question?

Lord Sheikh: The point I was going to raise has been asked by Lord Gilbert. I wanted to find out about participation by the parents and whether you get full co-operation from the parents. You have adequately covered that.

The Chairman: Let us go to Baroness Kidron.

Baroness Kidron: I know that both of you are experts in e-safety, but I wanted to broaden it out, because one of the things that we have become quite interested in is the concept of the well-being of children and that not everything that might affect their well-being is necessarily a risk or a harm in itself. I wondered whether both of you, in turn, would talk about some of the other challenges, whether around concentration, critical thinking or anything you can think of, that you see as an issue for young people that might not be expressly a risk or a harm as we think about it.

Karl Hopwood: It is a really important point. When I am in schools and able to have conversations with young people as opposed to standing in front of them and talking at them, I suppose, the number of young people who talk about the pressure that they feel when they are online is really striking. They talk about how much time they spend using their devices. Some of them are using apps now to manage how much time they spend online, which sounds counterintuitive. That is potentially quite helpful. They talk about the effects that they think blue light has, using Apple's night shift mode and so on to limit that.

What worries me the most is what mainly, but not exclusively, girls, say about the pressure that they feel to look a certain way and to behave in a certain way when they go online. We are also starting to see that backed up in the research. The Children's Society produced something at the end of the summer holidays that said that 34% of 10 to 15 year-old girls are unhappy with their appearance, and a lot of that was put down to pressure by social media. That is something that is quietly causing real concerns.

My worry is that they often do not have anybody to talk to about that. Not wanting to go away from the question, you mentioned parents before. Many of the children tell me that they will not tell their parents if something is happening because their parents will overreact, take the device away and then there is a problem. I worry about that.

Mary McHale: I totally agree. There is the ideology now of the selfie, and there are even tips on taking the perfect selfie. When students look at their profile, it is full of selfies of them looking much older than they are. There is a concern with that, too. When they are talking to other people, other people think that these students are much older than they are.

Another aspect is online gaming. We have some students in the local community who play for hours on end every night on these games getting to certain levels, and then when they come into school the next day they are so tired, their heads are down and it affects the teaching and learning. We have to look after the students' emotional and social well-being. For boys, a growing concern is how long they spend on these gaming, whether games they have bought or an online game that they are playing against other people.

Baroness Kidron: I am very interested to know whether you think you have a successful strategy for that in your school, because I know that children being tired out from the night before is a problem in schools.

Mary McHale: Yes. A bit of kinaesthetic learning always helps them in the morning, to be honest with you. A bit of jumping around seems to waken them up, but there is not really a good solution. We just need to work with the parents to make sure that there is an appropriate time or there is a limit when they are off these games. I have to say that it is down to parental responsibility to ensure that they are off games at certain times or that it is not affecting them. As teachers, we would alert any concerns to the parents if they were very tired. As I said, we have the training for the risks associated with that, which we would highlight to parents or to the e-safety committee and speak to the students about that.

Baroness Kidron: That is interesting because that leads to my next question, which is that we often hear in this Committee, "Oh, the schools have to do this; the parents have to do that". We are quite interested to hear from both of you whether you think there is an edge to the school's responsibility. What is it that you think schools can reasonably be asked to do and what responsibilities lie elsewhere, possibly beyond parents, such as government, companies, technology—I do not know—but I would love to hear from you?

Karl Hopwood: Anybody who works with a young person has a responsibility to deal with some aspect of online safety. The school probably does have the edge because most—but not all—children will go to school. Some of the things that the Government have done, particularly *Keeping Children Safe in Education*, which came out last month, are now saying that we must ensure that online safety is being taught. That is a fundamental shift from where we were when schools were just told that they should consider teaching it.

One thing we should do is to get parents to realise that they have some responsibility around that. I agree with Mary about devices. For example, there are many times that I talk to young people who tell me that they sleep with devices in their bedroom and are disturbed by them, and then when you talk to the parents, they say, "Oh, yes, my 10 year-old does

sleep with her phone because she uses it as an alarm clock". You think, "Buy one that you wind up and you cannot play games on it". Sometimes they look at this online safety "stuff" and they see what is in the press, and it is very extreme. Please do not get me wrong. It has happened and it has affected those children, but sometimes it is so extreme that parents think, "That is not really something I need to worry about. That happens to other people". One thing we need to do in schools is get them to realise that it is about them.

Mary has mentioned this already, but every school is different. The children are using different apps, games and so on. A brave school will carry out an anonymous survey of their pupils and then say to the parents, "We have X% of our pupils who are doing X, Y and Z. We think there is a bit of a risk with that. Come in and we can talk about it". But it is a brave school that does that because the parents may then blame the school and suggest that somewhere else would be better.

Mary McHale: I agree with what Karl has said. We have the document *Keeping Children Safe in Education*, and *Working Together to Safeguard Children*, which is an integral part of what we are doing in school. The onus comes down to schools, although I agree, as I said, that it is a cohesive approach that everybody needs to take. Students need to be part of that approach, too. They need to recognise the associated risks, but it is our responsibility as educators to teach them.

It is not going to be a culture that changes overnight. It has to be a drip-drip effect. So from the first e-safety parents' evening that we did—we did not have many, but now we have a lot more, to be honest. That is why we have opened it up to primary schools. It is something that we all have to take part in. It is not just a responsibility for the schools or for the parents. Most of the activity that we deal with in school, and other schools do this, is not what goes on in school but what goes on in the home, and then is brought into school the next day for the teachers to deal with. Then we should also get the parents involved with it. That can be a problem. We all need to take part to ensure that we are all working together for an approach to this.

Baroness Kidron: Finally, I am going to make an assumption that the internet has been remarkable as a methodology of teaching and delivering. Could you say something—you have already mentioned tiredness—about critical thinking, because that is something we do not hear very much about? Do you think that the way young people engage with the internet or digital technology is good or bad for their critical thinking? Do you have a view on that or is that outside your remit?

Karl Hopwood: It should be something that forms part of their personal online safety education. In schools where it is done well, they use that as a teaching opportunity to talk about the content that they find online and to get them to consider what is valid, biased and so on. I worry a little that those are not often the skills that are being taught. Too often the focus is on risk and harm and perhaps not looking at some of those much more important skills, which they will be using for the rest of their lives, to be quite honest, when they are using this sort of communication. There are many opportunities to do that, but my worry

is that a lot of colleagues in schools—not every school, clearly—do not feel that they can deal with this, because young people are talking about things that they are not familiar with or comfortable with; but that critical thinking comes back to basic pedagogy, in my view.

Mary McHale: I agree. There are concerns about critical thinking regarding use of the internet and then how much they critically think it through. It is, again, just a bit of a drip-drip effect; that we make sure we are allowing the students to become good critical thinkers and we give them the tools that they need to ensure that they are doing this successfully.

Baroness McIntosh of Hudnall: I am going back to this issue about the behaviour that children will get involved in, such as gaming, the overuse of certain apps and all the rest of it. I am very intrigued by this e-safety committee idea and about the kind of collaborative approach that you have taken to this. When you get parents and, indeed, teachers, involved in those discussions, do you ask them about their behaviour? Do you ask them whether they are playing games in the middle of the night or are constantly worried about their children? It seems to me that one thing is about the way behaviour is modelled to children, not just about telling them what they must or must not do. How much of that do you build into the way you think about talking to the whole community and not just your students?

Mary McHale: The staff also have their training. They are role models to the students, not just in our community but in all communities. They have to make sure that they are a role model in their behaviour. Within our community I would not have issues about that, but we do remind staff about their responsibilities of being online. Policies are in place. We have just looked at our social media policy and our rights and roles as a teacher using social media. The e-safety committee is successful because it does not put the onus on one person to embed e-safety throughout the school. It involves a lot of people working together to make sure that we are taking a whole-school approach to this situation.

Our staff are role models. There may be some staff who play the games that the students are playing, but the difference is, probably, that they are of a legal age, maybe, and some of the other students who are underage should not be playing these games. I have spoken to many schools where some primary school students are playing games that are for those aged 18 and above, and that seems to be okay. Our e-safety means that we would deal with any issues in that. The staff, from my experience, are very responsible and they are role models to the other students.

The Chairman: In passing, I would like to ask about children and their mobile phones at school. When you are in a classroom, do those little alerts go off? Is this the cut-off point so that at last silence reigns in the classroom?

Mary McHale: In our school, we have a "no mobile phone" policy, so if the teachers see them we confiscate them. We put them into the office until the end of the day; so we do not have any mobile phones in school at all. That also goes for our sixth-formers; we do not allow them to

have them. There is only one communal area where they have phones, because we have given them more responsibility, but if I see them somewhere else I confiscate them. The only digital technology that they have is that owned by the school and, therefore, no teaching or learning is being affected. We have safeguarded everybody.

That does not go on in all schools. There are some schools that issue mobile phones as a teaching resource to their pupils. It just depends, but it does not go on in our community. I have to say that I agree with it. It just takes that onus away and then we cannot see the mobile phones. Any technology that we have is owned by the school and we have made sure that everything is okay.

Karl Hopwood: That situation varies massively. The privilege of my job is that, because I am in a different school every day, you see some schools, as Mary said, where you would not have phones out, but I have also seen it being used effectively, where students can take a photograph of some homework that they need to do and so on. Often, the example set by staff is appalling, to be quite honest. I go into an awful lot of schools and I see staff sitting in sessions that I am delivering with a phone in their hand. I will wander round, and it is Facebook and things like that. Recently, the deputy head said to me, "Can I ask? Did you see any staff with phones?" I said, "Yes, I saw loads of staff with phones", and he said, "Our policy says that they should not have phones out when young people are around". Clearly the policy does not work.

We have talked about the whole-school approach. I think a lot of this stuff needs real, serious discussion. In one school I was at recently, last year they decided to allow students to have phones while they were eating their meal, which I thought was not good. This year they have pulled back from that because they said it really changed the whole atmosphere in the school dining room. It is really great that they were strong enough to say, "We tried this. We got it wrong. It is not for us". Real clarity is important and, again, *Keeping Children Safe in Education* asks for real clarity around a mobile policy for staff and pupils, which is helpful.

The Chairman: Excellent. Lord Gilbert.

Q96 **Lord Gilbert of Panteg:** I want to ask about the technology used in schools to monitor students. We heard last week from someone who represented a company that provides a service that monitors and reports what students are doing on their school networks. Mr Hopwood, what is your general view of such technology, do you use it in your school and is it part of the programme that you have described?

Secondly, it was not clear to us how and whether consent was obtained from children and parents, and what rights children in different age ranges had when they were monitored intrusively by this technology. Do you have any thoughts on that?

Karl Hopwood: There is a place for monitoring. Any young person who is thinking about this will not use the school-filtered monitoring system to get access to what they want to get access to. Having said that, there is a place for it. I have seen it used very effectively where, perhaps, they

have identified that a child has been searching for potentially difficult and challenging content around pro-anorexia, suicide and things like that. Provided that they are logging into the system as individuals, because that is not always what happens, that can be particularly useful.

In terms of the consent, one of the things I always say to parents is that, if we are going to monitor what somebody is accessing, we need to be transparent with them that we are doing that, otherwise it will damage their relationship, they will question the trust and, then, young people are less likely to talk about any problems that they face. There is a place for it, and I know that the guidance now is telling schools that they need to do it. My worry is that some of them I have spoken to this term have spent a lot of money putting in a very expensive system, but I am not sure that it is will provide them with any useful information that will make a difference to young people.

Mary McHale: Ofsted recommends that they have filtering systems in place, and we have that in our school community. I am all for the monitoring of the students. From one example we had—the pro-ana and pro-anorexia sites—some students might be in school and they might be trying to search for this online. Our system will then pick that up and we will be able to intervene straightaway before any issue goes along the line. So we can get parents involved and we can ensure that we look after their social and emotional well-being. We have had a number of alerts that have alerted us to something in the first instance, before it develops into a problem, so that we are being proactive to the situation rather than reactive when a problem evolves.

The parents are aware that we monitor the students and we get them to sign a policy. In their student journals, there is a policy. They sign the policy and so do the students, and that is revisited at the beginning of every academic year. Whether they have been there for one year or for seven, they revisit that, too. Staff are also asked to tick an okay box for the first time that they log on at the beginning of the year because staff systems are also monitored. It is like a whole-school plan that we take part in.

In my opinion, it is incredibly beneficial. I have not come across a situation where I have been alerted to something and had to deal with it where it has been a waste of my time. I have felt that it has been very good and it has alerted us to any issues that are going on. Sometimes, students who know they are being monitored and are struggling with something might start typing something in, so it is a way of them alerting us to them without them having to come to us first. That has also been beneficial too.

We also have an online bullying form about any issues going on in our school community. They do not have to speak to a member of staff. They can just fill in the form online. Then it gets posted to their lead tutor. That includes anything to do with any e-safety concerns inside or outside school.

The filtering system has been running in our school now for a number of years, and I have not had any negative aspects from it. I have always found it to be quite beneficial.

Lord Gilbert of Panteg: Could you give us any sense as to how many reports you would receive most weeks and actions you would take?

Mary McHale: It depends on your level of filtering system. Ours is quite high. We can ensure that key stage 3 would be quite high with the filtering and the alert, and we would tone it down for some of the content for key stage 5. That would be because of their curriculum. They might be looking at content that might alert or cause some concern, but there is not a concern there; it is just to do with part of their curriculum.

The one that comes up most comes under the category of porn. However, it is because we have a high monitoring and filtering system, so if you type in certain words it comes under that category. Obviously, it also helps us with our Prevent duties with radicalisation and is incredibly important in safeguarding our students. At the moment, because of the words and the words termed with it, "porn" would be the highest, and followed by that there would be "bullying incidents"; but, if you filter that down, you will find that a lot of the ones that come under the porn filtering system are because they have been searching for something on homework that would come under that category. It could be something to do with biology or some word that would just fall into that category there. That is why.

At the beginning of the academic year all the students are very busy; they are back in after the summer holidays and they are ready to work. Then, as the year goes on, we tend to have a little more concern over alerts, but we deal with them. In some weeks you could have something, and then some weeks you might not have anything at all.

Lord Gilbert of Panteg: For the sake of clarity, both parents and students proactively consent at the beginning of each year.

Mary McHale: Yes, they do. They sign the policy in the first week and then our tutors check that they have signed that. Also, when we have the e-safety evenings, we put out what we do to ensure that everybody is aware of what monitoring goes on in school.

Baroness Kidron: I am struck by the range of issues that you have to deal with, and at the same time this is all after the event. I am just interested in whether either of you has a feeling that there should be more responsible design in the first place and whether there is something that you would like to say on that.

Karl Hopwood: Definitely, yes. Very often, in my experience in schools, young people are struggling with something that could have been prevented. For example, if social networking sites set their privacy to "Private by default", it would not be hard. Let me give you a quick example. I was in a school earlier this week and two children who were nine years old were using ooVoo, which is a kind of Facetime for up to 12 people. Interestingly, when I spoke to their parents that night, they suggested that they used ooVoo instead of Instagram because they thought that was safer, for some reason, but because they used ooVoo and it was public, some very unpleasant people had been joining their chat and sending them inappropriate things. The parents said, "Shall we stop them using these things?" I said that it is more about the privacy.

But if we could get that done at source, it would make things so much easier.

Mary McHale: We also had the same problem in our school community just last year. I know that neighbouring schools also had problems with that particular app. We tell the students that their geolocations go on every time they have an update on the Apple phone devices, which a lot of students tend to have these days, and that it turns the geotagging or the geolocations back on. Therefore, every time a student takes a picture and posts it, you can actually find out the location of that. We have to keep saying to the students, "You must turn it off all the time". We say that to our parents too.

This is something for the producers of the apps. By default, it should be set to "private". Some of the apps that we have dealt with at school have been very good and worked with the school to ensure that we are taking a responsible approach, but for others you could be waiting for months. Part of the problem when dealing with that situation is that you may alert them to something going on and they are not quick to respond to it, although it is having quite a detrimental effect on students, not just within our locality but I am sure across the whole of the UK. Privacy settings are an important factor of e-safety. With these open forums that are open to the public, you need to make sure that everything is set to "private" on these apps, because that would cut down quite a number of the problems that we seem to have.

Lord Sheikh: Mary, I notice that you are teacher in Solihull, which is a very diverse area. Are there any problems particularly relating to children from the BME communities? Do you find that there are particular issues there and, if so, how do you deal with them?

Mary McHale: That is not within my knowledge at the moment. If I am being honest with you, in Solihull I have not felt that there are many issues surrounding that. I am sorry, but I would not know what more to say about that because I have not dealt much more with it.

The Chairman: Can I just pick up on the monitoring and filtering? You have found advantages in being able to do that in that it has helped the children as you have been alerted to problems in children's lives. My earlier question was about children having their mobile phones with them during school hours, which you do not allow, Mary, in your establishments. That means that you are only picking up the monitoring and filtering activity in relation to the child who goes online using the school's equipment.

Mary McHale: The network.

The Chairman: Did it go through your mind that if there was a more liberal policy in carrying your phone around with you that you would get more information and that the monitoring and filtering that you were finding rather helpful might be more extensive than it is?

Mary McHale: That is an interesting point. The amount of work that that would create would be unmanageable.

The Chairman: You could not cope.

Mary McHale: We have the filtering just on our networking system. We deal with any students or parents who come in who are concerned, but it does not extend to their own personal devices at all. Our sixth-form students are allowed to bring in their own device, so our policy extends over that, but just in the sixth form. That would be just key stage 5.

The Chairman: That is interesting.

Baroness Benjamin: Do you have parents who are monitoring at home who are using the system?

Mary McHale: We do. Parents are sometimes unaware of what their service providers can do. BT and Sky have very good ways in which you can monitor and filter what children can access at home. I have to say that parents are unaware of that. When we come to the e-safety parents' evenings we give them step-by-step plans so that they can put this on to their own systems. It is really beneficial for them at home.

The Chairman: I bet the children curse you for that.

Mary McHale: Yes. The children do not want me to show that to the parents, no.

Karl Hopwood: Can I add something to that, if that is okay? I dagree with what we are saying about filtering and monitoring, but the biggest challenge that parents have is when their children are spending time at somebody else's house and they have not done any of that filtering and monitoring. Yes, we must do it; we really need to do it, especially for younger children as there is some dreadful stuff out there. We also have to make sure that there is a channel of communication and that when—not if, sadly—they see something that has upset them or bothered them, they can come and tell somebody. I worry that too many parents think, "I have some really good filtering on there. That is it. Job done. Tick". It is so much more than that. I am sure you know that already but I just think it is important to say.

Baroness Kidron: I was really interested earlier when you used the phrase "digital citizen". I am curious about this age-group thing, because, with filtering, monitoring and so on, when you get kids who are 16 or 17, the idea of parental control in that sense is inappropriate rather than appropriate. I am interested to know whether you feel that there is anything one can do to enable young people to become digital citizens and not just protected citizens.

Mary McHale: It needs to start early. Lots of students get to secondary school and they have had some brief e-safety training, but it has not been embedded from a young age. My four year-old son could not type in what program he wanted to play on the iPad so he found the microphone button and was able to tell it. From a very young age, they can use devices really well. We need to start from a very young age and work through ensuring that they are e-safe. That means when they come up and we have a look at their filtering that they are responsible digital citizens because they can see the risks and awareness. They can deal with it then and associate any concerns that they would have or go to their parents or teacher and raise a concern about that. I do feel it needs to start from a young age and work its way up.

Q97 **Earl of Caithness:** I want to follow up on the age question, but, first, Karl, is there anything that you have found in your travels in Europe that would be of help to us in the UK, or is Europe pretty homogeneous in its approach to this problem?

Karl Hopwood: That is a very good question. One thing that some colleagues, particularly, perhaps, in the Nordic countries, are very good at is that they are more comfortable in discussing some of those more challenging issues around sexual content—pornography and so on. The other thing that they are particularly good at—we have some good examples of this in the UK—is peer-led education. Sometimes that can be quite risky, especially if you are talking about something like sexting, for example. I always remember a student telling other students that, if you were going to send a sexting image, make sure that your head was not in the picture and then nobody would know that it was you. Staff at the school were horrified, but there was a thought that, if it was going to happen, that might be sensible advice. Certainly, one of the things that they are more comfortable with is giving the mantle to young people, because somebody of my age, clearly, to them is over the hill. What do I know? If you can convince them that you do know something, you are okay, but I think young people understand more of the subtleties of it better than we do.

Earl of Caithness: So there is scope for us to learn from that.

Karl Hopwood: Absolutely.

Q98 **Earl of Caithness:** Going on to age, you have a vast age group of children from 0 to 18 and they are all going to respond at different times. Is there a better way to handle this, and is there any relevance as to whether you are a boy or a girl and whether race or religion comes into it?

Karl Hopwood: If I can jump in quickly, we know a lot more about what affects different groups now. The headline that is often quoted is that girls are twice as likely as boys to be victims of cyberbullying. I think if we know that, we can put some resource in there. It is really important that schools recognise that every year 6 cohort will be different. Quite often I will go into a school and the whole of a year group is using one particular app, which I am not even familiar with, because it happens to be something that is flavour of the month there. This has to be about behaviour for me. There needs to be some sort of progression. It is something that the UK Safer Internet Centre is working on at the moment to try to say to a member of staff who does not know much about this, "We think that, by the age of 11, these are the things, connected with online safety, that young people should know". Full stop, end of story. You make that your own and you make it fit your pupils, but there has to be some sort of benchmark. I still go into schools and talk to colleagues who are so far off the mark in terms of what they think those children need. The age range is huge, but we are seeing children in key stage 1 who are using things like Instagram, often with parental consent. It is very challenging. Knowing your children, but having something to benchmark it against so that children do not get missed, is important.

Earl of Caithness: You think that 11 is a good age to benchmark rather than 13.

Karl Hopwood: Are you talking now about the age of being able to use social networking and things like that? I just used 11 as the split between key stage 2 and key stage 3. I know that with the COPPA legislation in America the age is 13. Is that what you were referring to?

Earl of Caithness: Yes.

Karl Hopwood: I would say no. It will vary, and that should probably be a decision with which parents are involved. At 13, 16, 10 it does not work now. I am sure that, even if the European Parliament gets its way and we go to 16, it will not work either. For me it is about what they are doing on there, and when it goes wrong they can get some support. That is just a personal view.

Mary McHale: I agree. They have recommendations for age, but students use apps such as Instagram or Snapchat at 13. I can tell from working in our locality that there would be students at the age of eight and nine using these. There is no one to say that they need to come off it. The app will not turn round and say, "We cannot have you", because they just change their dates. They are all very savvy about what they need to do to make sure that they are of an age to use that app. When you have age numbers, there is no following through. Who is going to oversee that that is the case? If parents say it is okay for them to use it, that is their decision. The age is a quite difficult situation that we do experience in our school.

I agree with what Karl was saying that by certain ages, with the e-safety learning and the teaching that they should have, benchmarks could be put into place, and that would be very good, so that by a certain age all the students have had e-safety training up to a certain level. As I was saying previously, it should start from a much younger age all the way up. When we come to secondary school, there seems to be a greater emphasis on students being more savvy, more e-safe and protecting themselves online.

Earl of Caithness: Would you categorise those ages a little more clearly for us? How would you want that broken down so that by age six children knew X and by age 11 they knew Y?

Karl Hopwood: That is a piece of work that is being done. I always say to colleagues in school that we talk to children about sex, drugs, alcohol and tobacco before they should be getting anywhere near any of that stuff. If they are using Instagram and social media at the age of eight, although they are not supposed to be, I think we have a duty to give them some support to do that. I am not trying to dodge the question, but it is quite difficult to say. There are things around online reputation, validity and bias that we would want them to know or to have some understanding of—copyright, for example—by the age of 11. We have got that in the computing curriculum already but it just needs a bit of expansion, in my view.

Earl of Caithness: This is the final question from me. Is there sufficient online content addressing the needs and requirements of children, and if there is not in what form should it be?

Mary McHale: There is lots of help and guidance out there, a real plethora of it. What I find of concern at times is that something will be released and there will be some associated dangers with it. There is a growth in these anonymous apps now and students are becoming very good at downloading and using them as they do not believe there are any repercussions because of the word "anonymous" that is associated with it. What happens is that we will react and make sure that we have something in alert, but we should foresee, maybe, some potential problems that could be associated with this before it is released and then we could take a much better approach to it in educating the students.

Karl Hopwood: May I ask what you mean with regard to content to teach them about online safety?

Earl of Caithness: Yes, content specifically for under 18 year-olds.

Karl Hopwood: I, personally, think there is too much. The marketplace is very crowded. It is difficult for schools because some of the content is very good and some of it is very dated, but it is still there. I think there is a role for the Safer Internet Centre in the UK, with some endorsement from government, probably, to say, "This is what we recommend". I think a really good example is the parents' example from Internet Matters, which is a phenomenal site. It has everything there that parents need.

Of course, they go to places like ChildNet, the UK Safer Internet Centre and CEOP, but there are an awful lot more. What I worry about is when you go into a school and they say to you, "We have used the CEOP resources". You say, "How long have you used them for?", and they have used them for the last eight years. Children see it every year; they tick the box and they think it is done. That is not right, in my view.

Mary McHale: I would agree with that. The NSPCC does some very good ones, but there is not enough time and funding in schools to ensure that someone keeps up to date with all that is going on, because it is a minefield. To keep up to date with everything that is going on, you go to the internet and use the resources, and schools will tend to use certain websites that they become familiar with and they are happy using. So it is the same kind of thing. They are not going to extend the plethora of resources that they have a look at, but there is an awful lot out there. You will find that schools will go to surfs and internet sites that they have found to be very good in the past, but there is an issue in trying to keep up with it all the time and with the different resources that are out there. It is very time-consuming.

Q99 **Lord Sheikh:** You are both at the sharp end, and I commend you for the work you undertake. As a parliamentarian, I would like your views on two points. First, do you think that government recognise the importance of digital education? Secondly, is there enough funding from government to enable all schools to provide effective digital education? Is there enough space in the curriculum to cover these issues? What are your

views on this? Let us start with you, Karl.

Karl Hopwood: In answer to the question of whether the Government take it seriously, part of the Government take it seriously. The DfE has been particularly strong in taking a lead, and I know that DCMS has been in managing the UKCCIS process and things like that. I get the feeling that there is not always a joined-up approach in terms of how it comes down into schools.

With regard to funding, as an ex-headteacher, I am always going to say that, yes, we need more funding, but sometimes it is about more subtle things. Now that Ofsted has incorporated references to online safety in their evaluation schedule, that has been phenomenally powerful in getting schools to address it. I am not somebody who thinks that we should just do something because we are going to be inspected on it, but it is a lever and it has made things safer in schools.

There are possibly areas where we could still do more. We have made it statutory, but in a strange way, through *Keeping Children Safe in Education*, as opposed to, perhaps, through the curriculum, it is okay because at least we are getting it there. PSHE is the elephant in the room, I suppose. That is where possibly we need to be looking, because the people who deliver that in schools very often are the people who, probably, have a little more understanding of this. There are so many links. It felt last year as though we got almost there in terms of that, and then it stopped. I hope it might start again. That is perhaps where more could be done.

Mary McHale: I would agree. I think the PSHE is critical in school. We use it to teach students about everything outside of passing an exam. It is a real part of their social and emotional well-being. We talk about e-safety. We put careers in there and their future pathways. There are a number of issues that we would talk about with PSHE. We are all for ensuring that it is embedded through our school.

Lord Sheikh: Changing the subject, you talked about the fact that there was a variation in the practice of whether to allow mobile phones to be used by students. I, personally, feel that mobile phones should be completely banned. I am an employer, for example. I am the chairman of four companies. During work time none of my staff is allowed to use mobile phones, full stop. Do you think that a uniform practice could be adopted? I am certainly not very much in favour of mobile phones being used. Do you have any views on this? Can something be done to make it a uniform practice?

Karl Hopwood: I would say no. Where schools are allowing young people to use devices, when it is managed properly—and it has to be managed properly—it is a really good support for learning. It brings all sorts of benefits. I agree with you that where it is not managed well it causes chaos—it really is a problem—but to have a blanket "This is what is going to happen" would curtail what some schools are able to do and it would damage some of the opportunities.

Mary McHale: I believe that some of the schools have already put a huge amount of funding into issuing mobile devices to their students to use them as a teaching and learning resource. Then to have a blanket no

would have a detrimental effect on that. It works in our community because we do not have mobile phones—they are not allowed—but another school in the locality might not agree with that at all. It has to be bespoke to the individual school to take a decision on that.

Q100 **Baroness Benjamin:** It is so encouraging to hear the work that you are doing through your school, because I was in a school this morning and I was absolutely amazed by how many children admitted that they had phones and computers in their bedrooms and were online after the watershed. You said yourself that educating children about online safety is so essential. You hinted just now that PSHE, which is personal, social and health education, is a great way of getting to the heart of the subject matter, but not all schools have a place in their timetable to do that. We know this. A number of our witnesses have agreed and argued that PSHE should be made a mandatory subject on the curriculum, partly because the teaching of PSHE is a bit patchy across the country. A recent Ofsted report stated it was not good enough.

What do you think? Do think it is essential and important that we have it on the curriculum for all schools? Do you agree? What benefits and effect do you think it will have if that was to happen?

Mary McHale: I agree. It works in our community and in a lot of other schools to whom I have spoken and gone to visit. They have it on their curriculum, too, and it does work. As I said, not everything is about passing an exam; it is not just making sure that the students who are coming out of the schools are highly academic but that we have looked after their pastoral issues and ensured that they are wholesome students, who are academic, pastoral and well-rounded when they leave us and the other schools. It is a really intricate part of it.

Ofsted has mentioned talking about British values, democracy and individual liberty. That fits nicely into PSHE. That is not to say that some of the things that we teach in PSHE are not in other curriculum subjects, but by giving it scope in PSHE it just embeds it fully in the curriculum rather than in just one or two subject areas.

Karl Hopwood: I agree. PSHE is vitally important. It seems the right place for online safety to sit, in my view. I know it is much broader than that, but when we started to do e-safety in schools, it sat in the lap of the IT department—I understand why—but for a lot of people it made them think it is a technical issue rather than a behavioural challenge. It would bring consistency. It would force schools to do something. Again, I am not about beating people over the head with a stick, but if we are mandating them to do something, at least we can then say, "Why have you not done it?" and challenge them. It would be welcome.

Baroness Benjamin: At what age would you start?

Karl Hopwood: I would do it as soon as they come into school, right the way through from four.

Baroness Benjamin: One thing I spoke to the children about is keeping the phones in their bedroom, keeping the computers in the bedroom, but learning to switch off. That is one of the elements that the children have

to know—that they have to be in charge. Do you think teaching PSHE will help them to understand their responsibilities?

Karl Hopwood: When you have a conversation like that with them, they can understand that. Far too often, we just do something to them. Do not get me wrong because there is a place for parents to say, "These are the rules" and so on, but when you explain to children that the reason why you want them to stop using the phone 45 minutes before they go to sleep is because the blue light suppresses the melatonin and all that sort of thing, they can understand that and it is more difficult to argue against. Being open and providing those opportunities for discussion and for them to ask those questions is so powerful.

Baroness Benjamin: Do you think to teach PSHE would be dependent on what kind of children you have in the area? Do you think it should be a mandatory blanket set of rules about what you have to teach, because a lot of teachers are quite scared about what they are going to say and do? How do you think that we could get through this to make schools and teachers feel comfortable about teaching the subject?

Karl Hopwood: I would like to think that what you would do is to provide a framework, but then for the teachers who have the skills to adapt that framework so that you achieve the outcomes but in a way that is meaningful for your young people.

Baroness Benjamin: What happens if you do not have the skills?

Karl Hopwood: I hope that we can give them the skills. I hope that teachers have the basic skills. There is a place for specialist teaching, very definitely, but I often say to teachers, "Just talk to them about what they do online. You do not need to plan that lesson because they will come back to you. You may not have the answers to all the questions but we can find them out together". There is a place where we need to have a little technical knowledge or at least know where to get it, but a lot of it is about facilitating the debate and the discussion. If you have a framework to go alongside you, that helps.

Mary McHale: I also teach PSHE—a lot of staff do—across the school, and the kids absolutely love the lessons. We have a head of department who has produced an immense bank of lessons that are synced towards certain key stages. We look through the lessons. It is a time for discussion, so we all know what we are covering. It is all there for us. When it comes to e-safety elements, she will go to the e-safety committee and we will work on that bank of lessons together to make sure we are delivering the correct ones. When she talks about doing something on first aid—we do some first aid in year 8—she talks to them to make sure that we are delivering. The students thoroughly enjoy it as it takes away the emphasis for an exam subject, and it gives them the scope and development just to be able to talk.

The lessons that we have last an hour, the discussions in the classroom are great and all the students take part in them. Even the quietest ones in an academic lesson love the opportunity to discuss and go through the scenarios that we are talking about. In a lot of the lessons that we deliver, we talk about scenarios and what would they do. As I have said, it comes back to the critical scenario of what would they do. What is the

easiest option? What is the difficult option? What did they decide? I thoroughly love teaching PSHE, and the students do, too, so I am all for making sure that it is embedded in schools.

Baroness Benjamin: So they are empowered by learning.

Mary McHale: They are. It is for them to make decisions and to think through the process and scenarios that they could potentially be in. As Karl was saying, e-safety comes into that—absolutely. It can be embedded in different subjects, so in computer science we talk about e-safety. That is one of the first things we do in year 7 when they come in. It just helps to make sure that we are covering all the aspects, not in just one subject but in several.

The Chairman: We are coming to our last question.

Baroness Kidron: I have a tiny question. On PSHE, on e-safety, so many young people have said to me, "Once a year I get my e-safety and it is always about content and it is always about safety in a very narrow sense", but most of their anxiety is social anxiety and social norms, not having any parental help with social norms around the internet. I am interested to hear from both of you very briefly whether setting e-safety within the PSHE framework would allow it to be a richer diet for young people.

Karl Hopwood: It would be, absolutely, in my view, because, for me, e-safety pervades everything that young people are doing. I mentioned at the beginning that I work with these helplines. We work with some general helplines that cover all issues. They reckon that over 90% of things that young people contact them about have an online element. If we could embed it so that it was not something that you did once a year, it would be much more powerful and much more effective. We are not there yet, but if we could do that it would be great.

Mary McHale: I agree. It has to be something that is embedded throughout lots of subjects and not just visited once a year. There is the Safer Internet Day in February. You will find that all schools will celebrate that, but it should not just be one time in the year. It needs to be throughout the year with several reminders. Schools also need to deal with anything that is going on. We have, as I said, the e-safety alerts for the parents, and then we would deliver an assembly to the students to talk about the concerns about it.

We also celebrate their e-safety successes when they have made the right decisions and right choices. This just empowers them. It is something that needs to be not just in PSHE but embedded throughout, and several times throughout the year. What has worked well in our school is having a committee; the students know who the committee members are and they can come and speak to us, and we would be able to talk through the different scenarios and help them with that situation.

Q101 **Baroness Quin:** I think you have made a very strong case for PSHE. When you were talking about it, you talked also about British values and so on, which seemed more like civic education than PSHE. In taking these subjects together, is there an effort to try to ensure that in the schools you do not duplicate but that you complement the disciplines?

Mary McHale: Because PSHE is such a wide discussion point and there is so much that you can bring into it, that is what makes it so successful in schools. You might talk about British values, e-safety, careers and future pathways. There is scope for you to talk about lots of other things that you might not be able to fit into another academic subject. We are, as teachers, always struggling for time to make sure that we go through so much content because they are going to be examined on it, that it does not give the scope for discussions that we would like to have. Therefore, with PSHE it gives us the scope to sit back and give the students time to talk, to think through things and to talk about the different scenarios. That is what is so beneficial about it, rather than being under pressure that we cannot bring it too much into other lessons because we are going to be examined on the academic part of it at the end of the year or the two years.

Baroness Quin: I want to pick up on something you were saying earlier about training in your own school. I would like to ask both of you whether you feel that there is currently enough training across the board in schools, and, if not, how that should be addressed. Picking up again on the interesting point you made that some of the issues that you are dealing with are almost area-specific, there are issues and apps that are current in your area that may not be used in other schools. If there is a need for more national training, can that training also be designed to be sensitive to the needs of particular schools in particular areas?

Karl Hopwood: One of the challenges is that a lot of local authorities have lost personnel who, perhaps, could have specialised in that. There is some very good practice but there is also some pretty shoddy practice. That is a concern. As an ex-head, you look at all the things that you need to train your staff in, and you have a very limited amount of time to do that; it moves very quickly. There are certain things to do with the behaviours—to do with cyberbullying, for example. We have guidance around cyberbullying that we are waiting to have released at the moment. These are some of the staple things. Then, probably, one or two people in a school need to have some more bespoke training and they become the go-to people, and that can be cascaded and so on. Again, the mandate in *Keeping Children Safe in Education* says that we now need to incorporate online safety for staff and training is really helpful, but it is then where they go to, to get that.

Baroness Quin: Are there some good local authorities—I know their role has been reduced—in this field?

Karl Hopwood: Absolutely. Take Kent, for example, and Rebecca Avery, who is the e-safety officer. There was a time when that post was going to go. She now has somebody else working with her. She is nationally recognised, and the work that they do around policies for schools is second to none. It is really useful. Also, we have the UK Safer Internet Centre. I work alongside them, and they would expect me to say this, but they need to be better at promoting themselves as the people to go to for this sort of content. Perhaps government has a role to endorse a bit more forcefully that there is good stuff here.

Q102 **Baroness McIntosh of Hudnall:** After what Mr Hopwood just said, I

wanted to go back to the question I would have asked a moment ago. In your experience, Mr Hopwood, of not just your own school but many schools, first, can you give us, very briefly, any indication of why there is resistance in certain schools to incorporating all the things that you have put under the broad heading of PSHE but specifically to do with internet-related things? Is there anything general about the kinds of schools that do not want to engage with that? Secondly, since you have now said it, do you think that it would be important to renew the pressure to have PSHE included in the curriculum as a matter of statute?

Karl Hopwood: Yes, very definitely, to the last bit. That is quite easy. As to why there has been resistance, I believe that for something to happen effectively in a school it needs to come from the top. Quite often you have people on the senior leadership team who do not think that this is a huge issue. I had a headteacher recently who said to me, "We do not need to worry too much about this because they are meant to be 13 to use that. they cannot access it in school; it is not my problem", which I found shocking, but that is some of the concern. I also think—we have not touched on this—there is a real naivety with some colleagues about just what young people are having to deal with. If they knew, then perhaps they would think, "Crikey, we do need to step up and do something about this". Part of me understands why they are not aware of what it is.

There is always the pressure. Small schools, lots of different hats, "Where do we find the time to do this?", but for me it is great that it is in *Keeping Children Safe in Education*, because this is about safeguarding young people. Many of them talk to me on a daily basis and tell me what has happened, because I then disappear at the end of the day and I am not seen as a threat in that sense. We have to change those attitudes and opinions because this is about keeping children safe.

The Chairman: Last word, Mary.

Mary McHale: I agree with what Karl was saying. It is difficult regarding time. I remember many years ago when I started this, my headteacher said, "Just have a look over this for me", and I became intrigued by how much the students could access. They were signing up to some of these forums; you would have these alerts coming through and then you would hear the concerns from the students. It was a personal love of what is going on with the digital world and keeping up to date with what has happened that has led to us being so successful, but it has taken a lot of time and commitment. You have to have a real love and passion for it to do this. I believe schools see this as a huge problem, so where do they start? That is why our community is hoping to help the other schools, especially the primary schools, to say, "I know that this is water that is a bit scary to get involved in, in the first instance, but if we help you and we lead together we will make sure that your school is, hopefully, just as e-safe as ours".

You do need more accreditation. Parents always love accreditations for schools, but they are very costly. We are at a level where we could have an accreditation for our school, but it would be an extra £1,500. Everything is so tight. We know that we are doing the work on the

ground and we would love to have accreditations, but the funding is not always there to ensure that we are promoting how e-safe we really are. We know ourselves and our parents know, and we are working with the local community, too. There has to be an approach where lots of schools may be banked together—that might be a solution—where you take a school that is doing well and then you work with other schools in your locality and you help them find their feet regarding e-safety, because it is, as I said, an integral part of the safeguarding policies now in all the schools.

The Chairman: We congratulate you both on doing, obviously, some fantastic work—it is really impressive—and for bringing us the combination of that practical understanding and the policy dimension, which is incredibly helpful to us. If you see a recommendation about PSHE in our final report, you might get some credit for that. Who knows? Thank you both very much indeed for joining us.

Mary McHale: It was lovely. Thank you very much.

Horizon Digital Economy Research, University of Nottingham – written evidence (CHI0032)

Submitted by Dr. Ansgar Koene, Prof. Derek McAuley, and Dr. Elvira Perez Vallejos, Horizon Digital Economy Research Institute, University of Nottingham

1. Horizon[200] is a Research Institute at The University of Nottingham and a Research Hub within the RCUK Digital Economy programme[201]. Horizon brings together researchers from a broad range of disciplines to investigate the opportunities and challenges arising from the increased use of digital technology in our everyday lives. Prof. McAuley is Director of Horizon and was principal investigator on the ESRC funded CaSMa[202] project (Citizen-centric approaches to Social Media analysis) within Horizon to promote ways for individuals to control their data and their desired level of privacy. Dr. Perez and Dr. Koene conducted research as part of the CaSMa project. An important part of this work has included the facilitation of 'youth juries' - workshops with 13-17 year old youths designed to identify experiences, concerns and recommendations about the internet. A pre-print draft of the report summarizing the outcomes of the youth juries process is available from the CaSMa website[203]. This work was done in collaboration with the 5Rights[204] coalition and Prof. Stephen Coleman from the University of Leeds.

Questions

1. ***What risks and benefits does increased internet usage present to children, with particular regard to: … iii. Data security***

2. Data security for children revolves primarily around preventing the undesired dissemination of personal (or otherwise personally valued) data to third-parties by actors with whom the data was voluntarily shared, whether explicitly (e.g. social media platforms), or implicitly (e.g. by search engines or web trackers).

3. A recurring issue that was raised by the children during the youth jury deliberations was the way in which Internet users are invited to consent to having their data stored. As one juror put it: "It's the way it's like marketised; it's so friendly and appealing. It's like, 'Enable cookies'. It's like, you wouldn't reject a cookie because a cookie is … a nice thing to have."[205]

---

200 http://www.horizon.ac.uk
201 https://www.epsrc.ac.uk/links/councils/research-councils-uk-rcuk/digital-economy-research-rcuk/
202 http://casma.wp.horizon.ac.uk
203 Internet on Trial - Youth Juries Report on Internet and digital technologies http://casma.wp.horizon.ac.uk/casma-projects/irights-youth-juries/internet-on-trial-youth-juries-report-on-internet-and-digital-technologies/
204 http://5rightsframework.com/
205 Internet on Trial - Youth Juries Report section 3.1

4. In all of the juries, discussion moved at some point from third-party data collection to the 'terms and conditions' (T&Cs) that people are required to sign up to when entering commercial sites. The general attitude on this topic is clearly expressed in the following quotes by two of the young participants. The first expressing the difficulty of understand the T&Cs "The companies are really smart, because they know most young people don't want to sit there reading, like, paragraphs and paragraphs about it. And even if you did the way it's worded it's complicated so they know people won't understand it". The second highlighting the sense of being manipulated and exploited "And so I think things like that are quite interesting, because it's like, then they, they ... they're backing themselves up and saying, "Well, it was stated in the terms and conditions which you agreed that you'd read," and it's like really they know that, that no one would read it. So I think that's when they can use it against us."[6]

5. It is worth bearing in mind that the problems with the comprehensibility of 'terms and conditions' are an issue that applies equally to adults, as was shown by a previous study from our lab[206].

6. Among the recommendations from the young people for solving these issues were demands for clearer and more accessible presentation including video and audio formats, as well as fines for platforms that do not comply with minimum requirements such as word limits, clarity, or accessibility. Specific recommendations include more transparency regarding third party data-gathering and storage, for example: users should be informed and their explicit consent should be required for their personal data to be used, shared or tracked; the length of time personal data is stored should be limited; there should be an award for best practice in personal data sharing and protection of user's privacy.

7. Youth Juries participants also pointed out that removing personal online content should be easier and suggested a self-tracking tool to gain control over their own content, as well as screenshot blocking tools.

2. Which platforms and sites are most popular among children and how do young people use them? Many of the online services used by children are not specifically designed for children. What problems does this present?

8. The popularity of sites among children can change rapidly when new services are offered. A clear example of this is the PokemonGo app which is currently very popular but could quickly loose popularity once the novelty of the experience wears off and a new competing app is launched. Based on discussions with parents and with the youth jury participants, sites that have managed to maintain popularity for a prolonged period are:

   - Popular sites with young (pre-teen) kids: Swiggle, YouTube, CBeebies

206 Google's terms and conditions are less readable than Beowulf, the Conversation, Oct 17, 2013 https://theconversation.com/googles-terms-and-conditions-are-less-readable-than-beowulf-19215

- Popular sites with young teens: Facebook, SnapChat, Instagram, Whatsapp, Tumblr

Among these, only Swiggle and CBeebies are specifically designed for children.

9. A 2012 report by MinorMonitor[207] surveyed 1000 parents of children under 18 who used Facebook. More than 38% of the children were found to be 12 years or younger and 40 children were reported to be 6 years old or younger.

10. A 2011 study by Dana Boyd and colleagues[208] in the US investigating the efficacy of the Children's Online Privacy Protection Act (COPPA), which regulated the use of commercial Web sites by children under 13, found that 84 percent of parents were aware when their under 13 years old child first created their site account, and 64 percent helped create the account.

11. Exposure of children on and to online platforms and sites commonly start much earlier than their first personal accounts. According to a 2010 study by internet security firm AVG, 92% of children in the United States have an online presence (due to their parents' disclosure) by the time they are two years old.

12. Some service providers, like Microsoft and Apple, have introduced 'family accounts' or 'family sharing' as a way to allow children under 13 to create an account ID that will provide access to approved services and give parents greater abilities to monitor their child's activities online. An example application for this is video chat where the family account can allow the child to call family members but not be exposed to strangers.

13. The most frequently encountered problems that arise from the use of platforms that were not specifically designed for children is inadvertent exposure to material that is targeted at adults, for example through advertising on the site or automatically generated recommendations, such as on YouTube. For example, a 2015 study by A.E. Barry and colleagues[209] revealed that Instagram accounts that were set up with profiles of fictitious users with ages 13 to 19 were able to follow alcohol brands and received an average of 362 advertisements within 30 days.

3. What are the technical challenges for introducing greater control on internet usage by children?

14. One method for providing greater control on internet usage by children is to use filtering software, such as NetNanny, or 'safe' settings such as the 'SafeSearch' setting that is available in most popular web-browsers. Some browsers, like DuckDuckGo have opted to have SafeSearch on as default. Others like Google require users to access a settings menu to turn in on,

207 MinorMonitor infographic http://www.minormonitor.com/infographic/kids-on-facebook/
208 http://webuse.org/pdf/boydHargittaiSchultzPalfreyFM11.pdf
209 http://dx.doi.org/10.1093/alcalc/agv128 cited in http://www.aappublications.org/news/2016/02/04/AlcoholAds012616

with an option to lock the on setting that can only be reached ***by logging in to a google account*** and hence submitting to further tracking. Bing uses a filtering model with three setting where the default 'moderate' setting blocks adult images and video but not text from search results. Various Internet Service Providers (ISPs), also provide filtering services that allow parent to centrally set Child Safe filters that apply to all devices that connect through the home internet connection.

15. Most filtering services rely on either blacklisting or whitelisting of internet content. In the case of Blacklisting all content/pages are accessible except those that have been explicitly listed as unsuitable. In the case of Whitelisting everything that hasn't been listed as suitable is blocked. Both typically rely on humans to view and evaluate the content in order to populate the filtering lists; contracting such work can be costly at large scale.

16. However, even with the most carefully curated Whitelisting based filtering, in-site linked advertising can still cause problems because the advertising content hosted on websites is usually under the control of an ad delivery service, like AdSense, which run real time auctions to determine which advert to show. Various ad delivery services do include customization options that allow the site owners to tune the type of ads they allow on their site, but often these setting are not used or fail to match the age appropriateness of the whitelisted site content.

17. An important factor that needs to be taken into account is that there are discrepancies between PC and mobile platforms. Whitelist tools are often not available for mobile platforms, only for PC. Furthermore, when parents decide to use a Child Safe filter service from their ISP the filter will only apply to the smart phone of the child if it is connecting to internet via the home WiFi, not when the child is connecting via the mobile network. Since the way in which the device is connecting to the internet does not significantly change its user experience, parents might easily not be aware of this distinction.

4. What are the potential future harms and benefits to children from emerging technology, such as AI, Machine Learning and the Internet of Things?

18. The flow of information on social network sites is increasingly mediated by filtering and recommendation algorithms that select and rank the messages and news items presented to users, including children. Although critical in shaping the experience of social media, these algorithms and their effects remain opaque to users. This lack of transparency has the potential to be abused for censorship or manipulation purposes. Without transparency it is very difficult to identify what kind of bias these systems put on the information flows that children are exposed to. Furthermore, the increasingly smooth interfaces and high rates of success in producing satisfying results can lead to an uncritical acceptance of the information that is given.

19. If current trends continue, the Internet of Things is likely to become one of the largest problem areas for cybersecurity and for privacy. Far too often security and privacy concerns are given too low a priority in the design process, resulting in easily hackable IoT devices. Particularly concerning are the examples, including connected baby monitors, voice controlled TVs and toy dolls (e.g. Hello Barbie), that continuously stream very personal video and audio information to data centres, often outside of the jurisdiction of the UK (and EU) data controllers.

Education

5. What roles can schools play in educating and supporting children in relation to the internet? What guidance is provided about the internet to schools and teachers? Is guidance consistently adopted and are there any gaps?

20. Internet advice courses for parents provided by schools or external organisations via the school (e.g., NCPCC or Internet Matters) are reported by parents as very repetitive and lacking in interaction and engagement elements. Funding for quality educational, even online, materials should be a priority building on leading activities such as 5Rightsframework.com.

21. The advice that the schools deliver to parents should be tuned to the age of their children and the changing internet usage patterns for the different age groups. Currently the focus of the guidance is mostly on the risks of internet usage. This needs to be balanced more with guidance about the opportunities that the digital world can offer when services and apps are appropriately configured and used.

6. Who currently informs parents of risks? What is the role for commercial organisations to teach e-safety to parents? How could parents be better informed about risks?

22. Parental guidance comes primarily from schools. Some commercial organizations provide very short bullet lists of safety information, usually in the context of advertising Child Safe 'whitelisting' or 'safe search' services (e.g. BT, Virgin Media).

23. Organizations like Mozilla and Guardian have run campaigns to raise awareness of online safety. These campaigns however were targeted at adults and did not deal with child specific issues. There is a need for better awareness raising/improving internet literacy interventions for both parents and young people. These are contemporary societal issues that could be addressed through well considered plot lines in popular TV drama.

24. Participants of our Youth Juries suggested the creation of peer-group advice services to support both parents and children with practical advice based on personal experiences.

Governance

7. What are the challenges for media companies in providing services that take account of children? How do content providers differentiate their services for children, for example in respect of design?

25. A complicating issue arising is one of definition and appropriate regulation. The recent House of Lords inquiry into Online Platforms[210] and continuing EU activities highlight the complexity of categorization of platforms.

26. For example, social media sites rely on protections afforded to communications service providers and prefer not to moderate content in advance, but rely on take down requests for illegal or inappropriate content. Some do provide the means to label content as "adult", which is a somewhat blunt distinction – in film, TV and computer gaming[211], age labelling and controls are more nuanced and online service providers could quite simply provide similar content labelling schemes – even better if adopted globally as international standards. In combination with aforementioned "family account" mechanisms, these could bring much greater control to families.

8. What voluntary measures have already been put in place by providers of content to protect children? Are these sufficient? If not, what more could be done? Are company guidelines about child safety and rights accessible to parents and other users?

27. Examples of services that provide good information to parents about child safety and access rights include platforms dedicated to promoting wellbeing and mental health among children and young people including Kooth, Elefriends and YoungMinds (e.g., digital resilience section), which is only right given the very sensitive nature of challenges these services deal in.

28. User generated content sites like YouTube could adopt a policy of marking all content by default 'adult only', with users posting content able to suggest a lower age rating for content that is supposed to be child friendly. Other adult users could be requested to confirm or deny whether the rating is appropriate having watched the content – such a "crowdsourcing" mechanism can address the scaling issues of content rating, while having as a backstop the ability to refer the content to the site hosting service – invoking the current process for dealing with inappropriate content. Again a common international framework and ratings scheme broadly adopted would work best.

210 http://www.publications.parliament.uk/pa/ld201516/ldselect/ldeucom/129/12902.htm

211 Pan European Game Inforamtion http://pegi.info

Legislation and Regulation

9. What are the regulatory frameworks in different media? Is current legislation adequate in the area of child protection online? Is the law routinely enforced across different media? What, if any, are the gaps? What impact does the legislation and regulation have on the way children and young people experience and use the internet? Should there by a more consistent approach?

29. Specific consumer protection concerns arise in dealing with unbounded "in-game" purchases. Certainly for children controls need to be in place to prevent excessive charging. Given the child is not the bill payer, it could be viewed as negligence on the part of the service provider to not provide the bill payer with the controls necessary to cap such payments, something the credit card industry could champion backed by the threat to refuse to honour payments.

10. What challenges face the development and application of effective legislation? In particular in relation to the use of national laws in an international/cross-national context and the constantly changing nature and availability of internet sites and digital technologies? To what extent can legislation anticipate and manage future risks?

30. International coordinated regulation is required in order to have impact, and specifically on large US corporations which have emerged within the US's specific regulatory framework. In this regard the EU has been an important player, where the UK will be a minor voice unless it continues to coordinate and support EU action in this area.

11. Does the upcoming GDPR take sufficient account of the needs of children? As the UK leaves the EU, what provisions of the Regulation or other Directives should it seek to retain, or continue to implement, with specific regard to children? Should any other legislation be introduced?

31. Several of the suggestions that were made by our youth participants would fit within a rigorous implementation of the impending EU General Data Protection Regulation by the Information Commissioners, bearing in mind the needs of children.

32. Many commentators assume that the GDPR will in fact come into force given the timeline for the UK departure from the EU. Whether the UK would then decide to replace it would beg the question "what could be achieved by doing that?". As we have seen with the overturn of the US "Safe Harbour" and the immediate challenging of the new "Privacy Shield", any UK regulation would need to provide rights on a par with GDPR to maintain effective trade with the EU in digital services, and enable UK companies to export effectively.

12. What more could be done by the Government? Could there be a more joined-up approach involving the collaboration of the Government with research, civil society and commerce?

33. Civil society needs to be consulted at early stages of any legislative process, including not only child protection but also those concerned with freedom of speech, freedom of access to information and privacy advocacy groups, in order to provide balanced perspective. The approach adopted in the definition of the gov.uk Verify scheme provides a useful template for consideration.

34. The RCUK Digital Economy theme has a programme of research in Trust, Identity, Privacy and Security. The use of extra targeted funding for a managed call specifically aimed at children and internet issues would be a very focussed way to bring together the research, civil society and policy makers across the UK to address these challenges.

26 August 2016

Baroness Howe of Idlicote – written evidence (CHI0017)

0. Introduction

0.1. I have worked on the topic of children's safety online for many years and have brought five Online Safety Bills to the House for the parliamentary sessions, 2010-12, 2012-13, 2013-14, 2014-15 and 2015-16 and amendments to the Children and Families Bill in 2015. My Bills have required the development of tools which protect children from accessing pornographic and other harmful content online, since "*What is clear…is that children's access to pornography is fundamentally different from that of previous generations because of the prevalence of these materials on the internet*."[212] I have not suggested that my Bills are the ultimate 'silver bullet' but a tool for improving child safety on the internet. My submission relates to the content of my Online Safety Bills.

1. What risks and benefits does increased internet usage present to children, with particular regard to: i. Social development and wellbeing ii. Neurological, cognitive and emotional development, iii. Data security

1.1. Since I have been working on this issue, there have been continuing studies that highlight the same messages about the potential harms to children from unsuitable and harmful material, especially from sexually explicit material:

- In 2010, Dr Linda Papadopolous said our young people are being "*exposed to increasing amounts of hyper-sexualised images*" and that "*sexualising children prematurely places them at risk of a variety of harms*";[213]
- Reg Bailey's 2011 study said "*pornography has a negative impact on children and young people*" and advocated establishing age verification processes;[214]
- The Office of the Children's Commissioner reported in 2013 that "*professionals told us troubling stories of the extent to which teenagers and younger children routinely access pornography, including extreme and violent images…too many boys believe that*

212 "Basically... porn is everywhere" A Rapid Evidence Assessment on the Effect that Access and Exposure to Pornography has on Children and Young People. Published by the Children's Commissioner for England, 24 May 2013, page 4, http://www.childrenscommissioner.gov.uk/content/publications/content_667

213 Papadopoulos L, Sexualisation of Young People, Feb 2010, page 6, para 7; page 14 & Recommendation 3

214 Letting Children be Children. Report of an Independent Review of the Commercialisation and Sexualisation of Childhood, Reg Bailey, June 2011, Cm 8078, paras 43, 50 & Recommendation 5

they have an absolute entitlement to sex at any time, in any place, in any way and with whomever they wish…too often girls feel they have no alternative but to submit to boys' demands, regardless of their own wishes."[215]

2. **Which platforms and sites are most popular among children and how do young people use them? Many of the online services used by children are not specifically designed for children. What problems does this present?**

2.1. My focus has been on **ensuring those internet sites that are not suitable for children are not accessed by them regardless of the platform they use**. This is especially challenging for several reasons:

- The fact that media use is an independent activity without parental supervision: "*Increased use of smaller screens is making supervision more difficult, and the proliferation of devices is creating a need for parents to keep up to date with technology... [since] the internet is accessible almost everywhere and on a wide range of devices, so the risks are present constantly rather than just in the home*."[216]
- Technology is moving fast. A 2010 Ofcom Report on children's media usage[217] says nothing about tablets whereas the 2015 update reports that 81% of 5-15 year olds use tablet computers at home.[218] The touchscreen interface means that young children (0-8) are able to access tablets more independently at an earlier age than technologies such as laptops.[219] In 2010, 14% of 12-15 year olds used their mobile phone to access the internet;[220] in 2015, this jumped to 65%.[221] The world of media usage is changing presenting challenges for parents and for governments.

3. **What are the technical challenges for introducing greater controls on internet usage by children?**

---

215 "Basically... porn is everywhere", *Op Cit,* page 4

216 Ofcom report on internet safety measures, Strategies of parental protection for children online, Dec 2015, paras 2.22 and 2.23, http://stakeholders.ofcom.org.uk/internet/internet-safety-dec-2015

217 UK Children's Media Literacy, March 2010, http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/ukchildrensml1.pdf

218 Children and Parents: Media Use and Attitudes Report 2015, Ofcom, November 2015, page 31 http://stakeholders.ofcom.org.uk/market-data-research/other/research-publications/childrens/children-parents-nov-15/

219 Livingstone et al (2014) Young children (0-8) and digital technology: a qualitative exploratory study - national report - UK. Joint Research Centre, European Commission, Luxembourg. http://eprints.lse.ac.uk/60799/ - information taken from Executive Summary, pages 3-4

220 UK Children's Media Literacy, *Op Cit*, page 9

221 Children and Parents: Media Use and Attitudes Report 2015, *Op Cit,* page 24

3.1. My last three Bills have required age verification for video on demand and/or pornographic websites. I have not set out any views on how the age verification process should be conducted, but I am watching with interest the development of the British Standards Institution Publicly Available Specification 1296, (see http://agecheckstandard.com/).

4. What are the potential future harms and benefits to children from emerging technology, such as Artificial Intelligence, Machine Learning and the Internet of Things?

4.1. No response

5. What roles can schools play in educating and supporting children in relation to the internet? What guidance is provided about the internet to schools and teachers? Is guidance consistently adopted and are there any gaps?

5.1. No response.

6. Who currently informs parents of risks? What is the role for commercial organisations to teach e-safety to parents? How could parents be better informed about risks?

6.1. This is a tech-savvy generation and parents are often much further behind than their children. For instance, in 2015, 83% of parents of 5-15 year olds with home broadband were aware of eight technical tools that protect children online and more than half (57%) of parents used them.[222] This sounds positive; however, around one in five parents who used tools felt their child was able to bypass them; 26% of parents said they thought their child could bypass ISP content filters.[223] A third of parents are not aware that they can apply parental controls to YouTube, despite this being one of the most popular sites for children and young people.[224]

6.2. This evidence has made the **provision of information and support for parents a key focus of my Online Safety Bills**. While there are the websites https://www.thinkuknow.co.uk/ and http://parentinfo.org/ run by the Child Exploitation and Online Protection Centre, as parents regularly deal with ISPs and mobile phone operators, I am of the firm opinion that these commercial organisations have an on-going role in promoting e-safety especially as the needs of parents change with their

222 *Ibid*, page 160
223 *Ibid*, page 166. Note that this increased to 29% for the 8-15s, see page 29
224 Pace of Change Report, Research focused on how parents and children differ in their use of the internet, Internet Matters, December 2015, page 39 https://www.internetmatters.org/wp-content/uploads/2015/12/Internet_Matters_Pace_of_Change_report-final_2.pdf

children's ages and as new websites and apps come to their child's attention. The website https://www.internetmatters.org/ is supported by the industry and welcome. My current Bill[225] requires these providers to ensure that there is "prominent, easily accessible and clear information" about online safety at the time the service is purchased and for the duration of the service (clause 4). As well as the websites, I suggest that **literature should be given to parents when they purchase mobile phones for their children**.

6.3. I have also proposed in clause 6 that there should be a duty on the Government to educate parents about the use of family friendly filtering, online safety tools and how to protect their children from risky behaviour online (eg bullying and sexual grooming). **This could lead to leaflets being available in places parents regularly go, such as schools, libraries, doctors' surgeries etc**.

7. What are the challenges for media companies in providing services that take account of children? How do content providers differentiate their services for children, for example in respect of design?

7.1. The challenge is to act in a socially responsible manner in the provision of online content. Sellers of alcohol and gambling online already take action to prevent children accessing their products. Actions by these industries should provide sufficient precedents to ensure rigorous age verification procedures are available for media too.

8. What voluntary measures have already been put in place by providers of content to protect children? Are these sufficient? If not, what more could be done? Are company guidelines about child safety and rights accessible to parents and other users?

8.1. One of the key focuses of my Bills has been to ensure that **parents have the tools they need to decide how to manage their child's internet access** through family friendly filtering options being available on all internet service providers (ISPs) and mobile phone operators. Mobile phone operators currently operate on the basis of a voluntary code.[226] The big four ISPs (BT, TalkTalk, Sky and Virgin) also provide filtering options on a voluntary basis, described by the Minister as "*a vital tool for parents".*[227] Filtering became available to new customers at the end December 2013 and to all existing customers by December 2014.[228] The ISP Code requires customers to make an "active choice"

225 http://services.parliament.uk/bills/2016-17/onlinesafety.html
226 http://www.mobilebroadbandgroup.com/documents/UKCodeofpractice_mobile_010713.pdf
227 House of Lords, Hansard, 5 November 2015, col 1799, https://hansard.parliament.uk/lords/2015-11-05/debates/15110533000335/Pornography
228 Ofcom report on internet safety measures, *Op Cit*, pages 2-3

as to whether they choose to use filters or not.

8.2. There has been a very variable take-up of family friendly filters between the ISPs.[229] The 2015 Ofcom Report reported that 57% of parents of 5-15s were aware of content filters provided by ISPs but only 26% used them.[230] Most interestingly, Sky is now making filters 'default on' which is included in my current Bill (clause 1) so that filtering is a given unless customers opt out/change the levels of filtering. [231] **Sky has seen significantly more customers using filters under default-on than other ISPs**.[232]

8.3. My Bill would **put the requirement for family friendly filters on a statutory basis rather than a voluntary basis**, which would address the current weaknesses:

- that approximately 12% of the broadband internet market is not covered by the voluntary agreement.[233] Many thousands of children are left outside the scope of the agreement. Their rights to a chance of protection are just as important as those living in households served by the big four ISPs (see clause 1);
- the ISP voluntary agreement also comes without a credible and robust age verification policy after the initial choice (addressed by clause (2)(1). A common sense understanding of age verification is that it should happen *before* the activity requiring the verification is permitted. The only current safeguard for family friendly filters is that if someone disables filters and opts-in to adult content, an email will be sent to the account holder informing them of this fact. This so-called 'closed loop' arrangement is completely unacceptable because even if the account holder read the email on the day it is sent, some hours will almost certainly elapse before they become aware and take action during which their children could be exposed to completely inappropriate material. What is more concerning, though, is that polling demonstrates some people will take a number of days to read an email from their ISP and a significant number will never get round to opening it;[234]

229 *Ibid*, page 6
230 Children and Parents: Media Use and Attitudes Report 2015, *Op Cit,* page 161
231 https://corporate.sky.com/media-centre/news-page/2015/sky-to-automatically-turn-on-parental-controls-for-all-new-broadband-customers
232 Ofcom report on internet safety measures, *Op Cit*, pages 22, 23, 25 and 26
233 Smaller ISPs and EE currently hold 12% of the market (end of 2015), See Ofcom, Facts and figures http://media.ofcom.org.uk/facts/
234 See Second Reading Speech for Online Safety Bill, 17 July 2015, col 839. In response to an email from their ISP, 11% said that they would probably leave the email unread for up to a week, 9% would be likely to leave it for more than a week, 14% said that they were unlikely to read any email from their ISP at all. https://hansard.parliament.uk/lords/2015-07-17/debates/15071758000278/OnlineSafetyBill(HL)

- the current self-regulatory approach leaves deciding what is, and what is not 'adult content' to big business rather than to a publicly appointed and accountable body. There should be a public debate about what material is blocked. While the technology is improving all the time, it is not 100% perfect, so it is important to provide a mechanism for processing concerns about content which is being 'over-blocked', one in which the public can have full confidence. These challenges are addressed through my Bill and the role it gives to OFCOM (clause 2), which includes the need to consult on the codes used for filtering and age verification;
- **the legality of even the current arrangements are in question due to the EU plans on net neutrality which come into effect in December 2016**. The Government has committed to maintaining the current arrangements but how this is to be done before the end of the year is not clear; and even less clear since the EU Referendum result.[235]

9. What are the regulatory frameworks in different media? Is current legislation adequate in the area of child protection online? Is the law routinely enforced across different media? What, if any, are the gaps? What impact does the legislation and regulation have on the way children and young people experience and use the internet? Should there be a more consistent approach?

9.1. I have argued on numerous occasions that there should be a consistent approach between the regulation of offline and online media. If it is deemed by the British Board of Classification (BBFC) inappropriate for children to see '18' rated material offline, it would logically follow that it should also be deemed inappropriate for children to view such content online.

9.2. I am disappointed that the Government introduced a civil offence to manage online pornography in the Digital Economy Bill (DEB) rather than maintain the use of criminal offences. I would also prefer to see the requirement for age verification extend to all 'adult-only content' material that is "*offensive and harmful material from which persons under the age of 18 are protected*" (see clause 7 of my Bill). I note that the Minister for Online Safety said age verification should apply "*to all harmful content, not just to pornographic material*" last year.[236]

9.3. My Bill seeks to address **the need for consistency across media forms by**:

---

235 Minister for Online Safety, Second Reading, Online Safety Bill, July 2015, *Op Cit,* col 860 and House of Lords, Hansard, 5 November 2015, col 1799, *Op Cit*

236 Minister for Online Safety, July 2015, *Op Cit,* col 861

- ensuring that an age verification policy is put in statute for video on demand for all 18 (not just pornographic material) and R18 material; and
- introducing a licensing arrangement for pornographic websites similar to that for gambling websites, with criminal penalties for operating without a licence and the ability to block financial transactions if needed.

10. What challenges face the development and application of effective legislation? In particular in relation to the use of national laws in an international/cross-national context and the constantly changing nature and availability of internet sites and digital technologies? To what extent can legislation anticipate and manage future risks?

10.1. In my last two Bills I have included measures which have sought to extend regulation of pornographic websites based outside of the UK – in particular **the need to have robust age verification**. For this reason I strongly support the principles of the proposal in the Digital Economy Bill that will require age verification processes for all online commercial pornographic content accessed in the UK regardless of where in the world the website originates.

10.2. However, I have concerns about the proposal that any regulation should be "proportionate" as this implies that in practice the requirement will *not* apply to all commercial providers and children and young people could simply find smaller sites with little to no age verification mechanisms as a means of viewing adult content. This arrangement would undermine the protection of children and call into question the Government's age verification proposals.

10.3. My last two Bills have introduced a statutory power to allow financial transaction blocking (FTB) as a means of enforcing the requirements for compliance in cases of overseas websites. I proposed a similar power in the Gambling (Licensing and Advertising) Bill to ensure enforcement of unlicensed overseas websites, because I disagreed with the Government's assessment that voluntary arrangements were satisfactory. Despite the Government's rejection of a statutory FTB power to protect UK consumers from unlicensed gambling providers, it has adopted a halfway house measure in the Digital Economy Bill giving the regulator a power to inform financial transaction providers and ancillary services that a website or app is out of compliance with the age verification requirement. However, it is not clear whether the Government's intention is for the requirements on financial transaction providers to be voluntary or mandatory – there is no explicit power in the Bill to require a transaction be blocked or a service removed.

10.4. If we are serious about protecting UK children from commercial pornographic websites, we need to put in place a serious mechanism to generate a sufficient incentive for them to act in the best interests of our young people and cut off sites without age verification from a UK income stream. **The enforcement mechanisms should include mandatory financial transaction blocking and the power to require IP blocking** (blocking of individual websites) as happens with copyright infringement.[237] Without these it is not clear that the Bill will be successfully enforced, nor does it demonstrate that the Government's stated "*commitment [that] we are determined to hold the adult industry to account for its business practices which, inadvertently or not, cause distress and harm to children*."[238]

11. Does the upcoming General Data Protection Regulation take sufficient account of the needs of children? As the UK leaves the EU, what provisions of the Regulation or other Directives should it seek to retain, or continue to implement, with specific regard to children? Should any other legislation should be introduced?

11.1. Since the internet has a clear cross-border reach it will be important to ensure there are mechanisms in place to facilitate the necessary international co-operation to protect children (eg information sharing) and for the UK to continue its leading role in online safety. This should be a key consideration when establishing future relationships with the EU and its Member States. However, since the internet is a global phenomenon this need for international co-operation goes beyond the borders of the EU. There will also be a need to address funding for organisations that currently rely on EU support to provide projects for children's online safety.[239]

12. What more could be done by the Government? Could there be a more joined-up approach involving the collaboration of the Government with research, civil society and commerce?

12.1. The Government already has a track record of working with industry and especially through UKCCIS (the UK Council for Child Internet Safety) which includes various working groups.[240] The Government stated in their Consultation on Age Verification in February that they were going to *"launch a campaign to raise awareness of online safety issues"* and to work on "*what further progress can be achieved through*

237 Clause 97A, Copyright Designs and Patents Act 1988
238 Minister for Online Safety, Second Reading, Online Safety Bill, July 2015, *Op Cit,* col 859
239 See Minutes UKCCIS, June 2016, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/541728/UKCCISEB_MeetingMinutes_280616_Final__1_.pdf
240 https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis

the use of parental control filters."[241] I hope that both initiatives will be launched shortly and be supported through UKCCIS.

24 August 2016

241 Child Safety Online: Age Verification for Pornography, Department for Culture, Media & Sport, February 2016, pages 5 and 15 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/541366/AV_ConsultationDCMS_20160216_Final__4_.pdf

Information Commissioner's Office (ICO) – written evidence (CHI0049)

Inquiry: Children and the internet

About the ICO

The ICO's mission is to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

The ICO is the UK's independent public authority set up to uphold information rights. The Information Commissioner does this by promoting good practice, ruling on complaints providing information to individuals and organisations and taking appropriate action where the law is broken.

The ICO enforces and oversees the Freedom of Information Act, the Environmental Information Regulations, the Data Protection Act and the Privacy and Electronic Communication Regulations.

Introduction

Thank you for the opportunity to take part in this important consultation. We agree that the protection of personal data can pose a problem for children using the internet, in that there is a risk that their data may be collected or shared without them being aware of this. We also share your concern that the online activity of children may remain visible to future employers or academic institutions.

In answering your specific questions we have confined ourselves to discussing matters that fall within our area of statutory responsibility, primarily as regulator for data protection law in the UK. These important challenges will not be addressed by the law alone, a broader strategy including the law, digital citizenship and education is required.

Specific questions

Risks and benefits

What risks and benefits does increased internet usage present to children with regard to data security?

The Data Protection Act 1998 (the DPA) requires organisations offering online services to children – and to other individuals - to put appropriate security measures in place. The law does not contain specific provisions relating to the security of children's data – security must be appropriate across all systems including front line and back office, online and offline, regardless of the age of the data subject. A system that keeps an adult's personal data appropriately secure, would also keep a child's personal data appropriately secure. The real

difference lies in a child's ability and experience of identifying or recognising the systems of a poor performing or non-compliant data controller, prior to taking a decision to provide his or her personal data to a particular website. They may also be unduly incentivised or subjected to peer pressure to use a particular service, and may be more likely to spend more time online and therefore generate greater volumes of data to be stored and further processed "in the cloud".

Whilst there is no specific provision in the DPA specifying a higher standard of data security for a child's personal data in determining what is "appropriate" the ICO would expect a data controller to take into account the obligations associated with processing of a child's data imposed by society and thus should have a high level of security and privacy by default.

There is also a broader issue of the fate of personal data once a child has published it, for example on a social networking site. Although the rules of data protection may still apply to the further collection, use etc. of the data, in reality there may be little that can be done to prevent unscrupulous third parties from harvesting a child's data and using it for inappropriate purposes. The ICO is active in detecting and pursuing list-brokers and others who may engage in this sort of practice. However, our message to children, and their parents or guardians, is that once a child's personal data has posted – particularly publicly - it may be highly challenging to control what happens to it subsequently. The best protection for children is for their 'risky' personal data not to be put into the public domain in the first place. Therefore education also has a key role to play.

Risks are also present when data is intended to be shared privately, e.g. within a closed group or on a one-to-one basis, and where security settings are insufficient to prevent the wider sharing of material which was meant to remain private.

Many of the online services used by children are not specifically designed for children. What problems does this present?

This question touches on a major area of difficulty for the regulation of children's personal data online. A good example of the issue is contained in the General Data Protection Regulation (GDPR). The GDPR contains several provisions aimed at the protection of children's data. Essentially the GDPR seeks to introduce an age-based approach to protection, meaning that a child cannot consent to use an 'information age service' offered directly to him or her; there must be consent from the holder of parental responsibility.

Although the wording is not entirely clear, we take this provision as applying to commercial internet services specifically targeted at children. If such an approach is adopted in UK law, we think it could be difficult to apply in practice. There are services that are obviously aimed at children (e.g. Club Penguin or CBBC) and ones aimed at adults (gambling sites). However, in the middle of the spectrum there is a wide range of services – for example social networking, online video, marketplace and gaming sites - which are essentially age-neutral and are used by both children and adults. This leads us to be sceptical about

seeing an approach that seeks to differentiate between children's and adults' sites as being in itself a solution to the problem of children's online protection.

Instead we would prefer a more flexible approach, meaning for example that social networking sites should explain their data collection practices in language that all users of their services are likely to understand and to invest in a high standard of security for all users. This should also include privacy settings by default (e.g. publication of data). Of course, where it is clear that a service is aimed at children then the way the service is offered and the way it is explained must be age-appropriate. A young child, for example, would be unlikely to understand the implications of their details being passed on to a third party data brokerage – however clearly that is explained. In our view services that are clearly aimed at children should not engage in data sharing of this sort, no matter how simply the relevant choices are explained. (Of course the inappropriate harvesting and use of children's data can lead to inappropriate contact with children, for example the sending of PII or vehicle accident lead generation messages.)

We advocate a risk-based approach to ensure that the potential privacy intrusion of different data collection and usage scenarios is assessed. Organisations are encouraged to use Privacy Impact Assessments (PIAs) to assess potential harms and solutions to mitigate. This should enable privacy protections to be considered when a service is being designed – an approach known as privacy by design. The ICO has developed a Code of Practice for Privacy Impact Assessments. Organisations processing significant amounts of personal data related to children should be regularly using PIAs. A requirement to conduct Data Protection Impact Assessments is part of the new GDPR.

Alongside the obligations organisations have to process personal data in accordance with Data Protection laws it is also very important to focus on education. This should include the creation of safe spaces for children to explore and develop online. Of course parents and guardians should play a role in the protection of children's data in contexts such as this.

What are the technical challenges for introducing greater controls on internet usage by children?

There are a number of challenges in this area including identification and authentication, but also ensuring that any controls that are considered necessary and proportionate are effective in delivering the benefits that they promise.

For example, introducing web-filtering software, either in the home router or within the Communications Service Provider's network can help with the creation of a safer online experience for children. However its effect may be weaker than billed because but it may fail to deal with the multitude of different ways that a child can access the internet (i.e. home, school and public Wi-Fi as well as personal mobile phones). Children can also have an extensive peer group and quickly share tips and techniques on how to circumvent such controls. This can result in a false sense of security for the parent or guardian.

Another problem surrounds age-verification which is often used by a data controller to prevent access to a group of individuals below a specific age. An age-verification system is possible – for example based on the provision of an individual's credit card or other 'adult' details but authentication is a complex problem for all online services without also processing excessive or disproportionate amounts of personal data. Simple age verification systems can suffer from similar problems as web-filtering software in that they can create a false sense of security for data controllers and parents alike. Basic systems requiring the user to input a date of birth can be easily circumvented. More advanced systems requiring a valid credit card (by definition only issued to over 18's) can also be obtained by a resourceful child.

From a privacy point of view, we are concerned that introducing an age-verification system could lead to service providers collecting 'hard' personal identifiers about all internet users, not just the children which they are attempting to prevent access certain services which they would not otherwise collect. Many services are accessed through the use of relatively low-risk identifiers – aliases for example – and service providers may only collect relatively low-risk identifiers such as users' IP addresses. The implications of moving more widely to an age-verification system based on the collection of names, addresses, credit card details and so forth need careful consideration.

Federated ID management should be considered a privacy friendly solution, for example the UK Government's Verify system. When you use this system to access a government service, you choose from a list of companies certified to verify your identity. Information is not stored centrally, and this reduces the amount of information shared. The company you choose doesn't know which service you're trying to access, and the government department doesn't know which company you choose.

Despite the above, we can see some advantages of imposing an age-limit for accessing certain online services. At least the approach would be simple – people under a certain age would not be able to use social networking sites without parental consent, for example. This would mirror the way the sale of age-restricted goods such as alcohol or cigarettes is regulated – where the mental competence of the prospective purchaser is not an issue. However, on balance we favour an approach where even quite young children can access appropriate online services without the consent of a parent or guardian, provided organisations have taken other safeguards. In our view a child should be able to take part in an online activity that presents little or no privacy risk and is of such a nature that the child in question is capable of understanding the implications for him or her. A good example might be accessing a pop-star's website and subscribing to a newsletter. (Of course children must be able to access confidential counselling services such as Childline without parental involvement.)

What are the potential future harms and benefits to children from emerging technology, such as Artificial Intelligence, Machine Learning and the Internet of Things?

The issues for children are much the same as those for adults, although as previously stated children may be likely to adopt online services earlier or spend

longer periods of time using them. In short, we believe that more information about individuals is being collected. It is being shared more widely and is being analysed in more sophisticated ways. We do not necessarily see this as a negative phenomenon, provided that individuals are given an appropriate degree of transparency, choice and control at appropriate points in their online activity. However, providing this to children can be difficult or impossible, and of course it may be impossible to differentiate between an adult or a child user. As with our example of list brokerage above, we doubt whether a child – particularly a young one – could understand the implications of using an internet-connected smart device such as a TV or a fridge. This does not mean that children should be prevented from using such devices. It does mean though that there needs to be a suitable supervision, education or configuration by a parent or guardian and that when making privacy choices – for example whether to enable a particular connectivity feature of a device – the responsible adult takes the privacy implications (if any) for his or her children into account.

Education

What roles can schools play in educating and supporting children in relation to the internet? What guidance is provided about the internet to schools and teachers? Is guidance consistently adopted and are there any gaps?

The ICO has championed the raising of information rights awareness in our schools. We believe that it is important that children understand their online 'information safety' early on in their lives, given their early exposure to the internet.

This link: https://ico.org.uk/for-organisations/education/ leads to content aimed specifically at teachers and children. It includes an information rights video for schools and a series of lesson plans intended to help children understand the value and importance of their personal information, how to look after it, and the obligations organisations have. There is also a dedicated part of our website aimed at schools, universities and colleges.

We believe that the ICO's activity in this area will contribute to information rights becoming a mainstream part of every child's education. However, as we have seen in other areas such as sex and drugs education, we should not assume that all teachers are experts in this area. They may need ongoing support, and the training materials needed to provide effective e-safety to children. (Parents may also need similar support.)

Who currently informs parents of risks? What is the role for commercial organisations to teach e-safety to parents? How could parents be better informed about risks?

In data protection terms, all organisations collecting children's personal data have a legal duty to ensure the data are processed in a way that is 'fair'. In our view, this can extend to organisations having to ensure that parents and guardians are aware of the risks and implications of data about children being

collected – for example whether it will be made publicly available or whether it will be used for marketing purposes. This can be achieved through a combination of techniques for conveying privacy information, depending on the medium and the general circumstances.
The duties under the DPA are somewhat different to a duty to teach e-safety to parents. However, the DPA's transparency and fairness requirements can contribute to parents' education. As a general policy approach, the ICO has always championed the provision of clear, plain English, genuinely informative information to parents, children and other service users. Making sure that organisations adopt this approach will contribute to a better understanding of e-risk on the parts of adults and children.

We note that some commercial organisations are providing a degree of transparency and control, for example through 'dashboard' type mechanisms which may exceed the requirements of data protection law. We are keen to encourage the development of techniques such as this. To that end, we are in the process of revising our Privacy Notices Code of Practice, to give more prominence to these state-of-the-art transparency and control mechanisms.

Governance

What are the challenges for media companies in providing services that take account of children? How do content providers differentiate their services for children, for example in respect of design?

As we have explained above, providing transparency and consent mechanisms to children presents particular challenges, not least in the determination of whether a particular user is a child or not. However, generally simpler language and perhaps a more visual way of explaining information choices might help to protect and empower children. Again, our revised Privacy Notices Code of Practice very much promotes this approach. More specifically, when a child is offered an information choice – for example whether his or her data can be made available publicly or only within a limited group, then the choice mechanism should be both prominent and easy to understand. In addition, there should be a clear positive action by the child indicating that he or she has agreed to a particular proposition; in this context consent should not be inferred from inaction.

Legislation and Regulation

What are the regulatory frameworks in different media? Is current legislation adequate in the area of child protection online? Is the law routinely enforced across different media? What, if any, are the gaps? What impact does the legislation and regulation have on the way children and young people experience and use the internet? Should there be a more consistent approach?

We see one of the strengths of data protection law as being that it has a basic set of rights and principles that apply equally to all individuals, to all the situations where personal data are processed, regardless of the media used. We

believe that the current law provides us with the powers needed to carry out effective enforcement and to promote good practice in relation to children's personal data.

One problem area concerns the DPA's personal, family and household exemption. This largely dis-applies the DPA in respect, for example, of information someone posts online for personal reasons. The ICO frequently receives complaints about matters such as false and derogatory social-media pages being set up, or hurtful or threatening posts appearing on chat sites. These are often the result of some form of personal animosity. The data processing by the individuals involved will often fall within the terms of the DPA's 'personal processing' exemption so – in reality – there is often little the ICO can do to regulate this part of the internet in terms of the people who post the information. Criminal sanctions and a role for the Police will always be needed for the most serious cases. The ICO is not saying that there is a complete lack of regulation in this area or that it wants to become responsible for policing the content of social media and similar sites or to become the arbiter of personal disputes. However, we invite the Committee to consider this issue carefully, perhaps service providers should be encouraged – or required - to do more to clean-up problematic content from their networks. Most large social media companies do have some form of 'take down service' where individuals can comply but the volumes they have to handle are high and freedom of expression issues can be challenging to adjudicate on in some cases. We stress the need to work with other regulators and educators to provide a form of protection to children that is as comprehensive as possible.

It is important to consider the legal responsibility of publisher organisations that merely host content that others post or provide links to other publishers (i.e. a search engine), with no form of editorial control or moderation. Technically, if they process – i.e. host – personal data that are inaccurate, for example, then they will breach the DPA unless they have taken reasonable steps to ensure the accuracy of the data. However, how realistic is this for a social networking site that may host hundreds of millions of posts or even more? We believe that the responsibility of publisher organisations in this area needs further exploration, in terms of determining the most effective remedies for children who have been the victims of information posted about them by another private individual. Our experience of dealing with search engine 'right to be forgotten' delisting cases suggests that the taking-down of problematic search results can minimise the impact of, for example, damaging social media content on individuals. We think it important that children are aware of their deletion rights and have a simple means of exercising these.

The ICO recognises fully the need for a personal family and household exemption given the importance of 'private informational space'. We also note that the interface between the DPA's privacy protections and its provisions intended to protect freedom of expression add an additional level of complexity to this issue; one person's hurtful posting may be another person's freedom of expression.

What challenges face the development and application of effective legislation? In particular in relation to the use of national laws in an international/cross-national context and the constantly changing nature

and availability of internet sites and digital technologies? To what extent can legislation anticipate and manage future risks?

This could be a significant problem area. As it stands, most of the major providers of online services (search engines, social networks, gaming sites etc.) have some form of establishment in the UK (or EU). On the whole they seem committed to complying with local laws, including data protection law. So for the moment – within the EU at least – we are confident that we have a coherent set of laws that provide reasonable protection to children using online services.

However, there could clearly be problems where children use internet services provided by companies outside the EU and that are not required to meet EU-style data protection standards. It is questionable how much protection the ICO, or other EU data protection authorities, could deliver to individuals in respect of such companies. Although we can – and do – seek to resolve problems with overseas organisations, we must recognise the challenges we could face in carrying out any meaningful enforcement action should an organisation fail to cooperate voluntarily.

Given the methods individuals can use to register, operate and access online services we are aware of the problem of tracking down some organisations' physical location or those of the individuals who may misuse those services to cause harm to others. This might be a company making marketing calls to people registered with the Telephone Preference Service or an individual using an anonymisation service to post illegally obtained material on a social networking site.

However, the ICO is helping to develop more effective international co-operation mechanisms, for example our role in leading the Global Privacy Enforcement Network (GPEN). This is a global group of around 60 privacy enforcement authorities. Its objective is to develop better co-operation mechanisms and to learn how best to carry out effective enforcement when faced, for example, with a company that causes problems for individuals across the world. In 2015, 29 GPEN members conducted a 'privacy sweep' to look at websites and apps targeted at, or popular among, children. The project raised concerns about 41% of the 1,494 websites and apps considered, particularly around how much personal information was collected and how it was then shared with

Does the upcoming General Data Protection Regulation take sufficient account of the needs of children? As the UK leaves the EU, what provisions of the Regulation or other Directives should it seek to retain, or continue to implement, with specific regard to children? Should any other legislation be introduced?

The extent to which future UK data protection law will replicate the GDPR is currently uncertain. However, the GDPR contains specific provisions intended to protect children's data online. As explained above, it does this by invalidating children's consent, and requiring parental or guardian consent, before information society services can be accessed by a child. (A child can be defined on a Member State basis as anyone below the age range of 13 – 16 years.).

During the passage of the GDPR the ICO expressed its reservations about a broad age-verification/parental consent model that did not take account of risk. This was in terms of workability and effectiveness as a protection. Whilst not ruling out such a system completely, we continue to favour an approach that takes into account the nature of the service being accessed and the child's ability to understand the implications of using it.
Data protection law can still provide protection for children without having specific provisions relating to them, just as it can offer protection to other groups who – for whatever reason – may have a relatively limited level of understanding. However, there could be advantages in including specific child-protection provisions in future data protection law provided they are drafted in a realistic, flexible way and offer genuine protection to those that need it.

What more could be done by the Government? Could there be a more joined-up approach involving the collaboration of the Government with research, civil society and commerce?

Generally, we think Government should continue to recognise that the online protection of children is a multi-faceted issue that needs a co-ordinated response from the various agencies, departments and groups with an interest in the area. Data protection provides specific but effective protection to children but – for some of the reasons we have set out above – it is only part of the answer. The ICO will continue to recognise the importance of children's privacy and to work with the Government to ensure a coherent and joined up approach that results in an effective and comprehensive privacy protection system for children using the internet.

1 September 2016

ICO and Adam Glass – oral evidence (QQ 44-51)

Transcript to be found under Adam Glass

Internet Advertising Bureau UK - written evidence (CHI0036)

Summary

1. The Internet Advertising Bureau (IAB UK) is the industry body for digital advertising in the UK. It works to promote the optimal policy and regulatory environment for the digital advertising market to continue to thrive, and to promote good practice to ensure a responsible medium (***section 1***).

2. Advertising – increasingly underpinned by consumer data – plays a significant role in the internet and its development. It is the lifeblood of the digital economy in the UK, EU and globally. As with traditional media, it is the business model for making (non-publicly funded) content widely available to UK citizens, including children, for little or no cost (***sections 2 & 3***).

3. Digital advertising in the UK is effectively regulated by a combination of legislation and self-regulatory rules. General rules apply to all non-broadcast advertising, regardless of the age of the target audience, that state advertising must be responsible and must not mislead or offend. There are also specific rules that address advertising to children, recognising that in some areas they need greater protection. These rules apply to all digital media, including social media. Digital advertising is, by its nature, able to be targeted to include particular audiences and – importantly – exclude audiences, such as children, that are not appropriate (***section 4***).

4. The Data Protection Act provides effective, principles-based regulation of the collection and use of personal data in digital advertising, including in respect of children. In addition, the industry has developed EU-wide good practice to provide greater transparency and user choice and control over the use of data for online behavioural advertising, with specific provision relating to younger children (***sections 4 & 5***).

IAB UK makes the following recommendations to the Select Committee:

- **The Committee, and UK policy-makers in general, should recognise the significant benefits of digital advertising – in helping fund content, services and applications at appropriate cost to consumers.**
- **Any new or revised UK data protection legislation should:**
  - **be principles-based, flexible, and future-proof**
  - **be technology-neutral, to account for technological evolution**
  - **take a risk-based approach to enforcement**
- **The Committee – and the UK Government – should show support for and commitment to the advertising industry's system of self-regulation, particularly in the uncertain economic and regulatory climate that has arisen following the UK's decision to leave the EU.**
- **The Committee should also support MediaSmart, the advertising industry's flagship children's media literacy programme.**

Written evidence

1. Introduction

1.1 The Internet Advertising Bureau (IAB UK) is the industry body for digital advertising in the UK. It represents over 1200 businesses engaged in all forms of online and mobile advertising, including media owners and advertising technology businesses.

1.2 The IAB is actively engaged in working towards the optimal policy and regulatory environment for the digital advertising market to continue to thrive. We also seek to promote good practice to ensure a responsible medium. Further information is available at www.iabuk.net.

1.3 The Committee's call for evidence notes that 'the internet enables access to the World Wide Web, social media, games and many other online applications'. In turn, digital advertising enables that access to often be at little or no cost, playing a vital role in funding much of the content and services available online, including those used and enjoyed by children. IAB UK would therefore like to take this opportunity to provide the Committee with some information about digital advertising as it relates to some of the Committee's questions about children's use of the internet, including the use of personal data.

1.4 IAB UK's written evidence provides an overview of the UK digital advertising market, its role in and contribution to the digital economy, how

the various advertising business models work, the different types of approaches or techniques that a marketer may use to advertise, and how data is used to make some of these approaches even more relevant to consumers. It also highlights the challenges that the sector faces and how these are managed through a combination of legislation and self-regulation.

1.5 For the purpose of its inquiry the Committee defines 'children' as those aged 18 and under. Advertising regulation and self-regulation uses different definitions/age-based categories as appropriate to the issue in question. In some cases, therefore, measures or rules that are in place will apply to all 'children' (as defined by the Committee) or to or to a sub-set of 'children'. Some are specifically aimed at younger children (usually defined as those aged 12 and under). Where relevant we have made these distinctions clear in our submission.

1.6 IAB UK makes the following recommendations to the Select Committee:

- **The Committee, and UK policy-makers in general, should recognise the significant benefits of digital advertising – in helping fund content, services and applications at appropriate cost to consumers.**
- **In relation to the UK's data protection framework once the UK leaves the EU, we believe that any new or revised legislation should:**
  - **be principles-based, to enable a flexible, future-proof framework with a focus on regulating behaviour**
  - **technology-neutral, so that the rules have longevity in light of rapid and often unpredictable technological evolution**
  - **take a risk-based approach to enforcement: different data classes pose different privacy risks and the law should reflect this by lessening the regulatory burden for lower-risk data processing**
- **The Committee – and the UK Government – should show support for and commitment to the advertising industry's system of self-regulation, particularly in the uncertain economic and regulatory climate that has arisen following the UK's decision to leave the EU.**
- **The Committee should also support MediaSmart, the advertising industry's flagship children's media literacy programme, and promote the free resources it makes available to schools, teachers, parents and carers via** http://www.mediasmart.uk.com.

2. The UK digital advertising market: benefits

2.1 Advertising – increasingly underpinned by consumer data – plays a significant role in the internet and its development. It is the lifeblood of the digital economy in the UK, EU and globally. As in traditional media, it is the

business model for making (non-publicly funded) content widely available to UK citizens for little or no cost. It pays for much of the content and many of the services online: from search, webmail, social networking and price comparison sites, to productivity suites, blogs, video/photo sharing and the majority of news, information and video / entertainment sites. This is as true for children as for adults: children can access educational resources, carry out research for their homework, play games, pursue their hobbies, watch their favourite TV programmes and interact with their peers through online content and services that are funded by advertising.

2.2 Digital advertising – driven by consumer demand for content and services as well as quicker internet speeds – is the fastest-growing marketing medium in the UK outstripping all other advertising sectors. The UK leads Europe in digital advertising: in the UK, online and mobile has a higher share of the total advertising market (43% of a total £20.1bn) than in any other country in the world.[242] In 2015, £8.6bn was spent on online and mobile advertising in the UK, a like-for-like increase of over 16% on 2014. The UK digital advertising market in 2015 was more than the double the size of the next biggest in Europe, Germany.[243]

3. Digital advertising: how does it all work?

3.1 The internet and digital platforms (including mobile and other connected devices) offer advertisers a wide range of different approaches to market their products and services. In terms of advertising spend the three main approaches are: 'search' (e.g. via a search engine such as Google or Bing); 'display' (e.g. ads that you see on a website) and 'classified' (similar to the listings in a newspaper).

3.2 Advertising on digital platforms today is targeted to reach the right audience and to maximise the return on the marketer's investment (although there are restrictions on how children may be targeted – see section 5). Digital advertising is, by its nature, able to be specifically targeted to include particular audiences and – importantly – exclude audiences, such as children, that are not appropriate.

3.3 Primarily, targeted digital advertising has five main forms:

- **Contextual advertising:** This is where advertisements are served within a chosen 'context' (e.g. a 'banner ad' shown at the top or side of a webpage) based on the selection of a website or a search engine query on a particular topic and therefore assumed interest. An example: a user is shown an advertisement for lawnmowers because he or she is visiting a gardening-related website. No user data, personally identifiable or otherwise, is collected from the consumer or used in order to deliver this type of advertising. The relevant information is taken from keywords identified in the context by the context creator (i.e. the user).

242 http://www.iabuk.net/research/library/2015-full-year-digital-adspend-factsheet
243 Adex Benchmark 2015:European online advertising expenditure, IAB Europe/IHS, July 2016

- **Demographic advertising:** This is where advertisements are served based upon specific information provided by the user (e.g. gender, age, location). An example: a teacher living in London who has registered on a jobs website is shown advertisements for teaching opportunities in London on the website but not necessarily in the teaching section. It is worth noting that some information provided by the user may be segregated, retained and used without it being able to identify (or be associated with) an individual.

- **Content marketing:** Often called 'native' advertising, this can take many different forms. In essence, this is advertising that fits neatly within the surrounding look and feel of the site or app ('advertorials' being a common example). This is often content-based and is therefore more relevant to the user. However, this type of marketing needs to be clearly disclosed as such and the IAB has recently published market guidance setting out how businesses can provide transparency to consumers, to help them comply with the law and the Committee for Advertising Practice (CAP) Code.[244]

- **Behavioural advertising (also known as interest-based advertising):** This identifies large groups of users with similar interests based upon shared attributes, such as previous web browsing activity over multiple sites, in order to provide more relevant advertisements. This type of advertising operates without data being collected that directly identifies a user, rather by using device identifiers such as cookies. An example: a user's device is served with advertisements about golf equipment because the user has – over a period of time – visited different golf websites. An example of how this works is shown at www.youronlinechoices.com/uk/about-behavioural-advertising. The underlying business model and technology for this type of advertising can vary but they are most commonly browser-based and infer a user's interests from ads clicked on, content viewed and searches made. There are restrictions on behavioural advertising targeted at children – see section 5.

- **Retargeting**: This is where a specific user interest is derived from their interaction with a single site and adverts relating to the content viewed are served to the same device when a user visits other websites on that device. Thus the user is 'retargeted' on other websites and this allows the creative to be dynamic and more personalised. Like behavioural advertising, the adverts are served in real-time using intermediaries operating under contract to the advertiser / agency. For example: a user is offered a discount deal on a pair of shoes on a separate site following their visit to the site displaying the viewed shoes.

3.4 Dynamic advertising creative combined with automated trading of inventory (known as 'programmatic trading') now enables customised advertising to

---

244 www.iabuk.net/about/press/archive/iab-launches-guidelines-to-provide-greater-transparency-in-native-digital
www.iabuk.net/resources/standards-and-guidelines/content-and-native-disclosure-guidelines-phase-2.

be selected and delivered in real-time. In 2015, 60% of all digital display advertising was traded programmatically.[245]

Legislation and Regulation
9. What are the regulatory frameworks in different media? Is current legislation adequate in the area of child protection online? Is the law routinely enforced across different media?…

4. Digital advertising regulation and self-regulation

4.1 Digital advertising in the UK is regulated by a combination of legislation and self-regulatory rules. In terms of the legal framework and regulatory oversight, the activities of behavioural advertising and retargeting involve the collection and use of data – some of which may include personal data – and as such may be subject to the UK Data Protection Act 1998 (as well as the Privacy and Electronic Communications Regulations 2011) and are regulated by the Information Commissioner's Office (ICO).

4.2 The Data Protection Act is principles-based and effectively governs the collection and processing of children's information – whether for advertising or other purposes – without having (or needing) any specific age references. The ICO has produced practical guidance for organisations on how the principles should be applied in practice in terms of the collection and use of children's personal data (see section 5). In addition, the industry has developed EU-wide good practice to provide greater transparency and user choice and control (see section 5).

4.3 All non-broadcast advertising, including digital advertising, is governed by the Committee of Advertising Practice (CAP) Code, an industry agreed set of rules which are enforced independently by the Advertising Standards Authority (ASA). The ASA's remit was extended in 2011 to cover online marketing communications on organisations' own websites and in other non-paid-for space under their control. The CAP/ASA system is funded via an advertising levy meaning that complaints are dealt with at no cost to the consumer (or the public purse).

4.4 Self-regulation and good practice supplement legislation and fill the gaps where the law does not or cannot reach, often going beyond what the law requires, and offering an easily-accessible route for resolving disputes and the flexibility to respond to issues and adapt to new technologies and business models. This is particularly important in fast-moving markets like digital advertising.

4.5 The CAP Code is media-neutral and the ASA enforces the CAP Code rules consistently across all non-broadcast media. The Code includes general rules that apply to all non-broadcast advertising, regardless of the age of the target audience, that state advertising must be responsible and must

245 http://www.iabuk.net/research/library/2015-full-year-digital-adspend-factsheet.

not mislead or offend. It also contains specific rules that address advertising to children (as described below).

Regulation of marketing to children

4.6 The UK CAP Code contains specific rules on marketing to children in areas where they are seen to be more vulnerable and need greater protection, and to reflect the age-restricted nature of certain products and services. There are also stringent rules for marketing communications addressed or targeted to a child under the age of 16. For example, any marketing communication must not contain anything that is likely to result in their physical, mental or moral harm or exploit their credulity, loyalty, vulnerability or lack of experience.

4.7 The CAP Code prevents marketing communications from condoning or encouraging poor nutritional habits or an unhealthy lifestyle in children. It goes even further by implementing strict rules for food and drink advertising directed at pre-school or primary school children (CAP is currently reviewing these rules following a public consultation with a view to introducing further restrictions).

4.8 In both online and offline media, the CAP Code states that age-restricted products such as alcohol and tobacco cannot be targeted at people under 18 or 16 (respectively), for example through the choice of media, and can only be marketed in an environment where at least 75% of the audience is aged over the minimum age requirement. To serve advertising, or to market on a particular site or app, a brand should be satisfied (and be able to demonstrate, in the event of an investigation by the ASA) that the site/app has a target audience at or above the 75% threshold.

Advertising on social media

4.9 CAP code rules on marketing to children – including thresholds on ads for age-restricted products – apply to adverts in social media where they are shown to a UK audience. There are controls in place in social media to stop children seeing and interacting with age-restricted brands/advertising content. Different social media platforms will have their own minimum age requirements for individuals signing up to their platform. UK and EU law does not set a minimum age, but many services set a minimum age of 13 years, in line with the US Children's Online Privacy Protection Act (COPPA).

4.10 In addition, responsible platforms put in place measures to restrict what brand content and adverts children and young people can see. As well as ensuring that their advertising policies reflect relevant legislation and the CAP Code, social media platforms operating in the UK such as Facebook, YouTube and Twitter offer advertisers effective controls to ensure that only age-appropriate audiences are targeted by their marketing campaigns. Social media platforms are therefore better-equipped than some other more traditional forms of media – print, for example – to provide tools to

manage which users see a particular advert, and to avoid it being seen by children where that would be inappropriate.

4.11 In terms of digital advertising, online publishers and platforms succeed by offering advertisers a large number of potential consumers, underpinned by accurate data and evidence of an effective route to purchase. Advertisers have a reputational and financial motive not to advertise to children and therefore social media sites – that rely on advertising for revenue – prioritise this when designing their back-end functions.

4.12 In practice, advertisers use the data held by social media platforms about their users to 'design' an audience for their advertising campaign that matches their target demographic(s). For example, an advert might only be served to accounts of a defined age, in a set location and with a specific interest – and users who exhibit certain behaviours or have interests (such as content that they share and accounts they follow) that do not correlate with those criteria will be excluded.

Risks and benefits
1. What risks and benefits does increased internet usage present to children, with particular regard to:
…
iii Data security.

5. Addressing privacy Concerns: transparency and control

5.1 The use of personal data in digital advertising in the UK is regulated by a combination of the self-regulatory frameworks described in section 4, and legislative rules including such as the Data Protection Act of 1998 and the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011. UK Data Protection law is regulated by the Information Commissioners Office (ICO). The ICO's 'Personal information online Code of Practice' recommends that a marketer should obtain parental consent for the collection of personal data from young children (12 years and under) – data such as a name, address or email address.

5.2 In addition to legislative requirements and the mandatory self-regulatory system of CAP and the ASA, the digital advertising industry has established self-regulatory frameworks in other specific areas in order to set out accepted standards and good practice for responsible advertising. One such framework covers the use of personal data for online behavioural advertising.

5.3 IAB UK acknowledges that the collection and use of consumer data (such as web browsing and other information) could potentially raise issues relating to consumer privacy. In 2011, building on an US initiative and the development of good practice in the UK, EU advertising and media trade bodies published good practice for all EU and EEA markets to enhance transparency and user control for online behavioural advertising (OBA). This framework applies to advertising targeted at any user, including those

aged under 18, with specific provision relating to younger children, as described below.

5.4 The initiative is based upon seven key principles:

i. Notice: Transparency about data collection and use practices associated with behavioural advertising, providing consumers with clear, prominent and contextual notice through multiple mechanisms, including an icon in or around advertisements linked to further information and control mechanisms.

ii. User choice: Greater consumer control over behavioural advertising. For example, via www.youronlinechoices.eu.

iii. Data security: Appropriate data security and retention of data collected and used for behavioural advertising purposes.

iv. Sensitive segmentation: This principle recognises the need for additional protection for younger children, and requires participating businesses to agree **not to create 'interest segments' to specifically target children (12 and under) and on the collection and use of sensitive personal data for behavioural advertising**.

v. Education: For consumers and businesses about behavioural advertising and the self-regulatory Framework.

vi. Compliance and enforcement: Mechanisms to ensure the effectiveness of the Framework, including a trading seal to be granted to compliant businesses once independently audited and which demonstrates to other businesses that the holder adheres to the obligations under the Framework.

vii. Review: Regular review of the Framework to ensure it evolves with developing technology and business practices. For example, in 2016 the EDAA extended the existing principles to the mobile environment, so that they apply to ads shown on smartphones and tablets in addition to desktops and laptops.

5.5 A copy of the EU industry Framework can be found at: http://edaa.eu/european-principles/. At the heart of this work is a symbol or icon (see below right – often known as the 'AdChoices' icon) that appears in or around the advertisements on sites, as well as on site pages themselves. When a user clicks on the icon he or she will be able to find out more about the information collected and used for this purpose. In 2015, over 229bn icons were delivered by approved providers across Europe, giving consumers significant opportunities to manage or control their online advertising preferences.[246]

5.6 The icon also links to ways for internet users to manage their interests, such as via privacy dashboards or ad preference managers. It also links to a pan-European website – www.youronlinechoices.eu – with helpful advice,

246 http://www.iabuk.net/news/edaa-2015-activity-report

tips to help protect privacy and a control page where you can turn off behavioural advertising. There are on average 2.7 million unique visitors to www.youronlinechoices.eu every month.[247] The UK version of the website is at www.youronlinechoices.eu/uk. Further information on the initiative is available at www.iabuk.net/policy/briefings/updated-iab-factsheet-may-2014-online-behavioural-advertising.

5.7 The EU industry initiative is administered by the European Interactive Digital Advertising Alliance (EDAA) www.edaa.eu. The ASA administers OBA consumer complaints in the UK and in 2013 new rules on OBA were introduced to the CAP Code to ensure businesses provide:

- notice to be provided to web users **in or around the advertisement**;
- choice via an **opt out mechanism** to prevent data from being collected and used for behavioural ad purposes.

These rules are **complementary** to the EU Framework: those businesses complying with the EU Framework will be complying with the ASA's rules.

Education
5. What roles can schools play in educating and supporting children in relation to the internet? What guidance is provided about the internet to schools and teachers? …

6. Media Literacy

6.1 IAB UK believes education is central to better consumer understanding and trust of innovative and evolving advertising techniques (and broader online business models) that aim to provide discounted products, services and applications, and which also underpin high quality content and services.

6.2 The UK advertising sector promotes children's media literacy via MediaSmart. MediaSmart is a not-for-profit company that creates free educational materials for teachers, parents and carers, to help young people (aged 7-16) think critically about the advertising that they come across in their daily lives.

6.3 IAB UK is a supporter of MediaSmart and in 2015 helped it to develop and launch new lesson plans for secondary schools covering social media advertising. Social media enables young people to communicate, discover and share with friends or join global networks with mutual interests and concerns. The resources aim to encourage students to think about:

- the type of social media available to them
- the advertising that they are exposed to on these sites and how to recognise and manage it
- their relationship with social media sites, their sponsors and brand advertisers

247 ibid.

- the business models that allow them to access a whole range of services at little or no cost

The resources also explain behavioural advertising and the 'Your online choices' programme (as described in section 5).

6.4 MediaSmart is also developing a digital advertising resource aimed at primary school children that will address, in an age-appropriate way: why are there adverts online and how they work; how users can manage their own online advertising experience; and how they can get the best out of social media and the advertising they see.

6.5 As this resource will be targeted at pupils who are too young to be on most social media sites (although there are child-friendly social media platforms), it will emphasise the importance of being honest about their age when they sign up – even if this means waiting until they are 13 before joining. The resources aim to help children feel more confident online, empowered to make choices and inclined to engage with advertising by encouraging them to use the privacy settings and advertising controls available to them.

August 2016

Internet Matters - written evidence (CHI0040)

Children and the Internet inquiry

Q2. Which platforms and sites are most popular among children and how do young people use them? Many of the online services used by children are not specifically designed for children. What problems does this present?

2.1 The latest Childwise Monitor shows that gaming apps are the most used by 7-16 year olds, with Minecraft being popular amongst 7-10s. Photo/video apps are the next most popular apps used with Instagram the favourite amongst girls.

2.2 The Childwise research also found that 3 social networking sites are used by almost half of children – Instagram (47%), Snapchat (46%) and Facebook (46%). Snapchat is the favourite app for 13% of children and this popularity starts at age 11-12.

2.3 The latest Ofcom research on Media Use and Attitudes shows that children are now using technology and getting online from a young age. 53% of 3-4 year olds use a tablet with 51% using it to go online and 28% playing games.

2.4 The main concerns for younger children are about viewing inappropriate content and online pornography. There are safe search engines that are designed for children (such as Swiggle and Kids-search) that can be used and a site like CBeebies allows younger children to explore and have fun in a secure environment.

2.5 Children aged 8-11 now spend over 11 hours online in a week and 15% are going online in their bedroom. 24% of 8-11 year olds own a smartphone and smartphone ownership outstrips non-smartphone ownership from 10 years of age.

2.6 Our most recent Pace of Change research showed variations by gender. Girls are more likely to use their smartphone to go online, while boys tend to spend longer using games consoles. Overall children are most likely to use the internet for entertainment rather than practical uses, such a listening to music, watching video clips or playing games.

2.7 The research also showed that whilst only a minority of children take part in risky online behaviour, this does increase with age, as children test the boundaries of what they can and can't get away with, and boys are especially likely to take more risks and break rules, even from a young age.

2.8 Children aged 7-17 are far more likely to say they use YouTube than any other website – more than four in five children normally use it (83%, especially boys), with Google their next most used site with seven in ten actively using (69%).

2.9 Parents concerns about online risks are those which could damage the child's emotional well-being or put them in physical danger, such as sexual content, inappropriate content they find themselves, violent content, bullying and strangers/grooming. This came from Cybersafe research in 2013 and is even more relevant today.

2.10 The use of sites such as YouTube which aren't designed for children can increase the risks of accidentally coming across inappropriate or adult content. As YouTube continues to be a favourite site amongst children this means parental engagement is even more important. This is why we encourage parents to talk to their child, give parental guidance and set up appropriate technical controls.

Q3. What are the technical challenges for introducing greater controls on internet usage by children?

3.1 In the last few years we have seen the deployment of numerous technical approaches for filtering and controlling the content that children can see online. These services are predominantly free and easily accessible and we have seen an increase in both awareness and take-up of services by families. However, filtering is just one part of a solution. No technical tool is 100% accurate, and this can be seen with home broadband filtering where filters can be intentionally circumvented by the use of a VPN, or by visiting encrypted sites, e.g. Twitter, where content cannot be assessed and blocked. It is important to point out that the use of VPN to avoid filtering by children is low and largely associated with older children who are more familiar with technology. In the most recent Ofcom report, the satisfaction of filtering with parents is extremely high, with the majority of parents feeling they are useful and block the right amount of content.

3.2 We have also seen some improvements to privacy settings on social media networks and the UKCCIS guidance setting out a clear standard for smaller developers to follow with regard to services for young people. Whilst most offer a range of services that allow users to control what they share and to report and block anything offensive, there are clear inconsistencies across platforms and no real enforceable minimum standard of service delivery. The high prevalence of children under 13 using social media services designed for adults is a concern and we would like to see more being done by the social media companies to either enforce their minimum ae range or design products that are more suitable for children.

3.3 This year we have seen a range of new products come to market designed intentionally for children, from major corporate like Sky (Sky Kids) and Google (YouTube Kids) to smaller starts ups like Azoomee. These products demonstrate the demand for ring-fenced services for children that allow them to have an age appropriate internet experience. This is a positive use of technology and we anticipate there will be more and more devices and applications developed to address parents need to give their children a safe experience online.

3.4 We are excited by some of the new emerging positive uses of technology we are seeing in the form of data analysis of social media use. A number of

start-ups are bringing new products to market that claim to be able to identify bullying behaviour, inappropriate language and images, and violent or sexual content. Whilst these rely on having access to young people's social media accounts, they will perhaps provide a useful bridging service for parents, whilst young children develop their critical thinking and judgement skills. Like filtering, they will not be 100% accurate and will be part of a number of mediation strategies that parents may choose to use.

3.5 Finally, we know that the most effective solution for keeping children safe online is effective digital parenting. Educating parents about the risks, the technology their children are using, and how to help children develop their own judgment and resilience is key to ensuring they reap the many rewards the internet offers, whilst having an age appropriate experience.

Q4. *What are the potential future harms and benefits to children from emerging technology, such as Artificial Intelligence, Machine Learning and the Internet of Things?*

4.1 The online world will continue to develop and the popularity of new innovations will still take us by surprise. The launch of Pokémon Go earlier this month has captured the imagination of millions, inspiring many to take to the streets to play what could be seen as the future of gaming – 'Augmented Reality' (AR) – effectively merging the real world with the digital world.

4.2 New technology can bring great benefits - the concept of having access to endless information at your fingertips seemed like science fiction but most of us would be lost without it now. The increase of wearable devices such as smart watches, smart or robotic toys and home appliances or devices that connect to the network shows that people are keen to use technology in all ways. But new things can cause uncertainty and throw up possible risks – this means there is a continuous need for parents, children and teachers to be educated. Parents especially often feel they are not equipped to help their children successfully navigate this brave new connected world.

4.3 Artificial intelligence (AI) is one of the most exciting developments in this area with some believing it could be a breakthrough moment for internet safety. There have been some dramatic advances in this technology. A smart assistant on a phone is now capable of helping a child who has unwittingly posted an inappropriate photo on Instagram or his phone number on Twitter delete or change their post.

4.4 AI could be the trigger for parent-child conversations. And, perhaps most interestingly, AI is being paired with services that alert parents when there has been an intervention, giving specific advice on how to have a conversation with the child that's positive and supportive.

4.5 If new technology is developed so that the needs of control and empowerment are properly balanced and we couple it with structured education, then it could be key in the battle to keep future generations safe online.

Education

Q5. *What roles can schools play in educating and supporting children in relation to the internet? What guidance is provided about the internet to schools and teachers? Is guidance consistently adopted and are there any gaps?*

5.1 While this area is not our focus, we believe that schools have a vital role in educating and supporting children about the internet. School is one of the main sources of information for children and teaching them to be a good digital citizen is a key skill.

5.2 The importance was recognised by the UKCCIS Board who set up an education working group to look at how education settings in the UK are responding to the challenges of keeping their pupils safe online and the role that UKCCIS can play in supporting them. We would refer the committee to the report of the working group in December 2015 and their recommendations to the UKCCIS Board.

5.3 Schools have been teaching online safety either as part of ICT/Computing, PSHE or one off safety sessions for many years. Since September 2014 online safety has also been included in the statutory computing curriculum. But there is debate about whether computing is the appropriate place for much of the delivery of 'online safety' education as many of the issues are about behaviour and understanding risk. Many schools use PSHE lessons to deliver online safety education lessons as this can give a wider perspective and supports the idea of being a good digital citizen.

Q6. Who currently informs parents of risks? What is the role for commercial organisations to teach e-safety to parents? How could parents be better informed about risks?

6.1 Research suggests the most successful approach for parents to help keep children safe online is a combination of mediation strategies, which adapt and change dependant on the age of the child. Core to this is awareness of the risks children face, underpinned by an understanding of the technology being used, and appropriate use of technical tools. We also know that the range of issues and risks that children face online are constantly changing and this combined with the relentless pace of development in technology often leaves parents feeling ill-equipped and unprepared.

6.2 It is generally acknowledged that we need to help educate parents and encourage active and engaged parenting, providing them with the information and advice they need to help their children understand ways to behave online and to develop their judgement and resilience.

6.3 The biggest challenge we face is motivating parents to get engaged with the issue, before they have an issue. In the past government would have invested significant sums in public service broadcasting, to help drive home the message that parents need to get involved, however pressure on budgets means that this is no longer an option.

6.4 Whilst there has been significant progress and investment in the range and availability of technical tools across networks, devices and platforms, there has not been a comparable investment in driving awareness, education and engagement of parents.

6.5 While a lot of good advice exists for parents, research shows they struggle to know where to go for reliable advice, as evidenced in the Ofcom report and Internet Matters Cybersafe study. The plethora of information available through a simple internet search demonstrates the raft of information from varying sources that parents are faced with. The degree of duplication risks undermining the good work different charities and industry partners are doing. The challenge for the sector as a whole is better collaboration, with partners working to reinforce and amplify each other's work, rather than competing for the attention of parents.

6.6 We believe that there is a role for an organisation like Internet Matters to allow industry and the sector experts to collectively work together to address this hugely important issue. An independent, transparent organisation, that is funded by small contributions from the commercial organisation across the entire eco-system involved in children's safety online. It is no one single group of organisations that is responsible, device manufacturers, networks, retailers, content platforms, games providers, social networks must all play their part.

6.7 Importantly the collective group must support the work of existing providers of front line services. The primary purpose of the organisation must be to create awareness of the risks, motivate parents to get involve, organise services and resources so they are easy to access, and finally connect parents with the best advice for their issue, and for their child. The breadth and range of advice required is so diverse, and is further complicated by the age of the child, that we feel that without this we will continue to provide broad brush advice that is generic or make parents jump through hoops to find the most appropriate help.

6.8 Internet Matters already invests heavily in helping parents keep their children safe online. 80% of current industry funding is used to raise awareness of the issues and risks, in digital and traditional media, and the remaining 25% is used to operate the Internet Maters website, develop content specifically to fill gaps or to address new issues, and covers operational costs.

6.9 Our campaigns have received a number of awards and have prompted over 3m visitors to the Internet Matters website. We continuously monitor brand awareness of Internet Matters, which is currently at c.31-33% of the UK parent population, plus we have almost 40k followers on social media.

6.10 BT, Sky, TalkTalk and Virgin Media all have ongoing marketing programmes to promote the work undertaken by Internet Matters, connecting parents with the advice & help they need.

6.11 We partner with a number of organisations to ensure our high-level content is the most up to date, our goal being to present information to parents

in a way that is easy to understand, is actionable, and is relevant. We have developed a range of downloadable resources for parents, two apps to engage parents and children, and a tool which provides parents with personalised step by step instructions on how to set parental controls on up to 35 different networks, platforms and devices.

6.12 We invest in research to understand the issues parents face and also monitor our website to ensure this meets the need of parents across the UK. Our next research study will be published in the autumn of 2016.

6.13 We are actively engaged with industry, encouraging investment in this important area, and our ambition is to create a long-lasting charitable organisation, funded by industry, that can have a material impact on this issue. We have recently announced that the BBC, Google and now Dixons Carphone are supporting Internet Matters, through various programmes of activity.

6.14 The combined reach of the Internet Matters partner network is enormous. The ISP's alone reach 90% of UK households, and this will become even more effective with the addition of our new partners.

6.15 For information, we are members of the UKSIC Advisory Board and also the Google Workshops - Advisory Panel. We sit on the UKCCIS Filtering Working Group. We are members of the ABA and are supporting the APPG on Young People and Social Technology. We have our own Expert Advisory Panel that includes: Childnet, ABA, Family Lives, NSPCC, CEOP and John Carr. We are active supporters of Safer Internet Day and Anti-Bullying Week.

6.16 We work collaboratively with a number of organisations and have invested in the joint creation of resources and campaigns, e.g. Childnet & the Digiduck App, ABA & the Anti-Bulling Week competitions, CEOP & the Internet Matters app. All our services are free to parents and to the sector experts. This year we plan to work with UKSIC to fund the development of a new app and also are joint sponsor of Anti-Bullying Week.

6.17 Internet Matters and its partners are committed to trying to establish a model that allows us to collectively work together to help parents in their challenge of keeping their families safe online.

Governance

Q7. *What are the challenges for media companies in providing services that take account of children? How do content providers differentiate their services for children, for example in respect of design?*

7.1 As mentioned in our reply to Q3, this year we have seen a number of companies launching services designed for children. A child-friendly version of YouTube app is now available which filters out inappropriate content and hides comments on videos giving parents' peace of mind and a child a safer online viewing experience. Sky have launched the Sky Kids tablet app full of kids favourite shows where you can set up age related profiles and set time limits.

7.2 The minimum age limit is 13 for several social networking sites, including Facebook and Instagram. But we know that children under 13 are using these sites and enforcement of the minimum age could be improved. Sites aimed at under-10s like Moshi Monsters and Club Penguin also have social networking elements and these tend to give more protection.

7.3 We have already mentioned the UKCCIS best practice guide for smaller social media developers and we recommend this is widely promoted to encourage all sites to have common standards for child safety. This is a good first step but we also think there should be more consistency in how to block/report content and that the default setting should be private for children to make sure profiles and posts aren't shared publically without realising it.

Q8. What voluntary measures have already been put in place by providers of content to protect children? Are these sufficient? If not, what more could be done? Are company guidelines about child safety and rights accessible to parents and other users?

8.1 Our Pace of Change survey found that parents are best equipped to help their children use and be safe on well established social networks, but struggle to keep up and help with the more modern social networks that children are keen to use.

8.2 For longer established sites like Facebook, Skype, Google+, Twitter and WhatsApp, parents are very likely to know how to use these, and the majority would be confident helping their child to set up an account, and comfortable talking about how to use them safely.

8.3 The bigger content providers have already shown a willingness to protect children when accessing their services. But there is always more to do – protection mechanisms and guidance are only useful if parents know how to find them and set them up. At Internet Matters we have step-by-step guides to setting up controls on networks, devices and entertainment services across the home. This helps inform parents and allows them to have conversations with their children about staying safe online.

Legislation and Regulation

Q12. What more could be done by the Government? Could there be a more joined-up approach involving the collaboration of the Government with research, civil society and commerce?

12.1 The Government must continue to take an active role in tackling online safety. It is the role of government to set clear direction and strategy that engages all parties and effectively uses the resources that already exist. The focus on these issues from recent governments have put the UK in a strong position to protect children online. We strongly recommend that this focus continues to keep ahead of new challenges.

12.2 One way would be to use the UKCCIS Board to set a clear strategy, agreed with all parties and define outcomes. That way all groups can work towards the same goals and we can effectively measure progress.

12.3 Government also have a key role to encourage all organisations – commercial, NGO, education and government to work together for the common good. This would make it clearer for parents and easier for the education sector if all parties share the same goals.

August 2016

The Internet Service Providers' Association (ISPA UK) – written evidence (CHI0031)

About ISPA

The Internet Services Providers' Association is the trade association for the internet industry in the UK. ISPA has over 200 members from across the sector, including a large number of access provider ISPs from small to large, content platforms, hosting providers, and others. ISPA has been heavily involved in online safety policy since our inception in 1995. For example, we helped set up and still help fund the Internet Watch Foundation, regularly respond to parliamentary inquiries and government consultations and our members are at the forefront of helping their customers and users protect themselves through education, awareness, and technical tools.

Introduction

1. ISPA welcomes parliamentary interest in this area and supports the Committee's position on the importance of child internet safety. The internet as a vital tool in children and young people's development and key for a successful modern economy and society. In light of this, ISPA members have dedicated huge amounts of time and resources to helping make the internet safer, including by working with Government, and we believe that this approach has been highly successful and should be continued. Initiatives such as Internet Matters and the UK Council for Child Internet Safety have brought together industry, Government, and stakeholders and helped the UK to become a world leader in the area of child online safety. We believe that the current regulatory environment that promotes self-regulation over regulation has achieved a great deal, so would encourage caution before jumping into any new legislation that may be detrimental to this progress.

ISPA Position

2. The internet has been transformative in the lives of young people who have grown up as digital natives. It is now a part of everyday life for young people and is deeply ingrained in all aspects of their lives, with children often seeing no distinction between their online and offline lives. Educationally, the internet offers opportunities to learn and experience in a way that was not previously possible, and has opened up huge opportunities for their development. Crucially, the internet also helps children gain digital skills, which are important to the UK maintaining its place as a world leader in the digital economy and are only likely to become more so. For the UK to maintain this role, it is crucial that children have the chance to learn and explore the online world, honing their skills in a digital, knowledge-based economy.

3. Whilst the internet also carries adverse risk, as with other aspects of everyday life, we believe that if children's use of the internet is moderated

by a parent or carer in a sensible manner that the benefits far outweigh the risks. To help parents, carers, and young people themselves, our members have worked to educate and empower parents to become more internet savvy and keep their children safe online. An example of this has been the setting up of Internet Matters – funded and run by BT, Sky, TalkTalk and Virgin Media - which offers advice and information on tackling e-safety issues and gives parents and carers the support they need. We would suggest that this kind of education and empowerment is the most effective solution to managing online safety, supported by technological tools. Examples of technical tools and education and awareness programmes offered by industry include:

- Companies, including ISPs, operating systems, search engines and others, provide online safety guides, awareness raising and education to their customers to help make the right choices for them.
- A number of ISPs, both large and small, offer consumers the choice on whether to install network-level configurable parental controls, with more than 90% of consumers covered by a range of ISPs.

These tools offer granular filtering across a variety of categories determined by the end user, cover multiple devices in the home and are adaptable for different age groups. However, these tools have limitations, may over or under block and should not be viewed as a silver bullet solution.

- Other device-based technical tools can be used to help protect users online
- Content providers, search engines and other platforms stipulate within their terms and conditions what content they view as inappropriate, and moderate their networks to remove it. This includes websites like Facebook and Twitter which seek to remove extremist and pornographic content and are able to ban users.
- ISPA and many ISPs have helped to setup the IWF and have consistently supported the organisation which is considered to be world class in preventing people from access child abuse content and facilitating the removal of such content at source.

4. However, it is important that both industry and Government play their part in making sure the internet is safe for children. Government has led the way through the creation of UKCCIS bringing together stakeholders to identify, work through and solve issues. However, one further area in which Government could show leadership is on education and consider the value of an educational campaign, similar to that they have done for cyber-crime and a host of other more traditional public health campaigns, that would involve educating both parents and children on the dangers associated with the internet and how they can be avoided.

5. We would also highlight that some of the most harmful behaviours, such as cyber-bullying, are often societal issues rather than simply technological. Whilst the bullying is taking place online, it could just as easily take place in the schoolyard and should be treated in the same way. At times the current policy debate is sometime too strongly focused on finding a technological

fix to a problem that often has societal roots or is simply an expression of offline behaviour that was always present in some sort or form. The same approach of moderation and education is the most effective way to tackle societal and behavioural issues.

6. ISPA believes that current legislation in the area of child protection online is largely sufficient. The current approach, in which Government have partnered with industry and stakeholders and looked first at self-regulation, is we believe the most effective way. This approach is able to keep pace with technology in a way that legislation often cannot, meaning the UK is seen as a wold leader on internet safety. For example, the level of child abuse content hosted in the UK has fallen from 18% in 1996 to below 1% today through a self-regulatory approach, rather than legislation. That's not to say that legislation does not have its place as a backstop and to provide clarity on the law, and there may be a need to review and streamline legislation. For example, with the police are said to be using up to 30 pieces of legislation to prosecute online abuse. We also believe that Government will face numerous challenges whilst implementing their age verification legislation, due to many websites being based outside the UK. Thus, we firmly believe that Government should continue to work with industry in order to tackle the problem of children's safety online, such as through UKCCIS.

Technical Challenges

7. We believe that technical fixes to control internet usage should not be viewed as a silver bullet solution to the issues at hand. Whilst there will be technical challenges involved in introducing greater controls on internet usage by children, the main reason we do not support a solely technical approach is that we see it as less effective. For example, some have called for ISP-level blocking of non-compliant pornographic websites, as they see it as an effective means to make sure pornographic websites comply with the age verification measures. However, we believe that this would be an ineffective approach as in 2011, Ofcom reviewed the practice of blocking websites to reduce online copyright infringement and found that blocking websites could be easily circumvented, carried adverse risks, and could ultimately have an impact on privacy and freedom of expression.

8. Blocking would also carry an adverse impact on the operation of the open internet - the ability to impose technical measures on individual users will vary between ISPs and there could be unintended consequences for ISPs' networks. Moreover, there may be significant impact on business to comply with blocking orders that could have a negative impact on UK ISPs. Instead, policy measures are best targeted at the most effective part of the internet value chain, in this instance the sites themselves or those that help support them financially.

9. We would also highlight that it is important that the Committee considers the internet value chain and realise that different actors play different roles within the chain and not lump the 'internet' as one homogenous body. Whilst internet service providers can provide filtering products, they cannot

control what is hosted on social media platforms. Thus, policy in this area needs to take account of this and be directly targeted at the correct part of the internet value chain.

General Data Protection Regulation

10. GDPR is a robust framework for data protection and in our opinion it goes a significant way in terms of enhancing children's safety online. The introduction of an age of consent of 16 for processing personal data by a data controller offers new protections for children and the Regulation clearly states that 'children deserve specific protection of their personal data', especially when used 'for the purposes of marketing or creating personality or user profiles', allowing any data subject the right to object to the use of his/her personal data for the purposes of 'direct marketing'. These provisions will impact the experience of children online and especially their exposure to marketing and advertising, as children are explicitly protected and given the right to challenge if their data is used.

11. GDPR also contains provisions to make sure that any communications to users about how their data is being processed contain the use of 'plain language' and the use of pictograms or icons to make it easier for users to understand. This will allow parents to have a clearer picture of how a website may process data and make an informed decision as to whether they feel it is appropriate to allow their child to use a service.

August 2016

Internet Watch Foundation and National Crime Agency – oral evidence (QQ 28-36)

Evidence Session No. 2 *Heard in Public* *Questions 18 - 36*

TUESDAY 13 SEPTEMBER 2016

Members present

Lord Best (Chairman)
Lord Allen of Kensington
Baroness Benjamin
Baroness Bonham-Carter of Yarnbury
Earl of Caithness
Lord Gilbert of Panteg
Baroness Kidron
Baroness McIntosh of Hudnall

Examination of Witnesses

Ms Susie Hargreaves OBE, CEO, Internet Watch Foundation, and **Dr Jamie Saunders**, Director, National Cyber Crime Unit, National Crime Agency

Q28 The Chairman: Welcome to you both. Sue Hargreaves and Jamie Saunders, thank you very much for joining us. You have seen how the system works. We would like you, if you would, to introduce yourselves very briefly and, if you would like to do so, to make any kind of opening statement before we start. Although we have your biographical details, we need to have them on the record. Perhaps you could talk us through who you are, your organisations' purposes and where you think we should be going. Susie, would you like to start us off?

Ms Susie Hargreaves: Thank you very much for inviting me here today. I am Susie Hargreaves, the chief executive of the Internet Watch Foundation. The IWF is the UK hotline for reporting and removing online child sexual abuse images and videos. We are the most successful hotline in the world. When we started 20 years ago, 18% of known child sexual abuse was hosted in the UK. Since 2004, that has been less than 0.5%, and last year it was 0.2%.

To give you an idea of what child abuse is, we are not talking about harmful content; we are talking about criminal content that nobody should see. Last year we removed 68,000 URLs—a URL is an individual web page. Each web page could have one or 1,000 images of child sexual abuse. We removed 68,000 of them. Of the images and videos we removed, 69% of the children were aged under 10; 3% of the children were aged under two; and around 70% of all the

images and videos were categories A and B, which are rape and sexual torture. About 80% of the images and videos were of girls.

We are funded by the internet industry. We have 130 members, including all the big companies that you know of—Apple, Amazon, Google and Facebook—through to the internet service providers, the mobile operators and filtering companies. We receive about 90% of our funding from them and a further 10% from the EU, as we are a third of the UK Safer Internet Centre.

Finally, we have a self-regulatory model, which means that we are able to work with the internet industry on a voluntary basis so that it can voluntarily remove content when notified. If we find content in the UK, we can have it removed in under two hours. We work nationally and mainly internationally—because a majority of the content is outside the UK—doing whatever we can to get that content removed. We do that with international law enforcement, other hotlines and the internet industry.

The Chairman: Thank you very much. Dr Saunders.

Dr Jamie Saunders: I am Jamie Saunders. I am the director of the National Cyber Crime Unit in the National Crime Agency. We are responsible for combating all sorts of serious crime, the most relevant for today being child sexual exploitation online. We also deal with computer misuse and offences, online fraud and the sale of illegal commodities, particularly on the dark web.

The Chairman: Thank you very much. Just to get that in perspective, you mentioned that there are 68,000 such cases. What does URL actually stand for?

Ms Susie Hargreaves: Each URL is an individual web page.

The Chairman: But what does URL stand for?

Ms Susie Hargreaves: It stands for uniform resource locator.

The Chairman: That is pretty obscure.

Ms Susie Hargreaves: Instead of taking a website down—we do not do that—we work with the internet industry, saying, "On that individual web page, which is a URL, you have child sexual abuse images". So we work with the industry to remove an individual web page.

The Chairman: Will the company to which you are addressing this requirement—in Latvia or wherever—instantly do as you request?

Ms Susie Hargreaves: In the UK they will. If we find content in the UK, we notify CEOP, which then gives us permission to issue a notice for take-down, which then goes to the company and it will remove it immediately. When we work internationally, we have to work with the appropriate organisation, whether that is their hotline or law enforcement. Until they remove that content—I am afraid that it takes a lot of time to have the content removed—we place that URL on our blocking list, or URL list, which is deployed across the whole world. We check that every day, and if the URL has been removed we will take it off the list. If we find new ones, we put them on. To give you an example, today there are about 2,400 URLs on our list. The list is very dynamic; it changes every day. Some URLs will be on there for a day, and some URLs on our list have been there for four years or longer.

The Chairman: Because they are coming from a country where you exert no influence.

Ms Susie Hargreaves: I guess so. We work very much with law enforcement in those countries.

The Chairman: They are ineffective. Jamie, in terms of the overall picture, are we seeing an increase in undesirable activity here or have we reached a plateau?

Dr Jamie Saunders: We are dealing with looking at victims—children who are being groomed or whose images are online—or we are looking at indicators that there are offenders in the UK. Both those figures are going up, and of course it is always difficult to tell whether that is because of greater awareness or because more people are coming forward. It is very hard to tell.

Q29 Baroness Benjamin: Under the general data protection regulation, the personal data of children under the age of 16 may not be collected unless consent is given by the parent or guardian. Do you think there is adequate knowledge and expertise in the enforcement agency to address the needs of children of different age groups between nought and 18? You mentioned how many children are found under the age of two. Is there enough?

Dr Jamie Saunders: We have access to a lot of expertise, including age-specific expertise, from social workers or child psychologists, who either work within law enforcement or can easily access law enforcement, so we have expertise that we can turn to. The main thing we do, which is protective security and advice, is very age-specific. In other words, it is targeted starting at five to seven year-olds and going up to 16 to 18 year-olds.

Baroness Benjamin: With the images you find of young children, are they aware of what they are doing and how those images have reached that point in the first place?

Dr Jamie Saunders: Whether the children are aware is very hard to tell. Each case is different.

Baroness Benjamin: You say that you deal with victims, so I thought that you had got to that point.

Dr Jamie Saunders: The first priority at that stage is safeguarding the child. Normally they are in an abusive situation and the priority is to get them out of that position. In some cases, it is obvious how the image has been taken. It might have been live-streamed, for example, which is an increasing trend that we are seeing. But generally we will first identify who the child is, and that is extremely challenging and difficult. Once the child has been identified, we consider what sort of safeguarding and intervention can be put in place. Then we consider who the offenders are and how to deal with them. They will be all over the world, of course.

Baroness Benjamin: It would be good to know how the information got on to the internet in the first place through knowing how the image was captured. Parents are then made aware so that they can tell their children, "This is what to look for". That is what I am trying to get at.

Dr Jamie Saunders: There are two categories. One is where a child is being abused and an image is being taken obviously without their consent because there cannot be consent. How it gets on to the internet is hugely important, because we want to understand how to trace the child and the offender. You may be referring to the situation where a young person has taken their own image, which has somehow got on to the internet. That is a point for education. It highlights the dangers to children who may be capturing their own images and sharing them by showing them what can happen when they get out of control.

Ms Susie Hargreaves: I absolutely agree with Jamie that child sexual abuse images that are shared on the internet by paedophiles is completely different from self-generated content. In the olden days that used to be selfies of kids sharing images taken on phones, but now we are seeing quite young children on webcams set up in bedrooms where it is clear that they are being coerced and groomed at the other end, but actually they are children unsupervised in their own bedrooms. Anyone with a camera-enabled internet device really should be given age-appropriate supervision in the bedroom. Those children are clearly vulnerable and are being coerced, because they do not necessarily know what they are doing, if you see what I mean. However, the majority of the images that we see are not self-generated in any way. They are images, taken by people, of children being sexually abused.

Baroness Benjamin: I visited a school yesterday and I was amazed at how many children still have computers in their bedrooms that they can use during the night. We need that kind of knowledge so that children can be made aware as well.

Ms Susie Hargreaves: Absolutely. I can cite a specific video I saw recently involving a child who we thought was around 10 years old. She was in a very nice, smart bedroom. We could see around the room. She was doing some of the most serious sexual things on the computer and we could hear the mother calling, "Tea is ready". Clearly the parents had no idea what was going on in their child's bedroom.

Baroness McIntosh of Hudnall: Perhaps I may say, Lord Chairman, that the question I was going to ask has been wrapped into the answers we have been given to the last question, because the distinction between self-generated images and images that are produced by adults specifically using children as victims is important. Equally, what new developments make it more likely that children will, whether they are aware or not, be vulnerable? You have just given us a very graphic answer to that question, which is that the sophistication of the technology enables them to do things without parental supervision that not only should they certainly not be doing but that can be made widely available. Moreover, they are technically self-generated.

Ms Susie Hargreaves: Yes, technically that is so. While they may be self-generated, that does not take away from the issue of grooming and coercion.

Baroness McIntosh of Hudnall: I am afraid that I have a view that you might like to take up with my colleagues, but is not the question of children as both perpetrators and victims quite a sophisticated analysis? In my view sexting is not a useful word, but it is the one that everybody uses. It is about young people themselves generating, sometimes for other young people, stuff that if it

gets out into the wider world is as dangerous for young people as anything that might be done by someone else.

Dr Jamie Saunders: Perhaps I may comment on that, because we have looked at it in terms of providing guidelines for the police. Obviously the legislation is not for us to deal with, but in terms of practice we would treat it primarily as a safeguarding issue and secondly as a perpetrator issue. That is the guidance for policing purposes. Yes, technically an offence has been committed and there may be circumstances in which there has to be some sort of law enforcement process, but the first priority is to treat the individual as a potential victim.

Ms Susie Hargreaves: I was going to respond to the technology question. While technology is abused by people using it to generate images, at the same time the technology industries are doing everything they can to develop new strategies to combat the problem. We work closely with the internet industry by looking at ways in which we can be ahead of the game and fight this kind of content. For example, the majority of images that we see are duplicates. It is quite rare for our analysts to see new children; nearly all the images are duplicates.

Let me give a specific example. In the summer I met a brave young woman in America. She was a victim who had been rescued at the age of 12. In the United States, you can opt in to being notified when anyone is caught with your images on their computer. She has already had 1,500 notifications of people being caught with her images, one of which had been viewed more than 70,000 times. The issue of duplicates is a massive one for us, so we are working with internet companies, in particular Microsoft, which has developed a package called PhotoDNA. We can put a digital fingerprint on an image and use it to work with the internet industry to search for the known duplicates not only through one company's services but on Facebook and so on. We also have the power to search the internet proactively. That is an example of how the technology is growing and how young people have access to it. They need to be educated so that they understand how to use it, but at the same time the industry is working with us and other organisations to tackle the issues.

Baroness Bonham-Carter of Yarnbury: Dr Saunders, when you described what you do, it sounded to me as though you had to cover quite a lot of ground, not only policing child pornography, which is what we are talking about. Are there enough people?

Dr Jamie Saunders: First, the structure of the NCA means that it has a number of commands and specialists for different functions. There is the CEOP command, which Susie referred to, which is dedicated to this job, while another team focuses on cybersecurity crimes such as hacking. Another team looks at online commodities such as firearms and drugs. The structure is good. There are capacity issues at the national, regional and local level of policing which I think have been well expressed, but we are now getting a better understanding of the volume. The evidence is that the number of referrals of an offender here in the UK is increasing, which places a significant load on chief constables. Police and crime commissioners are aware of this, and while there is still a gap significantly more resources are going into it.

I will say one other thing, if I may. It is getting harder, because while it is one thing to show that there is a digital clue for an offender or a victim in a particular

location, resolving that with a real-world identity so that you can make a physical intervention is getting harder for all the reasons that have been discussed in the context of the IP Bill, which I am sure you are all very familiar with.

Baroness Bonham-Carter of Yarnbury: But presumably—I will get to my question in a minute—there is a financial incentive for this horrible crime.

Dr Jamie Saunders: In some cases. We have done a strategic assessment of this and one of the trends that we have seen recently is live streaming. Effectively, children are abused to order for the visual gratification of individuals, often in the West and sometimes with the knowledge of their parents. With the children in the developing world there is clearly a desperate financial motivation. So globalisation hits technology hits vulnerable children. Poverty creates an incentive, but we do not think that is the main motivation.

Baroness Bonham-Carter of Yarnbury: But that is a route for stopping the dealers of this.

Dr Jamie Saunders: Money exists and it follows the line of opportunities.

Baroness Bonham-Carter of Yarnbury: And that is a route.

Dr Jamie Saunders: But not in all cases.

Baroness Bonham-Carter of Yarnbury: But you can follow that route.

Ms Susie Hargreaves: The NCA's work on perpetrators and live streaming is different from the work that we are doing, which is to go after the content. Of the content that we see, about 20% is what we would call commercial content, so it is behind a legitimate payment barrier that is abused—using a credit card payment, for example. The majority of content that we see—80%—is freely available on the internet. That is about behaviour and collectors as opposed to selling, which is more about organised crime.

Baroness Bonham-Carter of Yarnbury: You said, I think, that 80% of the victims are girls. I think that answers the question that I was going to ask you, which is whether being a victim of the crime affects boys and girls differently. In fact, that is a slightly different question, but this is obviously overwhelmingly about girls. The boys are equally victimised, I imagine, but I am not quite sure.

Ms Susie Hargreaves: There is no distinction between the severity of abuse of girls and of boys; it is just that there are more girls. We have a category in which we cannot tell whether they are boys or girls, depending on what the act is. The impact is not our area.

Dr Jamie Saunders: We see no difference.

Q30 Lord Gilbert of Panteg: Looking at legislation and the legislative framework, is current legislation appropriate and useful? Is any further legislation required, either now or to meet technical developments that you foresee? Dr Saunders, do you think that the internet industry is doing enough, or should there be further regulations or requirements of it?

Dr Jamie Saunders: Perhaps I could leave Susie to comment on the filtering side. On the investigation side, which is where we are focused, there are enormous challenges because of the changes in technology. Our view is that in order to sustain our ability to investigate, new legislation is required. As I said, that is being debated as we speak. The precise obligations to place on service providers in that context are the most debated aspect of the legislation. But the short answer is, yes, I think that more legislation is required.

Ms Susie Hargreaves: Legislation is a blunt tool, as is regulation. I think that we have some of the best legislation in relation to the work that we do. Many countries need to catch up; we are ahead in what we are trying to do to combat online child sex abuse. Where the legislation falls down is that there are perhaps some unintended consequences, particularly in the impact on older children—the 16 to 18 year-olds—who have found themselves in a potentially criminalised situation if they have been sharing images that are legally child sex abuse images. That should not be a consequence of the current legislation. We are all aware of it, including the police, and we are trying to resolve it. That is one area that is a bit shaky at the moment. Could the internet industry do more? Of course everybody could always do more, but the internet industry in this country does more than the industry in any other country. It totally steps up. We work really closely with it. We are always trying to bring industry members on board, but the industry will do what it can to work with us. It is not just that child sex abuse is bad for business, but industry members are people too and nobody wants to be associated with what is the very worst content on the internet. Yes, it could do more, but it really steps up and does a lot.

The Chairman: Are there any anxieties relating to Brexit, in that quite a lot of these issues are cross-boundary, right across the EU in particular? Will this make a difference? Are any of those measures in the pipeline EU measures rather than UK-based measures?

Ms Susie Hargreaves: Yes. We work under the EU directive. Child sexual abuse on the internet is borderless, so we have to work internationally. We receive about 10% of our funding from the EU and work closely with our EU colleagues and through the International Association of Internet Hotlines, INHOPE, which is based in Amsterdam and is funded entirely by the EU. Although we are coming out of the EU, we will continue to work with all these partners, because we cannot solve this problem on our own. One great thing that has been set up is a centralised database, held by INHOPE, which means that when we find content in France, say, we all push our content into that database. It is then pushed to the right country, which will deal with it accordingly. Even though we will not be in the EU, we will continue to work with them. We are sending out that message very clearly, because it is hugely important in relation to our work.

Dr Jamie Saunders: There are a number of instruments at that level that we use routinely. We will give the Government the information that they need on the impact of certain arrangements being stopped. We use these all the time. We think that they are an important priority in order to ensure that we can carry on doing our jobs once we have exited the EU.

Q31 Lord Allen of Kensington: I want to turn to data protection and cybersecurity, Dr Saunders. Although there are specific requirements on

providers in relation to children, the law does not seem to differentiate between protection of children's data and protection of adults' data. It was interesting to note recently the WhatsApp decision to share data—as you know, WhatsApp is very popular with children, as is its parent company, Facebook. Are young people sufficiently aware of that as an issue? If they are, does it cause any specific problems for under-18 year-olds in sharing their data? Clearly, you would imagine that companies such as Facebook would want that data for advertising purposes and so on, but I am trying to understand whether there is a bigger issue. I would welcome your views on that.

Dr Jamie Saunders: An issue that affects the whole population is the nature of the consent and the use made of data. As has been covered, there is a lot of developing law in that area. I would pull out two things. There needs to be child-specific assistance on what you should be doing and looking out for. We are certainly seeking to promote that in the child protection context in the Thinkuknow campaign, which is age-specific and looks at different needs. The other angle is the vulnerability of children's information, or anyone's information, that is stolen and the ease with which criminals, voyeurs and predators can break the security around data. Alongside sensible advice about how to manage your own data controls and privacy settings, there are also the basics, such as how to protect yourself from being hacked.

Q32 Baroness Benjamin: We have spoken a lot about the horrors of online sexual abuse and child sexual exploitation, but radicalisation to incite terrorism is also seen as a form of inappropriate material that is available to children. What role does law enforcement play in preventing young people becoming radicalised online? Are the current strategies effective? What information and experiences can you share with us as far as radicalisation is concerned?

Ms Susie Hargreaves: Obviously, we deal with child sexual abuse content and it is really important to us that that is exactly what we deal with. Our remit is very much inch-wide and mile-deep so we can work with people around the world because they are all on the same page on this issue. It means that we can work with the internet industry. People are interested in our work from a process point of view—how we do what we do—but on the actual understanding of the issue, I am afraid I have to defer to Jamie on that.

Dr Jamie Saunders: I am slightly embarrassed to defer on. I think you are seeing the Home Office as well. It is not a subject that the National Crime Agency currently covers. I do not have any way I can help you on that, I do apologise.

Q33 Earl of Caithness: The Chairman asked about Brexit and your influence. As a country that is part of a group with a population of 500 million, you have more clout when you say to somebody, "Stop it". Do you think it will make any difference, although you will work closely with the EU, when we are only 65 million or 70 million people?

Ms Susie Hargreaves: That is a very good question. When it comes to our relationship with other hotlines, no. Last year we accounted for 73% of all the data that went into the INHOPE database, so we are very much a needed partner in that. We also bring a whole range of industry partnerships that other hotlines in other countries do not have. But inevitably our influence at the

European political level will be different and diminished. We have been able to be at the heart of any policy developments and debate, although clearly that is going to change. But we will do everything that we can to make sure that we are still in that discussion, because we simply cannot deal with this subject by looking at the UK alone. Because we are so well resourced and the UK is so much at the forefront of tackling this issue, it would be hard for people to dismiss us because we were not part of the EU. But we will have to make sure that people are aware that we are into collaboration and partnership and we want to work with people. We may lose 10% of our funding but we cannot afford to lose those connections.

Earl of Caithness: A moment ago you said, "We're all working on the same page", but clearly some countries are not. Who are the baddies? Who are not working on the same page?

Ms Susie Hargreaves: Obviously, this is a global problem. The majority of the content is hosted in countries where the internet industry is, so it does not necessarily mean that they are particularly bad. An awful lot of the content is in the Netherlands or the States, because that is where the hosting companies are. We also see countries where the internet is developing at a huge speed where they just do not have the mechanisms in place, which is why we are part of WePROTECT, the international initiative founded by David Cameron to look at tackling child sexual exploitation in a very structured way. Our approach is not to name and shame; it is more to work with countries and help them build their capacity. We are working very closely with the NCA on this. The States used to be pretty bad at take-down. When we started, it used to take 20 days to get any content down in America. We have worked very closely with our American partners, the National Center for Missing & Exploited Children, and we now have an agreement where we can simultaneously alert the companies and law enforcement if content is there, which means that we can bring the content down within three days. It is really important that we work with countries rather than look at where the problem areas are. We do everything we can on that front.

Earl of Caithness: The philosophy you are expounding is very much what I would call the rich western world philosophy. Are people in the rest of the world with different cultures also following your line?

Ms Susie Hargreaves: A few years ago, we launched the IWF portal, so we now work with other countries to help them provide a reporting solution. We now have 16 reporting solutions around the world for countries that do not have hotlines. In fact, I will be going to India to launch one there on Monday. It is really important that we look at where we can put that support in so that there is somewhere to report to. India is a great example because it is beginning to tackle this problem. The population is huge. The problem is huge. The legislative needs and the law enforcement capacity needs are huge. We are helping it by putting one of those building blocks in place so that there is somewhere to report to. That is what needs to happen. All these countries are becoming aware that tackling child sexual exploitation is a fundamental building block to being a thriving economy. I am sure that that is the NCA's position on helping these countries.

Dr Jamie Saunders: The challenge is capacity building rather than political will, I think.

Earl of Caithness: So there has been quite a seismic change in some of the attitudes in the countries?

Ms Susie Hargreaves: Yes, and there is a long way to go. For instance, we do not say "child pornography" in the UK, we say "child sexual abuse". We are very clear. We call it child sexual abuse because it is an abuse of children. Pornography is a legal activity that happens separately. We do not want to minimise that and we have been working really hard to get that message across. One of the great things about this work is that even though there are countries that do not have the capacity, there are very few countries that would not be opposed to child sexual abuse. It is a work in progress, but in each country we are identifying champions and people who want to work with us. But there is a long way to go for very many countries.

Q34 Earl of Caithness: My final question is: how effective is children's ability to filter unsuitable material and what confidence do parents have in that? Is there a better and more effective way of doing it?

Ms Susie Hargreaves: The IWF has a blocking list, as I say, that goes out, and 98% of the UK is covered by our blocking list of live child sexual abuse URLs. This is not for children to filter; it is filtered at network level. The companies filter it. All domestic broadband is filtered. To get the family-friendly sign, all public wi-fi has to have our list. It is deployed at that level. Our list is deployed by Google across the world, and many other organisations. Filtering will stop people from accidentally stumbling across child sexual abuse. Filtering and blocking will not stop the determined. The best way to deal with this content is to remove it at source, to issue a notice and take it down. We see it as a preventive, disruptive measure, but it will never replace removal of the content, education, awareness or any of those things.

Q35 Baroness Benjamin: It is often said that parents should educate, guide and protect their children from inappropriate online material, but not all children have that sort of parental guidance. What role do you think schools and the education system should play in safeguarding children in the digital world? What age should that start at, and should it be compulsory in schools right across the country?

Dr Jamie Saunders: Schools and other carers have an incredibly important role to play. That is something that we have really focused on. Earlier I mentioned Thinkuknow, which is very much a flagship campaign. It looks at a range of different ages and, school-wise, the penetration is pretty good. I think that altogether 3.5 million schoolchildren were reached last year. Obviously that is not 100% saturation, but the numbers are encouraging. The materials are there and it is helpful to get the message out that schools should be taking advantage of them.

Baroness Benjamin: At what age does it start?

Dr Jamie Saunders: Five. This is very carefully designed to appeal to certain age brackets, starting with cartoon characters for the youngest and going up to teenagers.

Baroness Benjamin: And what resistance do you find with the 12% of schools that have not taken this up?

Dr Jamie Saunders: I do not think that we are necessarily seeing resistance. To a certain extent we are producing or sponsoring the materials, and sponsoring a network that is there to promote the campaign. It is not getting 100% penetration, but I do not think that that is necessarily due to schools pushing back. I do not have evidence of that.

Baroness Benjamin: So is there a problem with schools not knowing that the material is available?

Dr Jamie Saunders: I think we probably need to do more to advertise it.

Baroness Benjamin: And that would come through you or, as far as the Government are concerned, the education system? Who needs to be proactive in making sure that every single school is aware of the excellent material that you are putting out?

Dr Jamie Saunders: If there were to be mandation, that would be a matter for the Department for Education. That is not the route that we have taken so far; it has been promotion rather than mandation. Mandation may be required. That might be something that you would want to consider in your report.

The Chairman: Would you recommend it?

Dr Jamie Saunders: It would be helpful.

Baroness Benjamin: When you read some reports, it is clear that some schools do not feel that it is appropriate for a five year-old to know about this because they want to protect their innocence. Is that a case of, depending where the school is, the parents not being aware that the material that you spoke about at the beginning of your evidence is out there? Is it ignorance? Does the school think that it is perhaps not what the parents would like to happen?

Dr Jamie Saunders: That is a very valid point, and again that would affect any recommendation on mandation. Clearly, there is the question of what parents want. It is really not our position to judge which way it should go, but if they think, "We do not want this", that is a legitimate concern that would have to be taken into account. I have seen no evidence of that, but you are absolutely right that that could be the reaction of some schools. I am sorry to keep deferring to others but I think that that is something for the officials in the department.

Baroness Benjamin: May I push you a little further? Some schools have taken it up and are promoting it, but have you taken any evidence about why they decided that it was important for them to promote this material?

Dr Jamie Saunders: Again, I apologise, but I am not aware that we have done an in-depth analysis of why things have been taken up with enthusiasm or not taken up at all, or somewhere in between. But I agree that if we are to aim to raise the level of penetration from the current level to much closer to 100%,

even if 100% is not achievable, then some further research in that area would make a lot of sense.

Baroness Benjamin: Because as we speak there could be children who we are not aware are being affected.

Dr Jamie Saunders: Absolutely.

Ms Susie Hargreaves: Our work concerns not harmful content but criminal content. We need to be absolutely clear that the issues around age verification and access to that content do not apply to our work. The overlap between the general internet safety rules and what we are doing is obviously around sexting and self-generated work. From our perspective, because we are seeing younger children becoming involved, that messaging needs to happen earlier. The NSPCC did a lovely campaign with the PANTS rule. Those sorts of messages are really important and need to start with children when they are as young as possible. As I said before, children need age-appropriate access to the internet—if they have a camera in their bedrooms, for example. In fact, that is nothing to do with us; it is about education. It is about awareness and working with parents, and the younger the children the better, really.

Baroness Benjamin: How do you recommend that we put that in our report regarding the Government taking responsibility for making schools aware of the material that younger and younger children are watching?

Ms Susie Hargreaves: As I said, the NSPCC video on the PANTS rule is pitched at very young children. There is no reason why it, and resources like it, cannot be shown in primary schools. There are ways in which specialists can broach the subject sensitively. Children need to be aware of the dangers so that they can build their own digital resilience and their own safety, even when they are quite young. We see very young children now, and they are getting younger.

Q36 The Chairman: You have covered a lot of ground. We have looked at schools and the things that parents need. Do you have any final thoughts about things that we have not yet tackled you on but which we ought to understand better? Please share anything that we have missed.

Earl of Caithness: While you are thinking of the answer to the Chairman's question, perhaps I may pose another one for you. In your brief, Susie, you say that you monitor trends in young people's use of online platforms. What trends are worrying you and, putting your eyes to the crystal ball, what is the trend for the future that we need to be aware of?

Ms Susie Hargreaves: Basically we monitor the trends in relation to material that we have seen. We also look at which companies we should work with. The issue of apps is hugely important to us. We are constantly looking at ways to engage with the new technologies. We work with app providers and find ways of helping those companies build their child online protection packages around what they do. The trends that affect us are technology-type trends. One of the most interesting things that we worked on—and we shared information with the NCA on this—is that there has been a perception over the last couple of years that all the content is on the dark web. We deal with what is on the open web. We deal with the dark web as well, but the majority of content that we see there

links to image-hosting boards that are available on the open web. The majority of the content is on the open web, so we need to work on ways to bring it down from there, rather than get totally focused on it in a different place. On trends and young people's behaviour, I guess the truth is that they are very tech-savvy and are becoming so at a younger and younger age.

Baroness Benjamin: What do you think is a cause of people wanting to access this type of material? Is it that they can do so themselves? You say that a lot of people are critical when you try to put a filter or a block on something. They say, "Well, there is always the dark web and people are going to find it". But now you are saying that it is out there in the open as well. What is causing the generation of this kind of material? Is it that people see something that is more openly available, so they know that they can do it as well? What do you think is the cause of all this?

Ms Susie Hargreaves: Obviously we are talking about people's behaviour and why they are interested in child sexual abuse images. Organisations like Stop it Now! and the Lucy Faithfull Foundation are experts in that field. From our perspective, we want to know when people first access that content, how they access it and the ways in which we can disrupt access to it. It is true that child sexual abuse images have always been available, but there has never been such a magnitude of them as there is now or with such ease of access. It is quite easy to find this stuff if you really want to. I do not think that people know enough about the motivations behind it. We know that a lot of people are looking at it, and there are all sorts of theories about why people look at it. Jamie might have a better view of this, because he is going after the perpetrators.

Dr Jamie Saunders: I guess that we are involved at that next stage of the process. If people view this material, that is an offence and they will be treated by a criminal justice process. The concern then is whether it is an offence that leads to other child abuse offences. The question is whether our interventions and how we deal with the image offences will help to reduce the risk of contact offending, for example. We come in at that next stage. Why people started and how they originally got there are in a sense issues before we get involved. Once they have done it, they are on our radar.

The Chairman: Are those final thoughts? Is there anything that we have missed?

Ms Susie Hargreaves: I just want to reiterate the point about not criminalising young people who, for some crazy reason, decided that they would take pictures of themselves naked and share them. It is about education, awareness, supporting young people and, from our perspective, putting the resources towards dealing with the serial offenders—the people who are going out there, sexually abusing young children and sharing the images on the internet. They are not 16 year-olds in schools.

Baroness Benjamin: Has there been an increase in the number of young people who do not realise that it is a criminal offence to share that kind of material? Have you seen people being prosecuted or have people come forward having realised the extent of their innocent act—that is, innocent in their heads?

Ms Susie Hargreaves: About two weeks ago the NSPCC published some research showing an increase in the number of arrests of people under 18 for that offence. It is certainly a conversation that we have regularly with the police. I think we are all aware that it is not a great use of resources. No one wants to go after and criminalise a 17 year-old. We need to put the resources into going after the bad guys. That is one of the perverse consequences of the legislation that we have in place now. We want to support young people and enable them to deal with this. We are working with our partners in looking at ways in which we can help them reduce the number of images, because we do not want people's lives to be affected for ever.

Dr Jamie Saunders: On the question of whether we can get 100% penetration, as we discussed in the previous debate, I think that there can be more general education about online safety through schools, parents and other carers. In that regard, child sexual abuse is very significant. There are other issues, such as fraud and the security of personal data. More can be done to provide that as part of PSHE education in schools, for example. We are not where we need to be on that.

Baroness Benjamin: And what about the media?

Dr Jamie Saunders: I hesitated because it depends what you mean by the media. Kids are not watching lots of telly.

Baroness Benjamin: I will give you an example. A 10 year-old boy raped a four year-old girl. We have gone over that. The four year-old girl was told by the 10 year-old boy, "I'm going to rape you and you're going to like it", so every time there is a news report about a woman who has been raped, the four year-old girl asks her mother, "Did she like it, mummy?". Should the language of the news reports be sensitive when very young children have had that experience? The person saying it might not think very much about it but, as you say, there is an increase in the number of people who have been abused and have had that experience. Should the media be more engaged in this conversation as well? Perhaps a more holistic view is needed. Do you work at all with the media?

Dr Jamie Saunders: The language that we use is incredibly important. We work a lot with the mainstream media in publicising this issue, and we are extremely careful about the tone and the language that we use to describe things. The example of not using the words "child pornography" is a very good one. We are very careful about the language that we use. Of course, you can lead a horse to water, but we are extremely careful in our use of language and how we describe things. You are right: it is a very important part of dealing with this.

The Chairman: Final word, Susie?

Ms Susie Hargreaves: We get a lot of support in terms of the media because it is an issue that people want to cover, particularly in the news. They want to hold people to account if they feel that not enough is being done. That is really important to us. There is a perception that this is a victimless crime because the pictures were taken ages ago, but there is a real child at the heart of all these images. Every time someone looks at the images or videos, they are victimising that child. We are trying to get that message across again and again. We find

that people are sensitive to that message. We work together very closely to ensure that people do not forget that they are real children at the heart of every single image.

The Chairman: Thank you both very much, and thank you for all the hard work you are doing, which sometimes must be quite distressing. Good for you, and thank you very much for joining us today.

Ms Susie Hargreaves: Thank you very much.

JAN Trust – written evidence (CHI0063)

Questions

Risks and benefits

1. What risks and benefits does increased internet usage present to children, with particular regard to:

i. Social development and wellbeing

Social development: Cyberbullying in its various forms is something all children and young people in schools we have presented to are aware of, though it is difficult to gauge how many of these have experienced it directly. However, in Bullying UK's recent national bullying survey,[248] 56% of young people said they have seen others be bullied online and 42% have felt unsafe online. It is a widespread concern in schools and can have significant effects on children – creating anxiety, depression and stress for the victims, and distracting them from their education.

Many of the children we have met in schools are hyper-aware of current world affairs, being familiar with the details of issues such as global terrorism and political instability in the Middle East. The ready availability of news on social media platforms means that young people today are perhaps more politically and globally aware than previous generations. 'Viral' and 'trending' news stories are as focused on recent bombings and ISIS as they are on celebrity gossip and the latest film releases. These topics are presented in concise bites of information on social media platforms and appear in and amongst updates from family and friends. Young people can no longer remain 'blissfully unaware' of global threats, which can result in a state of constant underlying anxiety – something perhaps illustrated by the increase of mental ill health amongst young people.

The risk to children and young people of being groomed by sexual predators or extremists are well documented. With regard to the latter our pioneering Web Guardians© programme has been designed to mitigate this problem by educating mothers about the existence and the perils of extremist online influences so they are able to safeguard their children from this danger.

ii. Neurological, cognitive and emotional development

Anxiety to maintain an impressive social media presence can lead to 'airbrushing' life, over concern with keeping up appearances and addiction to using phones to document activity – even personal life. Sharing emotions and mental health concerns can have positive effects, in building supportive communities, but equally can be extremely detrimental in exposing vulnerability to online predators (e.g. 'pro anorexia' communities, and online bullies, or 'trolls').

---

248 http://www.bullying.co.uk/anti-bullying-week/bullying-uk-national-survey-2014/

iii. Data security

Most children and young people we have spoken to in schools say they keep their social media profiles private. Nevertheless, there are different degrees of privacy – which they may not all be aware of. In addition, many children lie on social media accounts as to how old they are in order to create an account (the youngest age required to create a Facebook profile, for example, is 13 – yet many children amend their year of birth with few barriers to doing this).

2. Which platforms and sites are most popular among children and how do young people use them? Many of the online services used by children are not specifically designed for children. What problems does this present?

Anecdotal evidence from mothers and insight gathered from schools suggest that, in terms of visual platforms, Snapchat is more popular with younger children and teens, whilst Instagram is used by older teens. Facebook seems to be ubiquitous across all groups we have presented to. A large majority of school pupils and students we have presented to say they have a Facebook profile.

3. What are the technical challenges for introducing greater controls on internet usage by children?

The pace at which internet platforms change and adapt, and the abundance of methods for circumventing regulatory controls can render these controls obsolete almost as soon as they are implemented.
Moreover, many security measures are confined to the home: for example, controls linked to the home WiFi network. This issue was raised in one workshop by a mother who told a story of a friend who had restrictions on her home WiFi for her son, but her son would use public WiFi at the local Tesco to evade these restrictions.

Education

4. What roles can schools play in educating and supporting children in relation to the internet? What guidance is provided about the internet to schools and teachers? Is guidance consistently adopted and are there any gaps?

Schools vary considerably in terms of the level and quality of education about internet security. Some of the schools we have interacted with have run awareness sessions on extremism and how to protect against radicalisation, but others have not.

Many teachers are not aware of all the internet platforms, the ways in which these are used and what the differences are between them. It is difficult with this disparity of awareness and understanding between teachers and children for teachers to provide effective strategies in using the internet safely. New dangers are springing up all the time and it’s a challenge to keep up to date on these.

5. Who currently informs parents of risks? What is the role for commercial organisations to teach e-safety to parents? How could parents be better informed about risks?

We, JAN Trust are at the forefront in working with Muslim women and mothers to equip them with the education, skills and confidence to safeguard their children from online extremism.

Our experience with mothers in this community in particular gives the women a safe and confidential environment in which they feel comfortable to express fears without fear of judgement. To begin with when they join us, many of them are vulnerable, and not well integrated with wider society due to poor English, lack of confidence, financial deprivation, social isolation and lack of "know how" to get the best out of services and systems in Britain. Most commercial organisations would not have the insight and experience that specialist charities such as ours have accrued over many years in working with these communities. They would be less likely to be able to create the safe environment which is critical to gain the trust of the mothers. This trust is essential to alleviate their anxieties so they are able to get the best out of workshops and feel free to raise issues, and for these issues to be addressed appropriately and effectively.

In addition, speaking for JAN Trust in particular, our Director Sajda Mughal OBE regularly works with the mothers on our programmes and in running our workshops. We find they are inspired by her human story of her experience in narrowly surviving the London 7/7 bombings, and being the only known Muslim to do so. This gives us enormous credibility, which builds trust and enables us to make a genuine difference because the women are so much more receptive to learning. Our work with mothers is rooted in these tragic circumstances, and fuelled by passion, and the sharing of the lived experience of the marginalised Muslim communities we serve. This context is alien to commercial providers and in any event their prime concern will be to make a profit in delivering services.

Governance

6. What are the challenges for media companies in providing services that take account of children? How do content providers differentiate their services for children, for example in respect of design?

It is difficult to implement age restrictions in access to content, as many children are aware how to get round such restrictions. This leaves much of the internet completely open for children, exposing them to inappropriate content. Parents can instil controls on devices at home and WiFi servers at home, but as previously mentioned, these can be circumvented through using public WiFi or other devices.

7. What voluntary measures have already been put in place by providers of content to protect children? Are these sufficient? If not, what more could be done? Are company guidelines about child safety and rights accessible to parents and other users?

Platforms such as YouTube contain 18+ disclaimers on adult content, but these can be overcome by simply clicking a button to attest to being overage, even when the user is younger than this. A more effective barrier to accessing adult content is required.

The parents we have encountered have not been aware of child safety and rights, and therefore these company guidelines must be signposted more prominently.

Legislation and Regulation

8. What challenges face the development and application of effective legislation? In particular in relation to the use of national laws in an international/cross-national context and the constantly changing nature and availability of internet sites and digital technologies? To what extent can legislation anticipate and manage future risks?

It is difficult to ensure the effective application of effective legislation as the internet is constantly evolving, and ways to circumvent legislation are therefore constantly developing. Keeping on top of the ways around internet regulation may prove to be impossible, particularly given the stateless nature of the internet (which transcends domestic law). Our approach at JAN Trust instead has been to encourage better and more effective education about the dangers of the internet for parents and teenagers, in order for young people to be empowered to protect themselves and parents to be aware of dangers.

9. What more could be done by the Government? Could there be a more joined-up approach involving the collaboration of the Government with research, civil society and commerce?

We are aware that our Web Guardians© programme for mothers has been highly effective in educating parents. Our schools workshops educate pupils of the dangers of the internet and providing preventative strategies before it is too late. Schools should teach internet safety and teachers should be provided with training and education as to what platforms are being used and how. Programmes such as our Web Guardians© programme for mothers should be supported long term.

Governments should compile and work with a register of preferred suppliers who meet certain criteria, e.g.

- Credibility with the Muslim Community
- Track record of delivering training, holistic support and innovative services for grass-root women in these communities
- Record of community involvement in shaping services
- Embedded within the communities being served, with representatives serving within the organisation
- Mechanisms in place for being kept constantly up to date with latest issues being faced by communities – e.g. growth of online extremist influences, increase in hate crime, tracking how world events are affecting community attitudes

Charities such as JAN Trust fulfil these criteria. Our award winning Web Guardians© programme is an example of our innovative approach. As David Cameron Former MP and Prime Minister said: *"I personally see this as an excellent example of the importance of community-led schemes in tackling extremism online."* Our youth are subject to significant online dangers including extremism and we expect this to continue. In our view it is therefore vital that such work such as our Web Guardians© programme with mothers continues long term.

Companies who have no/lack of experience on the issue of extremism particularly within the Muslim community should not be utilised. We can highlight one example of a company who actually were detrimental to the issue. The company an IT education firm partnered with a well-known countering extremism organisation to create a list of 'key words' that would cause concern if a student typed any of them into the school internet/intranet. This compiled list included some individuals who had no cause for concern and had no links to extremism or terrorism. In turn, this caused members of the Muslim community to question this work and they wanted an explanation as to why this happened as well as apologies to be issued. This type of work can damage community relations. Profit making companies are not best placed to carry out such sensitive type of work.

December 2016

Mike Johnston – written evidence (CHI0062)

1) I am extremely grateful to all the Members of this Committee for the unanimous voice in calling for much greater regulation of the internet for children against the rising tide of easy access to pornographic material.

2) I am also greatly indebted to Baroness Benjamin who encouraged me to write to the Committee on this subject, even though the deadline for submissions has passed some time ago.

3) As a father of 5 children and grandfather to 14 children, I am passionate as a Christian to preserve not only my immediate family, *but all children wherever they are in the world*, from this dreadful scourge which is corrupting the minds, defiling the affections and ruining the lives of children, and young people.

4) I do respect Government as ordained of God, and really the first responsibility is to protect the youth of this nation from these dangers by an effective mechanism that works. I am pleased to hear of the adoption of age verification as a means to verify the age of young people, who may deliberately or unwittingly try to access this material online.

5) Therefore the steps taken by this Government in a world leading initiative, are to be warmly applauded, and I will pray that you may fearlessly recommend the highest level of protection that is practical in this very critical matter.

6) Your intention that the BBFC should act as the Regulator on this issue is very welcome too, and this body should be granted enforcement powers to warn, shut down and prosecute websites who refuse to comply with the regulations. These sites who blatantly defy the law should be named, so the public can be made fully aware and avoid them at all costs.

5 December 2015

Dr Nihara Krause and Dr Marc Bush – oral evidence (QQ 98-107)

Transcript to be found under Dr Marc Bush

Dr Nihara Krause, stem4 – supplementary written evidence (CHI0061)

Key Points - Dr Nihara Krause, Consultant Clinical Psychologist, Founder and CEO, stem4

One in 10 young people aged 5-15 present with a diagnosable mental health problem. This means that there are around 720,000 children and young people between these ages experiencing a mental health problem in England.

Child and adolescent mental health services (CAMHS) are, on average, turning away nearly a quarter (23%) of children referred to them for treatment. This is often because the condition was not considered serious enough, or suitable for specialist mental health treatment

Children follow a typical developmental pathway to adulthood, which is a process that is linked with maturing physical, language, social, emotional and cognitive growth. With such growth there will be the development of attachment and trust, learning about cause and effect and consequences, emotional regulation, autonomy, self-discipline, abstract thought, risk taking and intimacy.

Children's use of the digital world has increased significantly over the past ten years. This increase has meant that children are self-led in their ability to explore the online world.

Children and young people enjoy the positive social and emotional benefits the digital world offers them. Some of the benefits include feeling socially connected, being informed, having peer support, feeling their problems are shared and to learn more about themselves and the world.

However, the interaction between the digital world and developmental factors such as difficulty in emotional regulation, limit setting, thinking through the consequences of actions, impulsivity and peer pressure can lead to increased risk affecting mental wellbeing.

There is growing evidence that children who use the Internet for over three and a half hours per day present with increased anxiety, conduct disorders and depression. There is also report of shorter attention span. There are also a number of sites that support and encourage negative behaviour including suicide, self-harm and eating disorders. There is some documentation of Internet and Gaming addiction but research is on-going.

Dr Nihara Krause, stem4 – supplementary written evidence (CHI0061)

Some risks associated with the digital world include exposure to inappropriate sexual images, exposure to values that are negative such as radicalisation and to temptations such as gambling, gaming, pornography and shopping.

Some digital platforms are introducing blocking functions and reporting functions. However, these developments are still in their infancy.

It is important that children are taught to use digital media responsibility and are also encouraged to learn to self-regulate use. Increasing empathy and social competency, self-worth and good communication will provide children with tools they can use to protect themselves in their digital use.

It is also important that parents are kept up to date on developments in digital media and encouraged to help their child use technology responsibly.

It is essential that changes involve collaboration between all those concerned including those in government, the digital industry, education, the voluntary section and children themselves.

December 2016

Professor Derek McAuley and e-Safe Systems Ltd - oral evidence (QQ 37-43)

Transcript to be found under e-Safe Systems Ltd

Emily McDool, Philip Powell, Jennifer Roberts, Karl Taylor, Department of Economics, University of Sheffield – written evidence (CHI0008)

Written evidence to be found under Philip Powell

Mary McHale and Karl Hopwood, esafety Ltd – oral evidence (QQ 52-60)

Transcript to be found under Karl Hopwood, esafety Ltd

Dr Sarah Marsden and Dr Akil Awan – oral evidence (QQ 122-128)

Transcript to be found under Dr Akil Awan

Mayor's Office for Policing and Crime – written evidence (CHI0048)

I welcome the House of Lords Select Committee on Communications inquiry into *Children and the Internet*.

In the vast majority of instances the use of the internet is positive, but we need to ensure that children are aware of the dangers. This is an issue which is of considerable concern to me as Deputy Mayor for Policing and Crime for London. Both I and the Mayor have been clear that all children and young people should have the same opportunities to enjoy and achieve. The advent of the internet has both enhanced those opportunities but unfortunately brought with it new risks and threats.

We are witnessing evolving crime categories and child safeguarding issues which police and other public services must keep pace with. As you may be aware, the Mayor committed in his manifesto to develop a cyber-security strategy, led by a Chief Digital Officer, to work with the police and security services to ensure that Londoners have the information and resources they need to stay safe online. Your inquiry comes at a particularly timely moment for London, as the Mayor develops his Police and Crime Plan, which will include a strong emphasis on these issues and how we can take this work forward.

The Mayor's Office for Policing and Crime (MOPAC) has responsibility for oversight of policing in London. This includes specific statutory obligations to hold the Commissioner of the Metropolis to account for the exercise of duties in relation to the safeguarding of children and the promotion of child welfare. MOPAC funds the London Safeguarding Children's Board and commissions a range of services, which increasingly have an online dimension. MOPAC are also currently in the process of establishing an online hate crime hub to specifically tackle online hate crime.

Throughout MOPAC's areas of work, MOPAC are identifying concerns in relation to child safety on the internet in relation to online radicalisation; cyber bullying; grooming and child sexual exploitation; gang crime and online hate crime. Addressing online facilitation of crimes and online vulnerability will be a key priority as we develop the Police and Crime Plan for London.

Online Radicalisation

The Mayor has committed to leading a renewed push to tackle extremism and radicalisation in London, promoting the integration of different communities, and supporting and empowering communities in speaking out and challenging extremism. The Mayor and I are very conscious of the importance of tackling online radicalisation as part of these efforts. I jointly chair the London CONTEST Board, the mechanism that works with partners to support the implementation of the Government's counter-terrorism strategy in the capital and as the Mayor develops his Police and Crime Plan, we will be looking specifically at prevention strategies.

The Counter Terrorism Internet Referral Unit (CTIRU) was set up specifically to tackle illegal terrorist and violent extremist content on the internet.

The Counter Terrorism Internet Referral Unit (CTIRU) proactively searches for and requests the removal of content, which glorifies and seeks to incite people to commit acts of terrorism and works directly with service providers to instigate the removal of this material. It also responds directly to referrals to the public and the Mayor and I would encourage anyone who comes across terrorist or violent extremist content online to report it via the following website: https://www.gov.uk/terrorism-national-emergency/reporting-suspected-terrorism

Cyber Bullying

'Cyber-bullying' and 'revenge porn' are also evolving areas of concern. Where this amounts to a criminal offence and online harassment, the Metropolitan Police Service (MPS) will take appropriate action. There is relatively little data in this area, including data relating to young people as these incidents are covered by a plethora of existing criminal offences. These include Section 33 of the Criminal Justice and Courts Act 2015, which creates the offence of disclosing private sexual photographs and films with intent to cause distress; Section 1 of the Malicious Communications Act 1988; Sections 1 and 2 of the Protection from Harassment Act 1997; Sections 2A, 4 and 4A of the Protection from Harassment Act 1997 in relation to stalking; Section 21(1) Theft Act 1968 in relation to blackmail or the offence of coercive control under the Serious Crime Act 2015.

The Mayor and I are extremely concerned by incidents of this type and recognise the need to work with the MPS to capture more information on this issue so that we can work with schools, parents and partners to help prevent and promote greater awareness of these issues.

I welcome the work of the UK Council for Child Internet Safety and other partners in consultation with the National Police Chief Council (NPCC) in producing their guidance ahead of the new school term, 'Sexting in schools and colleges: responding to incidents and safeguarding young people', which includes advice about notifying the police .

Grooming and Child Sexual Exploitation

The utilisation of social media and the internet to facilitate grooming and child sexual exploitation has been well documented. Like other sexual offences, especially those committed against children, it is highly likely that such offences are significantly under-reported.

MOPAC and NHS England, London region, have jointly commissioned MBARC, an independent consultancy, to deliver a Sexual Violence and Child Sexual Exploitation needs assessment for London (a part of which will cover online issues), which will inform the way in which future services funded by both organisations can best meet the needs of victims/survivors post 2016/17. The needs assessment will consist of two core parts; Sexual Violence and Child Sexual Exploitation with the focus in the latter part being peer on peer abuse.

This two part assessment will enable a detailed overview of the journey of a victim/survivor of sexual violence ensuring the victims/survivors voice is at the forefront of future commissioning decisions.

The CSE Needs Assessment will incorporate data and identify needs related to Child Sexual Abuse and once this is published MOPAC will be happy to share key findings with the Select Committee.

Gang Crime

Gang videos being widely shared on YouTube and easily accessed on smartphones means that social media is used to recruit young people into gangs, taunt rivals, and can result in escalating violence. This is an emerging issue and few local areas have the resource or infrastructure to monitor the use of social media. Some London boroughs have invested in multi-agency Integrated Gangs Units which include dedicated resource to analyse the use of open source material such as social media to improve the understanding of gangs.

MOPAC have recently commissioned the Institute for Community Safety to continue the work of the erstwhile Home Office Ending Gang Violence and Exploitation front line team, who visit boroughs and undertake local area assessments on the response to gangs, youth violence and exploitation locally. Nine local reviews will take place over the next 12 months and these will be targeted on areas that boroughs feel they need most support with. It is expected that these will include addressing issues relating to gangs and social media.

Online Hate Crime

The Mayor and I are aware of the increasing role that online hate crime can play in making individuals and communities feel vulnerable and targeted.

Tell MAMA estimates that 75% of its reports are of online hate crime (402 in 2014/5)[249] and the Community Security Trust reports 20% of anti-Semitic offences reported to it are social media related (473 to June 2015)[250]. TruVision data also indicates approximately 1500 online hate crimes per year, 1000 traceable to the MPS area.

We are very conscious of the need to strengthen the police response to online hate and better equipping police officers to deal with it. It is not acceptable that perpetrators can hide behind a veil of anonymity and make individuals and whole communities feel targeted.

In order to trial a new approach to tackling this problem, MOPAC and the MPS are establishing a two year proof-of-concept programme providing an Online Hate Crime Hub. This will be a dedicated police resource to detect and respond to online hate crimes, and assist in training police officers and community groups in how to identify, report and challenge hate material online.

---

249 TELL MAMA, 2014/2015 Findings on Anti-Muslim Hate, June 2015

250 Community Security Trust, Antisemitic Incidents Report January-June 2015

It is also important to work closely with schools. The Mayor has already written to schools offering any assistance they may require in taking a stand against hate crime and MOPAC are currently exploring ways to build on the hate crime awareness-raising already underway in schools, and looking to see how we can support initiatives to provide counter-narratives to hate online.

I hope that this information is helpful to your investigation and I look forward to your recommendations. Please do not hesitate to contact me or my office if we can provide further details or be of any assistance to your inquiry.

1 September 2016

Microsoft UK – written evidence (CHI0050)

Children and the Internet Inquiry

Introduction

1. Microsoft welcomes the opportunity to respond to the Lords Communications Committee on its inquiry into Children and the Internet.

2. As a leading technology company, Microsoft has a responsibility to seek to create software, devices and services that have safety features, functionality and considerations built in from the outset. In addition, we devise and implement internal policies, standards and procedures that go beyond pure legal requirements in an effort to self-govern product development and content moderation with child and consumer safety top-of-mind.

3. Microsoft is also committed to staying abreast of the risks that individuals and families may face online; to alert consumers to such developments, and educate them about how they can help protect themselves and their families.

4. Perhaps most importantly, we encourage a "multi-stakeholder" model, and partner with others because no one entity or organization can successfully tackle these significant issues alone.

5. Microsoft works closely with the UK Government to promote child internet safety. Alongside our industry partners. For instance, we work in partnership with the Child Exploitation and Online Protection Centre (CEOP) and the UK Safer Internet Centre.

6. We have a number of tools that are available to help parents and teachers protect children online. For instance, parental controls are built into Windows and Microsoft devices.

RESPONSE TO CONSULTATION QUESTIONS

Risks and benefits

What risks and benefits does increased internet usage present to children, with particular regard to:

i. **Social development and wellbeing**
ii. **Neurological, cognitive and emotional development**
iii. **Data security.**

7. The Internet is an extraordinary tool that allows children to explore the world around them. While the Internet enables many beneficial experiences, it also exposes children to certain risks, including potential exposure to inappropriate content, contact with bullies or strangers, and the loss of privacy or identity.

6. One of the greatest challenges is ensuring that people of all ages and abilities have access to the tools, resources and educational guidance they need to help them stay safe online.

7. While we are acting to educate children about the potential risks of using the Internet, we have also invested significantly in aiding the benefits that it can bring, especially in education.

8. Microsoft worked with the Computing at School Group (CAS) and the British Computer Society (Chartered Institute for IT) to develop the Computing Curriculum introduced in England in Sept 2014. It is deliberately ambitious - world-leading - and represents a significant shift in what teachers are being asked to teach.

9. Microsoft, along with our partners, have also created, curated and shared resources to help teachers and schools to embrace innovation and implement technology effectively to support teaching and learning. Through these resources we can encourage better use of technology across all stages of education.

10. Part of this investment includes the deployment of new technology in the classroom, and teaching teachers how to use it. Good practice in teaching with technology not only supports learning goals, it also develops up to date digital fluency in students, and preparing them for the world they will enter, with the skills to continue learning for life.

Which platforms and sites are most popular among children and how do young people use them? Many of the online services used by

children are not specifically designed for children. What problems do this present?

What are the technical challenges for introducing greater controls on internet usage by children?

11. Online safety requires close and continued collaboration between industry, government and non-governmental organisations.

12. There are of course a number of technical challenges in introducing greater controls on internet usage by children, including the sheer volume of immediately available content.

What are the potential future harms and benefits to children from emerging technology, such as Artificial Intelligence, Machine Learning and the Internet of Things?

13. The modern computing era will be characterised by three key developments: i) computing interactions becoming more natural; ii) computing experience becoming more contextualised (i.e. Machine Learning); and iii) technologies working increasingly on our behalf.

14. Looking forward, emerging technology including the Internet of Things, Artificial Intelligence (AI) and Machine Learning, is projected to grow significantly. Accordingly, it will become increasingly important to ensure that society understands how they are interacting with these technologies.

15. Children are often the first to want to use emerging technologies, and many schools have not shied away from introducing such technology as teaching aids. By embracing such technology at an early age, we can help prepare our children for a successful future.

16. Microsoft is actively innovating in these areas. However, we are aware of the potential risks, which include data security, over exposure/ screen time, and exposure to harmful content in increasingly immersive contexts, and are working to mitigate them.

17. One of the ways we are achieving this is through the education and resources we make available directly to parents, schools and children across the UK. These resources are actively updated and reviewed, as the uptake of emerging technology increases.

Education

What roles can schools play in educating and supporting children in relation to the internet? What guidance is provided about the internet to schools and teachers? Is guidance consistently adopted and are there any gaps?

18. Microsoft works with parents, teachers and children to provide skills and training on becoming a good 'digital citizen'. We believe this means educating ourselves about both the benefits and risks of our online world, and then developing the habits that can help us stay safer there.

19. The Microsoft YouthSpark Hub[251] is one of the areas where we provide information for parents, teachers and children of all ages on how to stay safe online. This includes practical advice on good digital citizenship, online bullying, data security, and sexting.

20. We encourage teachers and parents to seize the opportunity to educate children while they are young to help them establish the good digital habits and skills they will need in order to deal with difficult situations, information and people they come across online.

21. Microsoft believes online safety lessons and courses should become an integral part of every school's efforts to achieve technological literacy for their students. Programmes should include modules that weave digital literacy and digital citizenship into the standard curriculum.

22. Just as students need education about safer internet use, teachers also need training to keep abreast of ever-changing technology. Teacher training should include updates on the risks of using the Internet, recognition of when students may be subject to online dangers, and guidance for helping students conduct themselves with civility on the web.

23. It is also important to recognise that there is a need to balance online restrictions with safety education. Restricting children's internet access may be appropriate in some areas, for example gambling and pornography – those areas that already have age restrictions in the physical world. However, safety experts agree that restricting access is not enough and that education plays a vital role in the safety of young people online.

---

251 YouthSpark Hub, Online safety for familes: https://www.microsoft.com/about/philanthropies/youthspark/youthsparkhub/programs/onlinesafety/resources/

Who currently informs parents of risks? What is the role for commercial organisations to teach e-safety to parents? How could parents be better informed about risks?

24. Parents face challenges when monitoring the content their children encounter online, the people they meet there, and what they share. Microsoft has built a number of safety- features, such as filtering, into our products and services to help parents minimise these online risks that their children can face.

25. Windows includes parental control features to help parents monitor, manage and administer their children's computer use and help keep them safe. The Family Safety Center gives parents two ways to limit the internet content their child can see. They can use web filtering to set broad categories of sites that they child can visit. For example, they might allow them to see known child-friendly and general-knowledge websites, while automatically blocking any sites that provide adult content. They can also allow or block individual websites by their web address or URL. When a parent turns on Family Safety for a child's user account, monitoring starts automatically. They then receive regular activity report emails from Family Safety, showing how much time their children spend on the computer, the websites they visit, the games and apps they use.

26. Microsoft also offers parents the opportunity to set limits on our search engine Bing by keeping sites that contain sexually explicit content out of search results using the SafeSearch settings of strict, moderate or off.

27. The Xbox 360 console lets users customise and manage their family's access to games, films and television content. The parental controls can be used to control the console itself and access to Xbox Live. Parental controls allows users to control features including which games can be played, which films and TV shows can be watched, and how long each family member can use the console on a daily or weekly basis. Parents can also change the online safety and privacy settings for the account or a manged dependent account to block or allow access to Internet Explorer or Xbox, determine who can see their profile and for parents, determine if approval is required to accept or send friend requests.

28. Education is also key in the protection of children. Microsoft has an extensive safety and security site which can be found at www.microsoft.com/safety and we have produced a number of useful documents for both parents and children, including:

a. Is your teen a good Digital Citizen?
b. Teach kids mobile safety
c. Protecting young children online
d. Producing "tweens" and teens online
e. Help kids stand up to online bullying.

29. In the UK we have worked with the education and skills arm of CEOP, the Child Exploitation and Online Protection Centre. Over 200 of our UK employees are trained to deliver CEOPs ThinkUKnow resources in school, and we also give presentations to parents.

Governance

What are the challenges for media companies in providing services that take account of children? How do content providers differentiate their services for children, for example in respect of design?

30. One of the challenges that media companies face is differentiating between when a child is using a device and when an adult is. Microsoft has therefore made it as easy as possible for parents and teaches to set up different accounts for devices, which can be adjusted where necessary.

31. The Family Safety Center gives parents the ability to monitor, manage and administer their children's computer use and help keep them safe. This includes allowing parents to differentiate between sites they may want their children to access, such as known child- friendly and general-knowledge websites, while automatically blocking any sites that provide adult content

What voluntary measures have already been put in place by providers of content to protect children? Are these sufficient? If not, what more could be done? Are company guidelines about child safety and rights accessible to parents and other users?

32. See above.

Legislation and Regulation

What are the regulatory frameworks in different media? Is current legislation adequate in the area of child protection online? Is the law routinely enforced across different media? What, if any, are the gaps? What impact does the legislation and regulation have on the way

children and young people experience and use the internet? Should there be a more consistent approach?

33. There are a number of different regulatory frameworks that govern different online protection issues. With regards to grooming, there is the Malicious Communications Act 1988 and the Communications Act 2003. For cyber bullying, there is the Education Act 2011, which allows teachers to look for and delete inappropriate images or data from electronic devices such a mobile phones. And for data security, there is the Data Protection Act 1998, and its soon to be successor, the General Data Protection Regulations.

34. Addressing the challenges of online safety requires global collaboration between the technology industry, governments and non-governmental organisations. It cannot be achieved by national government, in silo.

35. Following the UK's recent vote to leave the EU, we would emphasise the importance of ensuring harmonization of regulation with the rest of Europe.

36. Governments should address the risks to children online through transparent and harmonious content regulation, which will then allow for internet companies to manage inappropriate material through content moderation. When creating such regulation, governments must consider how best to balance free expression, privacy and public safety.

37. In the case of illegal content, governments are in the best position to strike the correct balance among their constituents' competing values, rights and interests, such as privacy, freedom of speech, and public safety.

38. If governments seek to ensure that internet companies remove certain types of violent, hateful or extremist content from their online services, governments should legislate those requirements.

What challenges face the development and application of effective legislation? In particular in relation to the use of national laws in an international/cross-national context and the constantly changing nature and availability of internet sites and digital technologies? To what extent can legislation anticipate and manage future risks?

39. Microsoft believe effective legislation should be based on six key principles:

1. Legal clarity: Legislation should clearly define what content is illegal and government officials should specify which types of online services must remove it.
2. Notice and Takedown: "Notice and takedown" remains the appropriate means for companies to address objectionable content on their services. There are significant technical, policy, subjectivity and resource barriers to proactive monitoring.
3. Proportionality: Legislation should specify that takedown notices must narrowly specify the service and precise location of illegal content so as to prevent removal of legal content, and notices should be detailed enough to enable efficient review of the request and implementation.
4. Remedy: Affected content publishers should be given a fair and efficient process to appeal and seek reversal of content removal requests that they believe are unwarranted.
5. Transparency: Governments should be transparent about the content removal requests that they send to online service providers.
6. International Norms: Most importantly, any legislation directed at content takedowns should be consistent with international standards, including those on due process and human rights.[252]

40. The WeProtect Global Alliance is one of the best examples of how the above principles have been brought together to create the Statement of Action to bring an end to child sexual exploitation and online abuse, in addition to our own contributions and innovations to the broad global effort, to best protect our children in the digital age.[253]

Does the upcoming General Data Protection Regulation take sufficient account of the needs of children? As the UK leaves the EU, what provisions of the Regulation or other Directives should it seek to retain, or continue to implement, with specific regard to children? Should any other legislation be introduced?

41. There are a number of child-specific provisions in the GDPR, particularly regarding processing and notices. Children are also identified as being "vulnerable individuals" who are deserving of "specific protection".

---

252 *Content Regulation*, Cloud Initiative Project, Microsoft.

253 Microsoft Blogs, *WePROTECT Global Alliance releases strategy to end child sexual abuse online*, (July 13, 2016): http://blogs.microsoft.com/on-the-issues/2016/07/13/weprotect-global-alliance-releases-strategy-to-end-child-sexual-abuse-online/#sm.0001ejz2jka1uey9w7g2edcadlzqe

42. The GDPR also stipulates that where online services are provided to a child, consent must be given or authorised by a personal with parental responsibility for a child. This requirement applies to children under the age of 16 (unless the Member State has made a provision to lower that age).

43. Whilst these provisions make good headway in protecting children online, Microsoft believes that education remains key.

What more could be done by the Government? Could there be a more joined-up approach involving the collaboration of the Government with research, civil society and commerce?

44. Microsoft has an established reputation for protecting children – and, indeed, all individuals – online. However, no one entity or organisation alone can solve child online safety and protection issues.

45. Online safety is a community challenge, and it is important that the Government and industry work together to establish and implement online safety principles. This must include comprehensive global initiatives to protect children and young people online, by creating holistic approaches involving parents and children, educators and trusted adults, and a variety of public and private sector entities, including government, law enforcement, NGOs, and tech companies.

September 2016

Poppy Morgan – written evidence (CHI0035)

I am Poppy Morgan, aged 11. My grandfather took nine questions for me to answer from the Committee's information, but all the answers are completely my own. I didn't have any help or suggestions about what I should say to the Committee. This submission is from me as an individual.

What are the benefits of the internet for children?

1. We can use the internet not only for educational purposes but for finding out new words.

2. Occasionally playing games.

3. You can get answers almost instantly without having to give yourself numerous papercuts flipping through heavy books.

4. You can communicate with other people and send pictures of something funny your pet did.

5. Also where would you be trying to research the Aztecs in a school with an awful library?

What are the concerns or bad things about the internet for children?

6. You never know where a dodgy website can lead you or who you're messaging, only who they say they are.

7. Pop ups which don't have an 'x' button always lead to trouble.

8. Online games that demand money.

9. Scary, inappropriate or upsetting pictures.

10. You don't always know where you could end up.

How can the internet be made better for children?

11. The internet could be made better by introducing a new way of searching something.

12. More child friendly websites.

13. Games that people won't want to play all day long.

14. Games that will inspire people to get outside or read a book.

15. Maybe easier to use for young children with simplified versions of Google.

16. Less interference from advertisements and popups.

In what ways do you think using the internet affects children?

17. It affects children in mostly a good way. However there are a lot of people I know know who go and play games on the internet as soon as they get home from school. My little sister when she was a toddler tried to swipe along the screen of the TV to change the picture so we do have some high tech gadgets but the internet still has opposite effects.

How can the internet be made safer for children to use?

18. More schools have blocks, but there are still some good websites so people aren't temped to hack.

Is there one new law you'd like Parliament to pass about children and the internet?

19. Maybe that there should a rule about the amount of time spent on the internet. Not every day and not more than 1 hour I think.

What do you think about computers and machines increasingly being able to think for themselves and learn to do things on their own, rather than just carrying out the instructions humans have given them?

20. I think it's fantastic and it opens up new possibilities. However it is a little disturbing and them being able to think for themselves is quite strange and worrying. It's good for the people around them, but how lazy will the human race become and how will we evolve and end up?

Is there anything you wish schools would do (or stop doing) to do with the internet?

21. I think things like YouTube and Wikipedia should be blocked in schools because there is a website that can be accessed through both and contains rude and inappropriate text and I'm sure there are plenty of others too. There was someone in my class who used it until it got found out.

22. However it is annoying when you search 'crab' for a school trip to the seaside and every single website is blocked. It would be good if simply things like that weren't.

How would you like this sentence to end … "When using the internet, every child has the right to …"

23. 'When using the internet, every child has the right to research anything and everything they want within reason'.

26 August 2016

Abhilash Nair – written evidence (CHI0037)

Lecturer in Internet Law & Deputy Director, Centre for Internet Law and Policy, University of Strathclyde, Glasgow

Children and the Internet

1. I am responding to the call for evidence in my capacity as an expert on internet law and regulation. Specifically, I have expertise in the regulation of illegal content and internet pornography and children's rights in this context. I have published widely and collaborated with leading international organisations in the area of regulation of child pornography and child safety online. My research monograph which examines the legal issues and policy challenges in the regulation of internet pornography is soon to be published internationally.

2. I am only commenting on the legislative and regulatory aspect of the inquiry, focusing on two specific issues within this sphere. The first is in relation to child pornography laws currently in place in the context of self-produced sexual imagery of children, and the second relates to the mandatory age verification proposal under the Digital Economy Bill 2016 currently passing through Parliament. I would also add that I would be happy to give oral evidence to the Committee if this was of use.

I. 'Sexting':

3. 'Sexting' commonly refers to the process of sending naked images or sexually explicit photographs or messages using mobile phones. Typically this would involve partners in a relationship consensually sending private images to the other person, although there is potential for redistribution of such images which is addressed further below. There is evidence to suggest that 'sexting' has become commonplace among adolescent relationships and is part of the 'growing up process'.

4. The UK currently has one of the most robust set of legislation in the world for combating child pornography. UK law makes it an offence to make, distribute or possess all forms of child pornography. The various pieces of legislation that created these offences were enacted with the primary objective of protecting children from abuse and exploitation. The law, however, does not distinguish between child abuse images created by adults, and images that are self-produced by children themselves. For instance, if a girl who is 16 takes and sends a sexually explicit image of herself to her 17 year old boyfriend, a proper interpretation of the law (s 1, Protection of Children Act 1978), would mean that the 16 year old girl has committed an offence of creating child pornography. The boyfriend

would be committing an offence of possessing child pornography (s 160 Criminal Justice Act 1988), and possibly also of 'making' child pornography depending on how it is stored in light of the wide interpretation of the term 'making' applied by the courts in cases like *R v Bowden.*

5. The law in this respect is arguably inconsistent with the realities of modern life. Current child pornography laws were enacted at a time when internet enabled mobile phones were not around. The possibility of adolescents producing self-generated sexually explicit images using mobile phones could not have been envisaged at that time. The intention of the law was primarily to prevent the abuse of children by adults, given the producers of child abuse images would almost invariably have been adults. The situation has changed now, and as noted above, 'sexting' is widespread among young people especially within adolescent relationships.

6. It is unfathomable that a law that was enacted to protect children from deviant adults could now be used to penalise the very children it is seeking to protect. In cases where both the sender and recipient are within the age group of 16-18, it also creates a rather preposterous situation: the law permits them to have sex (the age of consent being 16), but at the same time they would be committing a criminal offence if they send each other a sexual image of themselves.

7. The law does provide a defence for those who are married or have lived together as partners 'in an enduring family relationship' (s1A (1) Protection of Children Act 1978), which would protect some adolescents, but the vast majority are unlikely to be covered under this defence. The evidence of the extent of sexting among adolescent children speaks for itself: we are talking about what has become essentially normative behaviour among young people, and not all of them would be married or living together. Therefore, the law as it currently stands would criminalise the behaviour of a number of adolescent children that could be dealt with in more efficient and alternative ways rather than by legislation.

8. The CPS Guidelines on Prosecuting Cases of Child Sexual Abuse stipulate that care should be taken with respect to cases involving children, and that it 'would not be in the public interest to prosecute the consensual sharing of an image between two children of a similar age in a relationship'. However, this still leaves room for uncertainty and agony for the victim. Prosecutorial discretion does not eliminate the fundamental problem with the substantive law; it is simply an ad hoc mechanism to mitigate the harshness of the law. In my view, it is about time to revisit our legislation and consider a carefully drafted defence to Section 1 of the

Protection of Children Act 1978, so that the law that is essentially designed to protect children is not used as a blunt instrument to incarcerate them.

'Revenge Pornography'

9. Another significant drawback of existing law is that it makes it very difficult for someone under 18 who is the victim of 'revenge pornography' to report it to the police. Re-distribution and publication of private sexual images without obtaining the consent of the subject of the image (usually occurs when the relationship break downs), commonly referred to as 'revenge pornography', has recently been criminalised in England and Wales through s 33 of the Criminal Justice and Courts Act 2015 ('Revenge pornography' is criminalised in Scotland through the Abusive Behaviour and Sexual Harm (Scotland) Act 2016). Whilst this appears on the face of it to have solved any risks for children stemming from 'sexting', by the potential for misuse and redistribution of the images, a fundamental issue seems to have been overlooked.

10. Taking the example above of a 16 year old sending her naked picture to her boyfriend of 17, if the latter redistributes the image without her consent, there is really no incentive for the girl to report it to the police. A strict application of the law would mean that the girl could also be prosecuted for the offence of 'making' child pornography. In fact, by reporting to the police the girl would be essentially making a 'formal request' at her own peril for a crime to be recorded against her name. Since the introduction of the new Home Office 'Outcome Code 21' in January 2016, the police now has discretion to record that a crime has taken place but that they chose not to take further action as it was not in the public interest, but there is no guarantee that this will not be revealed in an Enhanced Criminal Records Check. The incident will remain on the record as a 'crime' and the child involved will be listed as a 'suspect'. The law ought to recognise the context and consent issues in such cases and should clearly differentiate between the victim – in this case the sender of the image –and the perpetrator who is the recipient who has re-distributed without the sender's consent. Whilst the latter should remain an offence (as per the 'revenge pornography' legislation), the law should not penalise the victim who sent the image within a relationship on the basis of trust. There is no need to leave this to the discretion of the police or the CPS when a simple amendment to legislation can resolve the problem, thereby avoiding further distress and uncertainty to the victim.

11. Whilst child pornography laws exist for a range of legitimate and pressing reasons, there are some limited circumstances where appropriate defence must be offered. A number of other jurisdictions including in the US and

Australia have already amended their laws by effectively providing a defence for consensual self-generated imagery shared between two children in a relationship. Similar amendments should be made to our child pornography laws in order that children who are victims of a crime can be supported rather than penalised or threatened with criminal sanctions.

II. Digital Economy Bill 2016 – Mandatory Age Verification

12. The second issue I would like to comment on is regarding the relevant provisions contained in the Digital Economy Bill which requires commercial providers of pornography to introduce age verification to prevent children from accessing their content. I support the position that the government has a duty to ensure that children do not have unfettered access to adult content on the internet: this is already the case in the physical world and it should be no different in cyberspace. The nature and variety of pornography available on the internet is such that it could potentially distort children's understanding of sex and healthy relationships and therefore poses a *risk* of harm to children. Lawmakers have a responsibility to respond to the threat so as to ensure a safe and healthy environment for children in cyberspace, while at the same time not compromising on the benefits and opportunities the internet offers them.

13. The proposed law requires commercial providers of pornography to verify the age of consumers in the UK. Whilst this is a good step in principle, I have serious concerns about the current enforcement model proposed. The current plan to target payment providers might solve part of the problem where such advertising revenue from the UK is a significant income for the content provider/host, but it will not have any impact on the numerous websites that do not operate under this model. The proposed model might reduce the number of pornographic sites that can be accessed without age verification, but children will still be able to access pornography through other sites. The purpose of the law ought to be to *prevent* children's access to inappropriate sites, not simply to *reduce* the number of websites available to them.

14. It should be remembered that a vast majority of adult pornography on the internet originates from the US. The right to free speech under the First Amendment to the US Constitution is generally broader than the right to freedom of expression under Art 10 of the Human Rights Act 1998 in the UK. Similar legislative attempts in the US (Communications Decency Act 1996 and the later Child Online Protection Act 1998) twenty years ago to regulate adult pornography with the intention of preventing children's access were unsuccessful following the courts striking down the relevant provisions as being unconstitutionally overbroad. Consequently, it is

highly unlikely that a UK law that regulates adult pornography that is lawful for adult consumption will be enforceable in the US (adult pornography would normally come under protected speech, except in its extreme and obscene forms, as judged by local standards).

15. Any regulatory attempt from our end therefore needs to focus on stakeholders within our jurisdiction and the only way to achieve this is to bring UK based ISPs within the regulatory framework, requiring them to block access to non-compliant websites. ISPs are in a unique position to regulate access to content on the internet. Whilst existing laws in Europe (Arts 12-15, Electronic Commerce Directive 2000, implemented into UK law in Regulations 2002 No 2013) offer ISPs immunity from liability for content, liability can arise where intermediaries have actual knowledge of the offending material in Europe (except when they act as 'mere conduits').

16. The current proposal in the Bill that focuses on payment and advertising providers to enforce the law is simply inadequate. Whilst this is worth trying for the larger commercial providers of pornography who are more likely to comply in any case, it would leave out a large number of non-commercial providers as well as commercial providers who do not rely on revenue from the UK. The only way to ensure total compliance is by requiring ISPs to block non-compliant sites. ISPs, as access providers to the internet, ought to have a general duty of care towards children and child safety.

17. The onus of identifying non-compliant sites, however, should not be placed on ISPs – this would be burdensome and disproportionate. The age verification regulator as envisaged by the Digital Economy Bill 2016, or an equivalent body, could identify such sites and share a 'blacklist' of sites with ISPs who should then be required to block them. This would be similar to the existing *de facto* model for regulating child pornography. Whilst the age verification regulator could be empowered to require ISPs to block non-compliant sites, past experience in child pornography regulation shows that ISPs could be persuaded to cooperate without the need for specific legislation (the threat of possible legislation could act as an incentive to self-regulate).

18. Whilst ISP blocking is generally susceptible to criticism for fear of censorship and over-blocking, in this case neither the Regulator nor ISPs are asked to make an assessment of the content *per se* (for example, whether the content is obscene or not). All the Regulator would be doing is to check whether a website is compliant with the law that mandates age verification – this is a simple yes or no exercise. At no stage will a decision need to be made regarding the appropriateness of the content hosted –

this is a separate matter and outside the remit of the Regulator. Such an identification and blocking model that simply seeks to ensure that websites are compliant with the age verification requirement should be seriously considered.

25 August 2016

Dr Victoria Nash, Oxford Internet Institute, University of Oxford – written evidence (CHI0021)

1. As noted in the Call's background document, children's Internet use continues to elicit widespread concern about the potential risks and harms. Some of this concern is driven by observation and experience, some by publication of new research evidence and some by media-driven campaigns and negative headlines. In this context it is important to note that on many of the questions raised in this Call, there is an absence of consensus in the research evidence. On issues such as children's exposure to cyber-bullying, sexting or exposure to pornography, for example, different studies suggest very different prevalence figures (Kowalski et al 2014; Klettke et al 2014; Horvath et al 2013). For ethical and practical reasons, it is also rarely possible to conduct the randomised control trials that would help researchers better understand the likely causal pathways that translate particular risks into harms for specific children. Policy intervention may still be justified in this area, however any resultant interventions should be understood as 'precautionary' only, implying a particular responsibility to ensure proportionality, frequent review of policy efficacy as well as reconsideration if new evidence emerges (Starr 2003).

2. The existence of some research gaps doesn't mean, however, that decisions should be taken without consideration of available research evidence. The recent inclusion in the GDPR of a default minimum age of 16 for consent to process any digital data was notable for its last-minute adoption in the absence of consultation with NGOs, academic experts or children and young people. There is no evidence base for this apparently political decision, and it is possible that it will may increase rather than decrease risks for children under 16 if they are incentivised to lie about their age in order to use online services that are important to their lives (Livingstone 2015).

3. In terms of the array of policy tools available it is perhaps most useful to note that no technical measures exist which might serve as magical 'silver bullets' which can prevent all possibilities of harm. The current government has chosen to place great emphasis on the potential of Internet filters to prevent children from accessing material deemed to be unsuitable. The 'active choice' system rolled out by the major four Internet Service Providers (ISPs) is intended to provide families with household-level (rather than device-level) filtering. Whilst the determination to empower families to act to protect children is admirable, filtering is an imperfect technology leading to both false positives (material which is unnecessarily or wrongly filtered) as well as false negatives (allowing through material which the filter was supposed to prevent) (ACMA 2008). In addition to the proven fallibility of filtering tools, there is little consistent evidence that using such filters is effective in preventing children's exposure to negative experiences online (Mitchell et al 2003; Fleming et al 2006; Ybarra et al 2008). Given the substantial

economic costs of implementing and maintaining effective filters as well as the informational costs of blocking legitimate content, there is a need to conduct randomised control trials to more accurately assess whether such tools are an effective, let alone cost-effective method of preventing negative experiences online.

4. Having led an expert panel for the Department of Culture Media and Sport in 2014, I reviewed the academic evidence on the means by which children may access pornography online. One of the main conclusions of that panel was that given the variety of modes of access, and the determination of some adolescents to access such material, there is no likelihood of finding a simple technical fix to this social problem (Nash et al 2016). Even the current proposed measures of requiring age verification for online pornography publishers serving UK consumers are likely to prove ineffective, even if they are a welcome step towards requiring this industry to act in a responsible and legally compliant fashion.

5. Given that effective technical fixes are in short supply, it is essential that we work with schools, parents and carers to help them support children who are exposed to such material and to help them develop resilience. One of the strongest recommendations of our expert panel was that personal sexual health education education (PSHE) should be compulsory in all British secondary schools, and that this should incorporate material on pornography as a form of fictional media, and the issues it raises for consent, body image and relationships. The same reasoning also applies to other types of content such as self-harm material or pro-ana and pro-mia sites (focused on eating disorders), which would be similarly hard to prevent all access to. Such issues may be challenging for teachers to address, and classes may be unpopular with some parents. It is, however, vital that children are given the chance to discuss them in a safe environment and that they are presented with the critical resources to reflect on the dangers such content may offer.

6. The final point I wish to bring to the attention of this committee is the need to consider the appropriate roles of different social actors in addressing these concerns. Over the past few years, large tech companies such as Google, Facebook, Twitter, and the major ISPs have been encouraged to play an ever greater role as self-regulating 'sheriffs' (Zittrain 2008) in limiting children's access to certain materials. Whilst companies should be expected to act responsibly in ensuring they are not serving up material that it is illegal for under-18s to access, there is a danger that such companies become the primary arbiters of freedom of expression and information without appropriate accountability.

7. Relatedly, the focus on these large tech companies risks obscuring the wider array of commercial actors whose products and services may pose risks to minors. In an era where much-loved toys such as Barbie and Lego offer opportunities for online games and voice recording, where even very young children are encouraged to use toy cameras that allow their pictures to be uploaded to a hackable website, and where online banking

is available to those aged 11 and up, the risks around misuse of children's data are greatly expanded. It would be desirable therefore to widen the focus on the full range of commercial actors providing digital goods and services for children to ensure that data and privacy risks, as well as the more familiar content-based risks, are addressed in this Inquiry.

REFERENCES

The Australian Communications and Media Authority (ACMA) (2008). *Closed environment testing of ISP-level internet content filtering*. http://www.acma.gov.au/theACMA/closed-environment-testing-of-isp-level-internet-content-filtering.

Fleming MJ, Greentree S, Cocotti-Muller D, Elias KA, Morrison S. (2006) Safety in Cyberspace Adolescents' Safety and Exposure Online. *Youth Soc*.; 38(2):135-154.

Horvath MAH, Alys L, Massey K, Pina A, Scally M, Adler JR. (2013) *Basically... porn is everywhere: a rapid evidence assessment on the effects that access and exposure to pornography has on children and young people*. Office of the Children's Commissioner

Kowalski RM, Giumetti GW, Schroeder AN, Lattanner MR. (2014) Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among youth. *Psychol Bull*; 140(4):1073-1137.

Klettke B, Hallford DJ, Mellor DJ. (2014) Sexting prevalence and correlates: a systematic literature review. *Clin Psychol Rev*.;34(1):44-53.

Livingstone, S. (2015). No More Social Networking for Young Teens? LSE Media Policy Blog. http://blogs.lse.ac.uk/mediapolicyproject/2015/12/18/no-more-social-networking-for-young-teens/

Mitchell KJ, Finkelhor D, Wolak J. (2003) The Exposure Of Youth To Unwanted Sexual Material On The Internet A National Survey of Risk, Impact, and Prevention. *Youth Soc*.; 34(3):330-358.

Nash, V.J., Adler, J.R., Horvath, M.A.H., Livingstone, S., Marston, C., Owen, G. and Wright, J. (2016) "Identifying the Routes by which Children View Pornography Online: Implications for Future Policy-makers Seeking to Limit Viewing". Report of the Expert Panel for the DCMS Consultation "Child Safety Online: Age Verification for Pornography".

Starr C. (2003). The precautionary principle versus risk analysis. *Risk Anal Off Publ Soc Risk Anal*.; 23(1):1-3.

Ybarra ML, Finkelhor D, Mitchell KJ, Wolak J. (2009) Associations between blocking, monitoring, and filtering software on the home computer and youth-reported unwanted exposure to sexual material online. *Child Abuse Negl*.;33(12):857-869. doi:10.1016/j.chiabu.2008.09.015.

Zittrain, J. (2008). *The Future of the Internet and How to Stop It*. Harvard University Press.

25 August 2016

National Council of Women – written evidence (CHI0030)

1. What risks and benefits does increased internet usage present to children, with particular regard to:

i. Social development and wellbeing

There are three items of information NCW is able to provide.

First, in 2012, NCW submitted the following resolution to Government and appropriate National bodies having researched the effects on children of internet pornography.

OPT IN - PROTECT CHILDREN FROM PORNOGRAPHY

The National Council of Women, in Conference assembled, deeply concerned about the physical, mental and moral harm internet pornography could have on children and wishing to protect them, calls on Her Majesty's Government to make it compulsory for Internet Service Providers to block pornography at source so that pornography can only be accessed by an adult exercising an active choice.

Reasons:

(a) There is ample evidence that young people have accessed pornography online and according to psychologists, viewing porn is more addictive than drugs and alcohol. Research shows that viewing pornography can lead to an acceptance of violent and unhealthy notions of sex and relationships, where women are treated as sex objects and aggressive and violent sexual behaviour is regarded as the norm. Learning about sex without any relationship connections - pornography is a poor sex educator. Exposure to pornography helps to sustain young people's adherence to sexist and unhealthy notions of sex and relationships. Dr Michael Flood 2009.

(b) It is suggested it is the responsibility of parents to control their children's viewing and use parental controls to switch off pornography sites into homes. However, this can be costly and complicated and many parents are unaware of the content and effect of pornography on their children. Not all parents are computer-literate and each generation is more knowledgeable than the previous one; often busy parents are unable to keep up with the technology. The onus is all on the parents to take responsibility; while this is the ideal it is not realistic and society has a responsibility to protect children too.

(c) Censorship

We have a situation where pornography material is the default option in our homes and this is NOT ACCEPTED in any other form of media: television, films, high street hoardings and general print advertising, including lad and porn magazines, are all subject to regulation. The government hopes the ISP will regulate themselves, but they are reluctant to switch off pornography at source. It is an industry worth billions of pounds and our young children are their potential customers. NCW therefore recommends to the government the simplest and most effective way to safeguard our children is to switch off pornography at source.

Second, in 2015, the NCW Conference held an intergenerational Seminar entitled, *Social Media and its Effects on Young Women*. This involved members of the National Council of Young Women together with students from local schools and colleges. Relevant issues were as follows.

- The huge audience potential of Social Media given its absence of geographical and social boundaries, the vulnerability of children of primary school age to its influence, and the 'slut-shaming' and objectifying of girls and women online affecting real-life attitudes and behaviour.
- Social Media, like certain films and adverts already in the public domain, promote the attitude that looks and sexual stereotypes are all that matter. This preys on the insecurities not only of women and girls but also of men and boys, in light of the statistic that the number of boys who had committed suicide in 2014 was three and a half times the number of girls.
- Re possible solutions, encouraging young people to reduce their contact with Social Media was rejected as a way of ignoring the problem without stopping it. Instead, the power of Social Media could be used positively to set better examples using celebrities as role models. Also, there should be more active policing of online culture, *all* generations needed to take responsibility by becoming familiar with the technology, and sex education and PSHE in schools should be made available to both girls and boys at a younger age.

Third, NCW held a Seminar in 2015 entitled, *Social Media Today*. The speakers were Pippa Smith, co-Founder of SaferMedia and Ian Maxted, Safer Cyber Coordinator, Gloucestershire. During the open discussion the following points were made:

Benefits: Most of the audience use Social Media, some much more than others, to keep in touch with family and friends. Instant communication and access to information improves daily life, empowers us and keeps us active.

Difficulties: How do we teach children and young people to understand why it is dangerous to behave inappropriately via Social Media and to be respectful of one another?

Much material is anonymous so it is difficult to resist or retaliate. Think: Who are you letting into your life?

Effect on the psyche – unrealistic expectations lead to anxiety, shame, depression, anorexia.

What should be done?

Better filter systems are required. **Opt out** to a site should be the default (no action needed), so that **Opt in** has to actioned if required. (There are proposals from the EU to make it illegal for mobile phone and internet firms automatically to block obscene material - needs watching.)

Better guidelines required regarding: removal of unacceptable material; blocking access to sites by minors. Should the industry police itself or is legislation required?

Gambling and gaming sites have strong verification systems in place to stop access for under 18s. Should these be made compulsory for other ISPs?

Much more education about Internet Safety is required (1) for children and young people (2) for parents who have responsibility for safeguarding their children. Who should do this, and how?

5. What roles can schools play in educating and supporting children in relation to the Internet?

The following resolution, submitted by NCYW and forwarded to Government in 2013 and again in 2015, upon its reaffirmation contains the findings and recommendations of NCW on this and similar issues.

<u>PSHE BECOMES A FOUNDATION SUBJECT WITHIN THE NATIONAL CURRICULUM MAKING IT STATUTORY FOR KEY STAGES 1 TO 4</u>

NCW urges that Her Majesty's Government makes Personal, Social and Health (PSHE) Education at Key Stages 1, 2, 3 and 4 a foundation subject within the National Curriculum. We also urge them to make the teaching of PSHE education in Academies at these stages compulsory. PSHE education should be seen as a distinct 'subject' with its own unique body of knowledge.

<u>Reasons</u>: (i) Statutory PSHE education will improve access for all, the non-statutory status of much of PSHE education means that some schools are not prioritising the subject and not allocating sufficient curriculum time to it. Some schools are not delivering it at all. (ii) PSHE supports academic learning and develops through its own unique body of core knowledge the capabilities children and young people need to flourish in life and at work. (iii) Research shows children and young people want opportunities to discuss issues that are relevant to their lives and their well-being including emotions, relationships, health issues such as mental health, sexual health, diet and exercise. (iv) HMG puts emphasis on issues such as obesity and dementia, but does not give schools an appropriate means to deliver such messages. (v) Educationalists recognise that many barriers to learning lie outside the classroom and that supporting children's personal development and well-being (in part through learning in PSHE education) impacts positively on standards of achievement in

all subjects. (vi) PSHE education is crucial in safeguarding children. Good PSHE education helps children to learn about personal safety and improve their understanding of positive and respectful relationships. (vii) It can help pupils to recognise positive parenting and family relationships, as well as abusive, harmful or inappropriate behaviours – such as Child Sexual Exploitation and sexualisation and the media. (viii) It can support children to develop the confidence to ask for help, which can contribute to a reduction in childhood abuse and neglect. Similarly, evidence shows that PSHE education is an important intervention for the prevention of bullying. (ix) Good SRE taught by trained professionals gives children and young people the knowledge and life skills to resist peer, partner and media pressures and to understand issues such as sexual consent and responsibility.

August 2016

National Crime Agency – written evidence (CHI0043)

Inquiry into children and the internet

Question 1 - What risks and benefits does increased internet usage present to children with particular regard to: social development and wellbeing; neurological, cognitive and emotional development; and, data security.

The National Crime Agency recognises that increased internet usage amongst children presents a wide range of benefits. However, as the national law enforcement agency with the remit to lead the fight against serious and organised crime threats facing the UK, the NCA also sees the risks that internet usage can pose to children and young people without appropriate support and protection.

Child Sexual Exploitation and Abuse

One of the top priority threats investigated by the NCA is child sexual exploitation and abuse (CSEA), including online child sexual exploitation. Online child sexual exploitation includes indecent images of children (IIOC), online grooming, sexual extortion of children and live streaming of child sexual abuse.

Whilst the scale of the threat from online child sexual exploitation is difficult to quantify, law enforcement is seeing more reports than ever before, with significant increases in the volume of information and intelligence received relating to CSEA. For example, the National Center for Missing and Exploited Children (NCMEC) receives reports of instances of CSEA activity from US-based providers of online services and passes these to the NCA where they relate to the UK. At the end of 2015, the NCA received over 1,800 referrals a month, primarily from industry, compared with around 400 per month in 2010.

The internet provides offenders with a means to sexually exploit children and young people, and this manifests in a number of forms including through online grooming and sexual extortion.

Offenders generally groom children online to achieve two objectives:

- to lure the child into a physical meeting with the offender for the purposes of contact sexual abuse and/or;
- to manipulate victims into abusing themselves in view of the offender via webcam and generate indecent images (and video) of themselves for the offender.

The NCA assesses that the balance between levels of grooming for contact abuse purposes and grooming to elicit IIOC is changing, with the level of grooming to elicit IIOC and video increasing.

In terms of extortion, academic studies suggest that young people recording and sharing sexualised images of themselves with their peers and entering into sexualised chat through ICT platforms ('sexting') is, whilst undesirable,

becoming a more normal part of sexual developmental behaviour that is not in itself harmful. However, the ease with which such images can now be shared via the internet may make the subjects of such material vulnerable to extortion and possible victimisation.

Cyber Crime

Intelligence gathered from operational activity, offender debriefs, partners within industry and academia indicate that there are a number of UK teenagers254 who would not otherwise be involved in traditional255 crime who are becoming involved in cyber crime. The increase in 'off-the-shelf'256 illicit services and products has decreased the skill barrier to enter into cyber crime. Resulting in relatively unskilled young people with the ability to cause significant damage. The NCA's National Cyber Crime Unit (NCCU) and Regional Organised Crime Units (ROCUs) regularly arrest individuals under the age of 18 for cyber offences.

Though the NCA will seek criminal justice outcomes for the most serious cyber criminals, there remains a number of people who are acting on the periphery of cyber criminality and may be judged not to have met the threshold for arrest. To date a large majority of these people are male children.

The NCA has developed the twin strategies of deterrence and positive diversion to influence individuals, many of whom are children, away from cyber crime.

Question 2 - Which platforms and sites are most popular among children and how do young people use them? Many of the online services used by children are not specifically designed for children. What problems does this present?

Offenders use different platforms to engage with children for grooming. The frequency at which individual platforms are used by offenders varies in accordance with the popularity of platforms among children and the effectiveness of management and monitoring systems applied by the platform providers.

Offenders continue to largely contact children via open social networks and then persuade them to move to more private forms of communication. Images may be created remotely and sent to the offender after the event or streamed in real time (live streaming) and captured by the offender.

There are a range of issues presented by the fact that online services used by children are not specifically designed for them including:

254 In 2015 the average age of suspected cyber criminals arrested by the NCA was 17 years old.

255 'Traditional' crimes are regarded as those typically recorded within Home Office police recorded crime and are generally thought of as committed in offline environments, for example, theft, fraud, sexual or harassment offences.

256 These tools are developed by programmers to perform hacking functions. The owners and programmers of these tools seek to make a profit through the selling of these tools on hacking forums to those who do not possess sophisticated programming or hacking knowledge (e.g. 'script kiddies'). These programmes can be very sophisticated and cause significant damage and harm.

- Children and young people sharing their personal information without realising the consequences;
- Children's exposure to harmful or sexual content. Content that is often adult in nature, e.g. sexual conversations / images;
- Online friendships being formed with adults rather than peers;
- Age-inappropriate interactions that the child is not prepared for developmentally and does not recognise as a risk;
- Difficulty disclosing when something goes wrong;
- A young person's ability to share their own sexual behaviour online;
- With webcam-based platforms, the possibility that footage can be recorded and possibly distributed with or without the user's knowledge.

The NCA monitors trends in young people's use of online platforms through information received from industry, members of the public, law enforcement and direct engagement with children and professionals working with children and responds accordingly. This response takes many forms, including: directing law enforcement interventions; producing guides for parents, carers and professionals on those platforms that are popular and/or present a risk to children; and proactively engaging with companies to help them make their platforms safer for children.

Question 3 - What are the technical challenges for introducing greater controls on internet usage by children?

Some of the key challenges with introducing greater controls on internet usage by children include:

- the internet can be accessed from so many different devices and locations;
- it is not just the content that poses a risk; for example, children may engage in risky behaviour on the internet with peers or with offenders;
- children may be deterred from platforms where they feel their internet usage is being too tightly controlled or monitored;
- the difficulties in ensuring that age verification is simple but effective;
- ensuring that tools to enable children to protect themselves or report issues are user-friendly;
- controls can easily be turned off and the internet is easily accessible to young people on a range of devices – most notably mobile connections – which can bypass filtering and controls set on a home connection.

The NCA views the main challenge with filtering or control settings is that they will never be completely effective and do not replace the need for adults to have open and honest conversations with children about online safety, alongside supporting and advising children when they are using the internet. It is important to embed controls alongside conversations with children about safety, trust and responsibility.

The most effective means of building a child's resilience against the online risks of sexual exploitation is for trusted adults, such as parents or teachers, to have open and ongoing conversations about sex, relationships and the internet.

Question 4 - What are the potential future harms and benefits to children from emerging technology, such as Artificial Intelligence, Machine Learning and the Internet of Things?

CSEA offenders will look to exploit any perceived vulnerability in emerging technologies. The NCA Annual Strategic Assessment of CSEA reported that "…the boundaries between different types of CSEA offending in the physical and online environments are becoming increasingly blurred with the expansion of communications technologies."

Question 5 - What roles can schools play in educating and supporting children in relation to the internet? What guidance is provided about the internet to schools and teachers? Is guidance consistently adopted and are there any gaps?
Question 6 - Who currently informs parents of risks? What is the role for commercial organisations to teach e-safety to parents? How could parents be better informed of risks.

Child Sexual Exploitation and Abuse

Education and guidance are key elements in the NCA's response to the threat from child sexual exploitation and abuse, and the NCA works routinely with law enforcement and non-law enforcement partners to deliver key messages to children, young people, parents, carers and professionals.

The NCA develops and implements a range of activity with partners, targeting children and young people, and parents and carers, in order to increase their resilience to risk, including through training a network of Ambassadors of over 6,500 professionals. Ambassadors are trained in the nature of online offending against children, how young people use the internet, including risk-taking behaviour, and school/organisation responses and policies addressing this threat.

'Thinkuknow' is an education programme developed by the NCA with three strands: children; parents and professionals. It provides high quality education about sex, relationships and the internet aimed at reducing the vulnerability of children and young people to sexual abuse and exploitation. These messages are delivered through a network of over 140,000 professionals across the UK.

- The programme's innovative and engaging films, cartoons, websites and lesson plans enable parents, teachers, youth workers, police officers and health professionals to explore difficult and sensitive issues safely with children and young people. Thinkuknow education resources reach over 3.5 million children and young people every year.

- Parents play a vital role in the protection of young people from sexual exploitation and it is crucial to build their confidence in knowing the facts, understanding the risks and learning where to get help, so that they can feel better equipped to have conversations with their children. The NCA is running a Parents and Carers' Campaign throughout Summer 2016 to raise awareness of Thinkuknow resources, with the aim of encouraging

conversations with children about how to stay safe online. A wide variety of partners from law enforcement, charities and the private sector are supporting the NCA with this activity.

- Thinkuknow has a dedicated website for parents providing expert information and advice on protecting children from abuse online. There is a wealth of preventative information for parents who want to understand more about keeping their child safe, and also reactive advice for parents who are concerned about their child or who need to report an incident.

In September 2015, the NCA launched ParentInfo, a website and newsfeed providing up-to-date and expert advice for parents and carers which schools can host on their own websites. ParentInfo provides articles across a wide range of issues which aim to help parents increase their children's resilience to risk. Over 3,000 schools have signed up for the free service, around 10% of UK schools.

The NCA and a range of partners also regularly produce guidance, using an evidence-based approach, for children, young people, and parents and carers on specific topics such as how to use a webcam safely or the risks associated with sharing self-generated nude or nearly-nude images.

Cyber Crime

The NCA has devised a "Positive Diversions" project which is engaging with private, public and third sectors to dissuade, divert and direct young people away from engaging in cyber criminality, and to use their skills more positively and productively. The toolkit of positive diversions currently being developed for children and young people could range from participation in a local coding club to mandatory attendance at a Prevent workshop covering ethics, legislation, careers and education.

Many children and young people encountered by the NCA have claimed that they did not know that the activities they were engaged in were illegal. Although there may be an element of false reporting within these claims, it is important that limits of the law and the consequences for transgressing this limit are well-publicised to those children and young people who may be engaging in such activity.

The NCA has delivered a communications campaign aimed at parents257 called #cyberchoices, and will deliver another aimed at children and young people in 2017. NCA continues to work with partners to deliver this campaign message to parents and teachers.

These campaigns illustrate the consequences of becoming involved in cyber crime whilst highlighting the positive alternative options available to young people who use their skills for good.
The NCA wants children to be aware of:

257 #cyberchoices, December 2015

- the ethical considerations and legislation regarding cyber crime in the UK (specifically the Computer Misuse Act 1990);
- the potential consequences of becoming involved in cyber crime; and
- the range of positive options available to those interested in coding, programming, technology and computers.

The NCA highlights these messages when working with partners such as Cyber Security Challenge UK. The NCA has also created a module for the upcoming Cyber Security Extended Project Qualification that highlights these priorities using cyber criminal case studies.

The NCA is also conducting a project targeting the market for "off the shelf" tools for committing cyber crime. Intelligence indicates that such tools can be a gateway into crime and lower the barrier to participation in crime as no skill is needed by the user. The aim is to make it too difficult for children and young people to begin a journey into crime in the first place.

NCA and police officers have coordinated and carried out multiple "cease and desist" visits across the UK. If an individual has become involved on the periphery of cyber criminality258 but does not necessarily meet the threshold for arrest, officers may visit the individual and have them sign a cease and desist notice. The majority of cease and desist subjects to date have been young males.

Question 8 - What voluntary measures have already been put in place by providers of content to protect children? Are these sufficient? If not, what more could be done? Are company guidelines about child safety and rights accessible to parents and other users?

The NCA has worked with industry to develop search term blocking and, through collaborative work with the Internet Watch Foundation (IWF), has shared hashes - digital footprints of indecent images of children - to enable industry to remove and prevent the sharing of potentially hundreds of thousands of images from their platforms and services. Industry has committed to build on this by continuing to work with UK law enforcement agencies and the IWF.

The NCA is a member of the UK Council for Child Internet Safety (UKCCIS) which has produced the *Practical Guide for Providers of Social Media and Interactive Services*. The guide provides advice for such services on how to report behaviour which is of concern to the NCA and/or the Internet Watch Foundation.

The Internet Watch Foundation (IWF) works internationally to identify, assess, report and help remove illegal child sexual abuse images. The business model is self-regulatory (government, IWF and online industry globally). The IWF coordinates the blocking and removal of illegal child sexual abuse images through, amongst other activity, the issuing of takedown notices to remove

258 An example would be someone who has registered on a website that is offering criminal services, such as DDoS, but there is no evidence that the criminal service was used by the individual.

these images and stop them from being spread further. The IWF also manages a hotline for anyone to securely and anonymously report child sexual abuse images.

There is an online reporting system for UK industry via existing mechanism that enables UK industry to report illegal traffic to the NCA (via ClickCEOP) on a voluntary basis.

In the United States all service providers are mandated under US legislation to report the sharing of all indecent images detected by NCMEC. This is beyond any internal action that the organisation takes. NCMEC then disseminates that information to the designated law enforcement agency in the relevant country where the offender is located. The NCA is the designated recipient of reports relating to UK cases.

24 August 2016

National Crime Agency and Internet Watch Foundation – oral evidence (QQ 28-36)

Transcript to be found under Internet Watch Foundation

National Society for the Prevention of Cruelty to Children (NSPCC) – written evidence (CHI0014)

Executive summary:

The internet can be extremely beneficial for children. They can use it to learn, communicate, develop, create and explore the world around them. Yet, in spite of the fact that children make up one third of the internet's users, in too many cases it also leaves them vulnerable to the risk of maltreatment, for example online abuse or exploitation, and exposes them to experiences which they find upsetting. It is essential that we ensure children are afforded the age-appropriate, comparable level of adult protection, care and guidance in the online space as they do in the offline world.

Through the NSPCC's Childline service, our frontline service delivery and social research, we are able to attain a unique insight into young people's experiences online. We regularly hear from children about the negative impact that viewing inappropriate content has on them, as well as the impact of being subjected to online harassment, grooming and sexual exploitation. Inappropriate content includes pornography and violent and degrading portrayals of sex, as well as material which incites them to self harm or compete to lose weight. Key insights from Childline include:

- In 2015/16, there were over 11, 000 Childline counselling sessions relating to online sexual abuse, cyber-bullying and internet safety, which was a 9% increase on the previous year.

- A third (3,716) of these counselling sessions were related to online sexual abuse, of which 41% led to referrals to the Child Exploitation and Online Protection Centre. During 2015/16 Childline carried out 844 counselling sessions with children and young people who had concerns about being exposed to sexually explicit images online.

Our research with young people has provided further evidence about children's experiences online:

- Research by the NSPCC and the Children's Commissioner with over 1,000 young people aged 11-18, found that over half had been exposed to online pornography, with nearly all of this group (94%) having seen it by age 14. In many cases they first encountered this material inadvertently, i.e. via a pop-up.[259]

---

259 Martellozzo, E., Monaghan, A., Adler, J., Davidson, J., Leyva, R., and Horvath, M., "'I wasn't sure it was normal to watch it'", 2016, (available at http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/october-2013/research07Oct2013.pdf).

National Society for the Prevention of Cruelty to Children (NSPCC) – written evidence (CHI0014)

- A survey of over 1,700 young people found that 50% had seen inappropriate content, including material that was sexual and/or violent, or involved bullying and self-harm, on the most popular sites for children age 13+.[260]

- Young people have told us that they want to be protected from harmful content online. In a survey we conducted with over 1,600 11-16 year olds, 65% felt that social media sites needed to do more to protect them from adult content, 67% from self-harm content, and 60% from violent content.[261]

260 NSPCC, 'Net Aware', (2016).
261 NSPCC, 'Net Aware'.

National Society for the Prevention of Cruelty to Children (NSPCC) – written evidence (CHI0014)

Key recommendations:

- The Digital Economy Bill should go further than proposed by introducing blocking at the Internet Service Provider (ISP) level against all pornographic sites that fail to provide effective age-verification. The breadth should also be widened to incorporate user-generated content, as well as commercial.

- An independent regulator, as proposed within the Digital Economy Bill, should be endowed with the power to set minimum standards of child safeguarding across all social networks, platforms and ISPs to ensure that child safeguarding is incorporated into the design, content and functionality of all online services.

- There is a lack of consistent and universal terminology for what constitutes online abuse specifically relating to children and young people. It is imperative that we establish a common understanding of online abuse so that we can develop robust and consistent evidence on the nature and scale of children and young people affected.

If it is helpful for the Committee, we are able to arrange visits to Childline or for members to meet with a group of young people.

What risks and benefits does increased internet usage present to children, with particular regard to:

i. Social development and wellbeing
ii. Neurological, cognitive and emotional development,
iii. Data security.

1. The NSPCC, through its Childline service, frontline service delivery and research, is able to attain a unique insight into young people's experiences online. From the contacts that we receive from young people, it is evident that too many children are being exposed to dangerous and harmful content online, or being subjected to online harassment, grooming, and sexual exploitation. **In 2015/16, there were over 11,000 Childline counselling sessions relating to online sexual abuse, cyber-bullying and internet safety, which was a 9% increase on the previous year. A third (3,716) of these counselling sessions were related to online sexual abuse.**

Inappropriate content:

2. At the NSPCC and Childline, we frequently hear from children about the negative impact that viewing inappropriate content has had on them; content that they felt incited them to self-harm; to compete to lose weight; and that allowed them to access violent and degrading portrayals of sex. Young people tell us that they feel anxious, shocked, and guilty as a result of what they have seen online.

- During 2015/16 Childline carried out 884 counselling sessions with children and young people who had concerns about being exposed to sexually explicit images, of which 41% led to referrals to the Child Exploitation and Online Protection Centre

- Recent research published by the NSPCC and the Office of the Children's Commissioner England with over 1000 young people, aged 11-18, found that over half of the sample had been exposed to online pornography, with almost all (94%) of this group having seen it by age 14. They were as likely to have been inadvertently exposed to pornography (e.g. via a pop-up), as they are to have actively searched for it.[262]

- 16% of children have seen something online that they found nasty, worrying, or offensive.[263]

"I came across some pornographic images recently when I was online and I feel really guilty for even looking at them. I am frightened the police or other people will find out that I have seen them. It makes me feel disgusting."

"I'm being bombarded with pop-up windows showing pornographic images. It's starting to make me really anxious because some of them are of children. I'm worried someone is going to think I've been looking at the sites and I'm going to get into trouble. I don't know what to do because it's becoming a problem. I think someone is accessing my computer or something because I don't understand why I'm getting them. I can't ignore it anymore."

(Contacts to Childline, 2016)

3. Young people may seek out inappropriate content online as a result of curiosity which is a natural part of child development and adolescence, or they can stumble upon it by accident, but the impact can be equally severe either way. Our research found that pornography has a desensitising impact on young people: on first watching pornography young people expressed feeling shock and disgust, yet for many children, these feelings were replaced with arousal and excitement the more that they viewed.

   - **Many young people stated that they perceive pornography to be an accurate representation of sex; with just over half of boys and four in ten girls believing that what they have viewed is realistic.**

262 Martellozzo, "'I wasn't sure it was normal to watch it"'.

263 Ofcom, 'Children and Parent's Media Use and Attitudes', (available at http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/october-2013/research07Oct2013.pdf).

- **44% of boys and 29% of girls also reported that online pornography has given them ideas about the types of sex they want to try out.[264]**

- Many girls expressed concern that pornography changes boy's attitudes towards females and impacts upon their understanding of sex and relationships. This was echoed within Girl Guiding's annual Girls' Attitudes Survey, where 7 in 10 respondents stated that pornography normalises violence against women.[265]

"A few of my friends have used it for guidance about sex and are getting the wrong image of relationships" (Female, 13)
"They (boys) become a different person - and begin to think that it is alright to act and behave in such ways. The way they talk to others changes as well. When they look at a girl they probably only thinking of that one thing - which isnt how women should be looked at" (Male, 14).
"I wasn't sure it was normal to watch it", (NSPCC, 2016).

Online sexual exploitation:

4. In 2015/16 the NSPCC's Childline service performed 1, 480 counselling sessions with children about online child sexual exploitation, including grooming.

- Further to this, the NSPCC made a Freedom of Information request in April 2016 to police forces across England and Wales, and found that **the internet is used in eight cases of child sexual abuse every day**, including rape, online grooming, and live-streaming of sexual abuse.[266]

    a. **In 2014/15 the number of police-recorded offences for obscene publications rose by 62% in Northern Ireland, 69% in England, and 114% in Wales.[267]** Meanwhile, Police Scotland's first national operation to tackle online child sexual abuse (Operation LATISSE), which ran between early June to mid-July, resulted in the identification of over 500 children pictured in child abuse imagery, and the recovery of 30 million child abuse images.[268]

---

264 Martellozzo, "'I wasn't sure it was normal to watch it'".
265 Girl Guiding, 'Girl's Attitudes Survey, 2015', (available at http://www.girlguiding.org.uk/pdf/GAS_15_website.pdf)
266 BBC, 'Child sex abuse: more than 100 rapes with online link in last year', 2016, (available at http://www.bbc.co.uk/news/uk-36578945).
267 Bentley, H., O'Hagan, O, Raff, A. and Bhatti, I., 'How safe are our children? The most comprehensive overview of child protection in the UK', (London, NSPCC, 2016).
268 Police Scotland, 'Thirty million images of child sexual abuse recovered', (available at http://www.scotland.police.uk/whats-happening/news/2016/july/thirty-million-images-of-child-sexual-abuse-recovered-during-operation).

5. Yet to be published research carried out on behalf of the NSPCC, looking at the impact of online abuse on young people, has highlighted specific online characteristics which increase the severity of the experience. In many cases of online grooming there is evidence of the abuse, in the form of child sexual abuse images or videos, which may be available for others to view. **The victim is condemned to repeated re-victimisation, violation and degradation each time the image or video is accessed.** Fear of people viewing the content, can prevent the victim from speaking out about their experiences and seeking help.

6. Due to the online nature of the abuse, and the fact that the young person may not have met their offender, they can find it difficult to identify that they are being abused. If the young person has sent the groomer images or videos, they can feel complicit in their abuse and experience shame or guilt. They may be less inclined to disclose their abuse due to the perception that they will be judged by others for their actions and that they are somehow to blame, meaning that they may not receive the support that they desperately need.

> "*I was being groomed online by men and it went on for years. Then people started finding out and getting involved. They didn't know the full extent, but I spoke to the police. When they questioned me I felt so ashamed so I didn't tell them the full story. I feel like such a coward. I tried to kill myself recently because it's constantly on my mind". (female, 12 to 15)*
> *I met this guy on my social network and he was really nice at first, telling me that he loved me and paying me all these compliments. I sent him some naked pictures and now he is threatening me saying that he is going to show them to my friends and family if I don't send him more. I have also found out that he lied about his age and he is much older than he said he was. I don't know what to do and I'm too embarrassed to talk to anyone. (Girl, 12-15)*
>
> (Contacts to Childline, 2016).

Online harassment, hatred and bullying:

7. Evidence from Childline shows that online bullying counselling sessions increased by 88% in the last 5 years (2011/12 to 2015/16), making it one of the most counselled issues relating to children's experiences online. The latest figures show that during 2015-16, Childline provided 4,541 counselling sessions about online bullying; this is the highest number of counselling sessions that we have ever had to provide for this issue and represented a 13% increase on 2014-2015.[269]

8. The NSPCC performs annual research with over 1700 young people and 500 parents on the top 50 social networks that children use, in order to inform the information that we provide on our parental tool, Net Aware. As part of this research, 33% of young people reported that they had seen bullying/hatred on the social networking sites they used most frequently.

269 Bentley, 'How safe are our children?'.

This aligns with UK Safer Internet Centre's research which highlighted that 86% of young people (aged 13-17 years old) felt that the internet made it easier for people to be mean, and 82% of respondents had seen or heard something hateful online.[270]

9. Young people have expressed to Childline the impact that bullying behaviour and hate content has on them: reducing young people's self-esteem, impairing their ability to establish relationships, and in extreme cases leading to mental health problems, including self-harm and suicidal thoughts.

> *People have been telling me to kill myself through a social media site. I don't understand why they are being so horrible but it's really affecting me. I've tried to ignore it but I can't. I thought if I changed my account details but the messages are still getting me to. I don't know what else I can do? I can't find how to report it. (Girl, 12-15)*
>
> *My self-esteem is so low at the moment. It's all these girls calling me names and spreading all these horrible rumours about me over the internet. Everyone believes them and now they all hate me. One of them hacked into my social network account and sent mean messages to all my friends and family. I am going through a lot at the moment. (Anon)*
>
> (Contacts to Childline, 2016).

cognitive development, so that support services can be tailored to the young person's needs.

Which platforms and sites are most popular among children and how do young people use them? Many of the online services used by children are not specifically designed for children. What problems does this present?

11. The NSPCC has created a tool called Net Aware, where parents can find information about the top 50 sites that young people have told us they use. It is based on evidence collected from 1700 children and 500 parents about their experiences on the most popular platforms. From research for the tool we know:

    - 50% of young people have seen inappropriate content, including sexual, violent, bullying, and self-harm content, on sites included in the Net Aware tool which were rated as being suitable for children age 13+

        - 23% of young people have also seen inappropriate content on those sites rated for children aged 12 and below, in particular bullying and violence.

---

270 UK Safer Internet Centre, 'Creating a Better Internet for All', 2016, (available at http://childnetsic.s3.amazonaws.com/ufiles/SID2016/Creating%20a%20Better%20Internet%20for%20All.pdf).

- Young people want social media sites to protect them from harmful content: 71% think there should be more protection from bullying; 69% from racism; 67% from self-harm content; 65% from adult content; and 60% from violence.

- 98% of the top 50 sites included on Net Aware have been accessed by children before they reached 13.

12. Although most sites state that they are suitable for children 13+, our research highlights that young people are regularly stumbling upon sexual, violent, and self-harm content. This is because categorisation for sites is not based on the content or nature of the platform but relates to privacy laws – specifically the Children's Online Privacy Protection Act (COPPA), which states that websites must obtain permission from a child's parents if they are under 13 before collecting personal information from that child. Sites are often rated as 13+ for ease, when they are actually designed for adults and expose young people to harmful content or contact. This was highlighted within research performed by the NSPCC and the Office of the Children's Commissioner which found that **children are as likely to accidentally stumble upon pornographic content online as they are to actively search for it.** The NSPCC would like site-ratings to be based upon the impact of the content and service on young people's cognitive and emotional development. To ensure that ratings are appropriate further research into the effects of social networks on children should be performed.

13. To prevent young people from accessing social networks before they reach the required age, age-checks should be introduced when users create an account. According to those parents that helped develop our Net Aware tool, it **would be easy for an 11 year old to lie about their age to sign-up to 78% of the sites on Net Aware and on 22% it would be very easy.** Ineffective age-rating systems can enable adults to communicate with young people or result in children seeing age-inappropriate and potentially harmful content on social networks.

"On popular hashtags on instagram, which younger children can access, there are some explicit pictures. Makes me feel irritated that people can come across these when they don't want to or have tried to" (Female, 13-14).

"Often when on Tumblr, someone would have reblogged a post, or a post leading to recommendations of pornographic .gifs. Normally, these take me by surprise and make me feel quite uncomfortable" (Female, 13-15).

"On facebook peoples accounts get hacked and then the hackers post pornographic videos and tag my friends in them and it pops up on my news feed" (Male, 11-12).

"'I wasn't sure it was normal to watch it'", (NSPCC, 2016).

National Society for the Prevention of Cruelty to Children (NSPCC) – written evidence (CHI0014)

What are the potential future harms and benefits to children from emerging technology, such as Artificial Intelligence, Machine Learning and the Internet of Things?

14. It is essential that young people's safety is incorporated, from the outset, in the development of all emerging technologies. For this reason, the NSPCC has raised the importance of ensuring that children's needs are recognised and responded to within the recently established PETRAS Internet of Things Research Hub. As with all online services, we would expect that the principles laid out in the ICT Coalition for Children Online and UKCCIS guidance, where relevant, are applied to emerging technologies. This would include managing content, parental controls, dealing with abuse and misuse, strategies and processes to deal with child sexual abuse and illegal contact, effective privacy and controls, as well as safety education and awareness. New technologies must also monitor their safeguarding processes and be transparent about their effectiveness. Industry must harness new technologies to create innovative solutions to keeping children safe online.

What roles can schools play in educating and supporting children in relation to the internet? What guidance is provided about the internet to schools and teachers? Is guidance consistently adopted and are there any gaps?

15. The internet has a huge bearing on how children interact with one another. Schools should therefore have policies in place which address how technology such as social media can be used to perpetrate abuse. As such the Government should ensure online and digital safety has a place in the school curriculum as part of wider efforts to develop a whole school ethos focussed on increasing young people's awareness and understanding of the motivations, consequences and risks of some online behaviour.

16. Teachers need to be provided with guidance and resources on the different manifestations of online abuse so that they can better educate, support and guide children. Schools need to ensure that children and young people are able to recognise abusive, coercive and exploitative online behaviour, and understand what constitutes inappropriate behaviour and relationships online. Children also need guidance on blocking unwanted sexual approaches, not being drawn in by manipulative behaviours, understanding what coercive and controlling behaviour can look like online, and know where to report suspicious activity and access support.

17. Schools need to have clear reporting mechanisms for on and off-line abuse and should be able to signpost to support services (both in school and outside of school) – that are developed with young people, parents and teachers. This includes a clear understanding of how images can be reported and removed from the internet. Teachers need to have concrete risk assessments so as to be able to spot signs of online abuse, escalate and report cases appropriately and know how to signpost and support each child taking into consideration the additional impacts that online abuse has on the child.

Who currently informs parents of risks? What is the role for commercial organisations to teach e-safety to parents? How could parents be better informed about risks?

18. The NSPCC have partnered with O2 to provide parents with the skills and support that they need to keep their children safe online. We are delivering online safety lessons in O2 stores, schools and communities across the country and have established an Online Safety Helpline that parents are able to call for advice on parental controls, social networks, or technical settings. Furthermore, we have created Net Aware which offers information on registration processes, privacy settings, and reporting features on the top social networks, as well as explaining the type of content that children can expect to see on the site or app.

19. However, everyone has a part to play in helping to inform parents and keep young people safe online. Parents are not always receiving the support that they require. Research conducted by the NSPCC with over 1000 parents on the issue of sexting found that only 13% of parents had received any information or support around sexting, despite the fact that 50% said they would like to know more. Of those parents that said they want support, 69% would like to receive information from schools and 49% from the police[271]. Both of these organisations have an educational role to play and must reach out to parents.

20. Internet Service Providers (ISPs) and social networks additionally have a responsibility to provide parents with information about the risks online and the services that they provide. According to Ofcom, 43% of parents of 5-15 year olds that have broadband and whose child goes online are unaware of ISP level filtering[272]. If parents are to make informed decisions about their child's safety online, it is essential that they are educated about the tools available. Internet Service Providers should also apply default-on privacy settings to that all children receive protection and that the most vulnerable children, whose parents may not be able or interested, are not overlooked.

21. There additionally needs to be a collaborative effort to engage with harder-to-reach parents, such as those that are facing adversities or who do not have the time or knowledge to use online safety tools. We need to reach out to parents in the places where they already are, such as their children's schools, their doctors, and their local communities.

---

271 NSPCC, 'Sexting and Young People: The Parent's View', 2016, (accessed at: https://www.nspcc.org.uk/services-and-resources/research-and-resources/2016/sexting-young-people-parents-view/?_t_id=1B2M2Y8AsgTpgAmY7PhCfg%3d%3d&_t_q=sexting+parents&_t_tags=language%3aen%2csiteid%3a7f1b9313-bf5e-4415-abf6-aaf87298c667&_t_ip=10.97.160.97&_t_hit.id=Nspcc_Web_Models_Pages_ResearchReportsPage/_d9e07248-0772-4639-bb72-7ed34f8d23cc_en-GB&_t_hit.pos=2)

272 Ofcom, 'Children and Parent's Media Use and Attitudes'.

What are the challenges for media companies in providing services that take account of children? How do content providers differentiate their services for children, for example in respect of design?

22. Despite the fact that 1/3 of internet users are under the age of 18, many social media providers are failing to prioritise young people's safety across their platforms. The UK Council for Child Internet Safety (UKCCIS), of which the NSPCC is a member, have produced 'A Practical Guide for Providers of Social Media and Interactive Services', which supports social media companies to safeguard young people using their sites. It is composed of six key principles: managing inappropriate content; providing parental controls; dealing with abuse; dealing with child sexual abuse content; providing privacy settings; and serving an educational function to children and parents. It is essential that all social network sites providing services to children adhere to the principles laid out by UKCCIS.

23. We would also like to see greater transparency from social networking sites about the effectiveness of their safety features in protecting children online, and whether they are adhering to UKCCIS guidelines. Only when social networks begin to publish this information will it be possible to develop robust and consistent evidence on the nature and scale of children and young people affected and impacted by online abuse.

24. Platforms that attract both adults and children should distinguish between their audiences by verifying the user's age and providing specific features to under 18s:

    - Default-on privacy settings for children so that their profiles are not searchable and they cannot be contacted by strangers.

    - Alerts to young people whenever they are communicating with an adult.

    - The option to install parental controls to help protect young people from viewing harmful content.

    - Age-checking to distinguish between children of different ages so that tailored, age-appropriate protection can be applied. This should be based upon an impact assessment into the neurological and developmental impact of services upon children of variable ages.

What voluntary measures have already been put in place by providers of content to protect children? Are these sufficient? If not, what more could be done? Are company guidelines about child safety and rights accessible to parents and other users?

25. The NSPCC have been pleased to see innovative work being introduced across the field of online safety, including the Child Abuse Images Database, the UK Council for Child Internet Safety, and the WeProtect Global Alliance. There are also examples of good practice amongst social networking sites. However, there is significant variation in the safeguards available on social networking sites and it is often the case that the less

well-known sites and apps offer fewer protections to young people. More detailed information about the effectiveness of individual social networks' safeguarding practices can be found on the NSPCC's Net Aware tool.

26. There is also concern that emerging sites are failing to consider safety by design and technologies, such as augmented reality and live-streaming, are presenting new concerns and not adhering to UKCCIS guidelines. Minimum standards and best practice guidance must be established in these areas so that when new sites emerge on the market they can check that they are providing the requisite safety features to enable young people to participate in a safe environment.
27. The guidelines available on social networks about online safety are variable. UKCCIS recommends that all sites providing services used by young people clearly articulate what behaviour is and isn't acceptable online, and respond to reports of harmful content quickly and effectively. All social media site's guidelines should be prominently displayed, in easy-to-understand language, preferably in a safety centre or contact centre for ease of access. However, many sites are not reaching these standards: only 8% of the sites included on Net Aware were judged by parents to have easy-to-find reporting processes and 10% were difficult to find. Meanwhile, 14% of the sites were judged to have difficult to find privacy settings.

Legislation and Governance

28. We welcome the Government's commitment to prevent children from accessing online pornography through the Digital Economy Bill but we are concerned that the Bill does not go far enough to protect children online.

    - Proposed civil sanctions will not protect young people from viewing pornography, as they will be unenforceable against overseas pornography companies. Only by blocking non-compliant sites at the ISP level can we ensure that young people cannot access pornographic material and an equal system, where the whole pornography industry is held to account, instead of only UK-based firms.

    - The Bill only covers commercial pornographic material. While a welcome step, it leaves out user-generated material, and as such fails to cover revenge pornography, individual pornographic sites, or the proliferation of live-streaming and video-chat. By allowing this material to remain children will continue to be exposed to potentially harmful sexual content.

        - 22% of young people who told us about video-chat sites on Net Aware had been exposed to sexual content.

29. We welcome the proposal of the Regulator within the Bill but would like to see its scope widened. To resolve the above concerns, the Regulator should be independently appointed and granted the power to enforce a minimum set of child protection standards across all social networks, web operators, services providers, and ISPs. Sanctions, including blocking and

financial, should be enforced against all platforms that fail to comply with the Regulator.

30. To ensure consistency in the application of legislation and policy, a universal and consistently applied definition of online abuse must also be established, and then applied by the Regulator. Any definition needs to incorporate abuse that takes place through social media or other online channels; abuse that is repeated by sharing it online; abuse that is orchestrated, planned and organised via online channels; abuse that is recorded and uploaded online (for personal use or for distribution/sharing with others); and abuse where the internet is used as a means to exploit.

31. Lastly, another gap in legislation is Section 67 of the Serious Crime Act 2015, which was passed into law following an NSPCC campaign that received support from over 50,000 people, but has still not received a commencement order. This legislation makes it illegal for an adult to send a sexual communication to a child and is crucial in light of evidence showing an increase in the scale of child online sexual abuse.
    - In 2015 there was a one-third increase in the number of cases of child sexual abuse compared to the previous year, with one known method used by paedophiles being sexual communication online[273].

    - At the same time, the number of contacts to Childline from children and young people about online grooming increased by 10% to 3,150.

Section 67 is an essential step to help protect children online and counteract the worrying rise in sexual abuse cases and the Government must commence it as soon as possible.

Does the upcoming General Data Protection Regulation take sufficient account of the needs of children? As the UK leaves the EU, what provisions of the Regulation or other Directives should it seek to retain, or continue to implement, with specific regard to children? Should any other legislation should be introduced?

32. The NSPCC welcomes the fact children are seen to merit specific protection with regard to their personal data within the GDPR; that Article 35 is mandating for risk assessments for children with regards to new technologies, and that in Recital 64 and Article 17 reference to the right to be forgotten (or right to erasure) is also raised. However, Article 8 of the General Data Protection Regulation stipulates that information services, including social networks, cannot process the personal data of young people under the age of 16 without prior consent from their parents. This legislation changes the provisions of the Children's Online Privacy Protection Act and will effectively ban under 16's from using social networking sites. We are concerned that there has been no independent evaluation or impact assessment carried out in order to make the explicit

---

273 NSPCC, '5 Child Sex Offences Reported Every Hour', 2016, (available at https://www.nspcc.org.uk/fighting-for-childhood/news-opinion/child-sex-offences-uk-record-rise/).

decision about the age at which a child may decide for themselves whether or not to hand over personal data to an online service provider without the provider having to obtain the consent of the child's parents. Of equal concern, is that there has never been an impact assessment on the explicit decision about the age at which technologies or online services are suitable and suited to children or young people.

33. Furthermore, young people have not been consulted in a decision that will fundamentally impact their online experience and the age rating does not distinguish between different ages of young people in order to provide tailored, appropriate services: the age 16 benchmark treats all under 16's as a synonymous group.

34. We are additionally concerned that if this age rating is introduced in the UK, without being accompanied by effective age verification measures, there will be an increase in the number of children lying about their age, in order to retain access to social media sites. Using social networks in secret will hinder parent's ability to provide online safety advice, and will discourage children from speaking out if anything upsetting happens online. Children will also be exposed to advertising which is targeted at adults, due to the fact that they should not be accessing the site.

35. Before decisions are made about what age rating is applied, we would like to see research performed, assessing young people's capacity to make decisions about how their data is used, which should inform policy makers in this area. Furthermore, evidence must be gathered, exploring the social, neurological, and cognitive impact of social network sites on young people of different ages. We would also want effective age-gating mechanisms to be introduced, which will prevent young people from attaining access to age-inappropriate services; without such processes, the age rating will be obsolete.

What more could be done by the Government? Could there be a more joined-up approach involving the collaboration of the Government with research, civil society and commerce?

36. The NSPCC welcomes the work being undertaken by Government to help protect young people online, including the introduction of the Child Abuse Images Database, the UK Council for Child Internet Safety, and the WeProtect Global Alliance. However, technological solutions that exist to either safeguard children and young people or flag and monitor suspicious and illegal behaviours are not always fully available or joined up. Some companies are much more committed to this problem than others, and there needs to be greater consistency. In addition, greater attention needs to be placed on what more can be done and what longer term technological solutions could make a difference in keeping children safer online. There is a role for UKCCIS to make this happen and as stated above we believe expanding the power of the proposed age verification regulator will help keep children safer by setting minimum standards.

37. To ensure that young people are able to develop the knowledge, skills, and resilience to use the internet in a safe manner, the NSPCC is supportive of compulsory, age-appropriate PSHE. This would ensure that the most vulnerable young people, whose parents may not be engaged with online safety, are still afforded the opportunity to build digital resilience.

August 2016

NSPCC and Parent Zone – oral evidence (QQ 18-27)

Evidence Session No. 2 *Heard in Public* *Questions 18 - 36*

TUESDAY 13 SEPTEMBER 2016

Members present

Lord Best (Chairman)
Lord Allen of Kensington
Baroness Benjamin
Baroness Bonham-Carter of Yarnbury
Earl of Caithness
Lord Gilbert of Panteg
Baroness Kidron
Baroness McIntosh of Hudnall

Examination of Witnesses

Dr Julia Fossi, Senior Analyst, Child Online Safety Team, National Society for the Prevention of Cruelty to Children (NSPCC), and **Ms Vicki Shotbolt**, Founder and CEO, Parent Zone

Q18 The Chairman: Thank you both very much for joining us. We are very depleted. We do not have all the number that we should, but you are extremely welcome. Everything you say will be faithfully recorded and put on the record. Would you say a few words about yourselves? Although we have your biographical details, it puts it on the record if you also speak them. If you then want to make an opening statement to help us with this inquiry into children and the internet, that will be a very helpful start.

Ms Vicki Shotbolt: My name is Vicki and I run an organisation called Parent Zone. We are, first and foremost, an organisation interested in parenting. We are interested in the quality of parenting that young people get, because we know one of the most important influences on how well a child turns out in life is the quality of their at-home parenting, to use a horrible phrase. Over the last 10 years our focus has been pretty much exclusively on the impact of digital on family life and the profound effect it has had on children's interactions with their parents, and on the requirements on parents to guide their children through a much more complicated space. That is us.

Dr Julia Fossi: I am Julia Fossi. I am acting head of child online safety at the NSPCC. Child online safety is a core priority for the NSPCC. We know that the internet can be extremely beneficial for children, who use it to learn, to explore, to create and to develop. Yet despite the fact that one-third of internet users in the world are children, it exposes them to inappropriate and often damaging content. At the NSPCC we feel it is essential to ensure that children are afforded

age-appropriate, comparable levels of adult protection, care and guidance online as they are offline. We are looking for parity of protection in the online space as offline.

The Chairman: Thank you very much. The first question is from Baroness McIntosh.

Q19 Baroness McIntosh of Hudnall: Thank you. The online world is fairly recent to all of us. Children have always been exposed to risk, including some of the risks we now associate with the internet, such as bullying and pornography. Could either one or both of you talk to us a bit about the differences between the risks children face now online and the risks they faced before we had the internet? Is it simply a question of scale and reach, or are they exposed to different specific risks now?

Ms Vicki Shotbolt: I think it is both those things. One of the things that is very difficult when we talk to parents and encourage them to take a balanced approach to raising their children through these risks is that the reality is that we have a window into children's lives that we never previously had. It has always been the case that children can be uniquely unkind to each other. The difference now is that we can see some of that unkindness and it is recorded for all time. But there is a specific difference about the scale, volume, inescapability—if that is a word—and amplification of those experiences that previous generations did not have.

Some of the risks are new and different. One of the risks that sounds like a very mundane one but is one that parents routinely talk to us about is young people being exposed to things at a much earlier age than they would previously have thought they might be, such as girls of eight, nine and 10 obsessively watching make-up videos and feeling it is important they present to the world a version of themselves that is beautiful enough to go on Instagram. That is quite different. Girls of eight, nine and 10 did not use to have to have that experience. Then there are the emerging risks. The emerging risk of gambling would have been unthinkable a few years ago—that a child of 14 could be facilitated in a gambling habit—because we would have taken offline measures to ensure that they were not going to be. But in an online world, enterprising services have figured out ways to facilitate gambling if you are 14. So there is a mixture of both: it is certainly true to say some of these risks are not new, but it is also true to say that the internet has facilitated risk-taking on an industrial scale and created some risks that did not previously exist.

Baroness McIntosh of Hudnall: Specifically on gambling, are you talking about access that children and young people can now get to adult sites—i.e. there are not enough barriers—or kinds of gambling that have been developed specifically for children?

Ms Vicki Shotbolt: I am talking about the latter: kinds of gambling that have been developed specifically for a youth audience.

Baroness Bonham-Carter of Yarnbury: Is that just by luring them in?

Ms Vicki Shotbolt: There is definitely a lure element and encouraging certain behaviour. One of the very common methods of getting points in an online game is to buy a pack. You have no way of knowing what is in the pack. In effect, you are rolling the dice and seeing whether you get something good or not. There is

certainly a behavioural element to it, but there are also sites that facilitate gambling; you buy something virtual, then you gamble with it. The gambling site will say that it was only virtual, but of course a money transaction has gone on in the background. It is still money.

Dr Julia Fossi: There are similarities in children's offline and online experience, but certain angles and activities take place that are specific to the online world. As Vicki said, the additional impact for children and young people of bullying in the online space is that it is 24-hour. They cannot escape from it. It is everywhere. They go home with it. It is all-pervasive. It is that inescapability and the anonymity the online world offers: it allows people to create fake profiles to harass and bully, should they wish. Equally, we have had a number of calls from children and young people about baiting sites: sites where children and young people develop videos where they go into the local community and say—not in this language; imagine worse language—"Who is the worst girl in your class?" They then identify that individual and upload those on to the internet. So there are newer developments that children would not necessarily have experienced in the past. The knowledge that that is being shared widely and of who can access that material is another form of victimisation for that individual: not knowing who can access it.

The Chairman: Who would host those baiting sites?

Dr Julia Fossi: The contacts we have had from Childline have been children and young people uploading it themselves and it has gone viral. It is older children in the community. Children are using the online space to test and push boundaries, just as they have done in the offline world, but the repercussions and consequences are much greater, not only for themselves but for the individuals they are targeting.

Q20 Earl of Caithness: I would like to explore this a little further. Dr Fossi, you said that the good things for children were to explore, create and develop. In what way could the internet be used more positively in that direction compared with how it is used at the moment? My second question to both of you is as follows. When one talks about the problems that children face, the major problem that seems to come up is bullying on social media. When people are asked what they are going to do about it, the first thing they talk about is pornography. Which is the more insidious of the two? You can go into the British Museum and see any sort of pornography you want as opposed to damaging pornography.

Dr Julia Fossi: Children have the right to explore and use the internet for their benefit. It is there and it should be open to everybody. However, provisions should be put in place to provide an age-appropriate experience for children and young people. In the Digital Economy Bill, the Government have offered to set up an age verification regulator to target pornography in particular. There is a possibility of that regulator's remit being extended so that it can provide a code of practice with minimum standards for providers of internet services, with child protection at its core. That would allow a filtered experience for children and young people so that they were not exposed to inappropriate content. Age appropriateness could be used in relation to pornography, for example. It is fantastic that sanctions will be in place for websites that do not have effective age verification procedures – however, the NSPCC does not believe that the

current sanctions are strong enough, particularly for overseas sites. There should be backstop blocking powers at an ISP level to ensure that those sites cannot be uploaded in the United Kingdom.

So I think that there are huge possibilities. There are technical capabilities that could be applied in the online space to better protect children and young people. Instagram has today launched a filter that individuals can apply themselves so that certain things do not appear on their feeds, and the UK Council for Child Internet Safety has put together guidance for interactive services, setting out best practice. That is fantastic, but who is ensuring that internet service providers are fulfilling or applying those basic principles? The regulator could perhaps look at whether internet service providers are applying the minimum standards, and if they are not it could apply sanctions to ensure that they do.

Ms Vicki Shotbolt: At the risk of going back over ground that Julia has covered, can I pick up on the positive point again? I think that we miss a lot of the positives about the online world. I look at the generation coming through—the 16, 17 and 18 year-olds—who have forged entirely new careers completely by themselves. We absolutely did not guide them towards blogging as a career, yet there are fantastically successful bloggers. For all the football fans in the room, anyone who saw the YouTube charity football match would think it incredible. A generation of young people have done something really special. One thing that we could get much better at is recognising young people who do good stuff online and celebrating it in the same way as we celebrate offline achievements. I do not think we do that enough. It is problematic for parents, because they understand that their children are going to have careers in technology, and children understand that. When we recently worked with children, 70% of them expected to have a career that involved tech. So surrounding them with a space or a narrative that is very negative is not terribly helpful, and we should really challenge it.

On porn and bullying, it is fascinating that we always turn to bullying as a front-of-mind issue when we talk about the internet. I do not think it is correct to do so or that it is necessarily what young people themselves would say, and it is not necessarily what parents say is their front-of-mind concern. That is in no way, shape or form to say that it is not a significant issue. However, it is one that we seem to have caught hold of and can quantify quite easily, and we have organisations in place that can respond to it. Therefore, we are missing a whole load of other things to which we ought to be paying just as much attention.

Turning not least to the porn aspect, there is something very, very different about online porn. I absolutely take your point about the British Museum and the Victorian collections of pornography that we would now describe as art, but the sort of porn that children can access is hardcore, non-consensual and extremely unpleasant. The most powerful description that I had of it came from ATVOD, as it was, which said that this content would not be licensed for sale in a licensed sex shop. So we are talking about a new form of porn that is readily and easily available.

On filtering, I agree that there should be backstops, but I also think that we have done amazing things with filtering in this country. However, there are new services such as Snapchat, which is not that new any more, coming through that do not have parental filters on them. You can use that service once you are 13, and if you have the digital skills, which most kids do, to know how to look for a

porn Snapchat handle, that can be added to the storyline and then you can have a newsfeed of porn on your Snapchat app. So encrypted services are making it extremely difficult for us to filter porn, which is a huge concern given the unpleasantness of the porn that is out there.

Earl of Caithness: Thank you. You said that we could do better. Who are "we"?

Ms Vicki Shotbolt: That is a really hard question. I think it is we, the people. Am I allowed to say that here? I think that the media could do better and that schools could do more—I think we could be more creative in the school curriculum. I also think that parents could be encouraged. Instead of feeding them a diet of "Screen time is bad, bad, bad", we could feed them the fact that there is also good screen time. I think that parents need to hear that. The industry could do better as well. It is possible to find some fantastic apps that help young people to be creative, but it would be nice to see an awful lot more of those being made available so that parents can guide their kids towards the stuff that will be creative, useful and empowering.

Dr Julia Fossi: I think that everybody has a moral, social and ethical duty to safeguard children in the online space. Putting children at the forefront and putting their needs at the front, centre and heart of the designs in the online world would help us to develop a better internet for children. I am thinking about tech developers and engineers, as well as at corporations, industry, schools, and parents and grandparents. A multifaceted approach is needed in relation to online safety.

Q21 Baroness Bonham-Carter of Yarnbury: I am going to ask my questions back to front, because my second question picks up on what you have been saying. It sounds to me as though there almost needs to be a new kind of teacher. How do parents keep up with the new technologies that are emerging all the time? Vicki was saying that Snapchat is being used in a way that was never intended. How can parents, teachers and adults in general keep up with what is going on out there—what the potential for young people is?

Ms Vicki Shotbolt: It is almost impossible to keep up. One of the exciting things about the internet from my perspective is that when working in parenting 15 years ago we used to talk about the democratisation of family life and how teenagers and adults are having to have different sorts of conversations. The internet really has done that. Our young people are guiding this generation. That is good and healthy, except that we also rely on providers to be a bit more explicit about the services they are providing. At the risk of harping on about one particular app, I did a conference call recently with Snapchat and was flabbergasted. I thought that I understood how to use it but clearly I did not, and there was nothing on the device that would have helped me to understand it.

Baroness Bonham-Carter of Yarnbury: So is this something that should be introduced into the education system?

Dr Julia Fossi: At the NSPCC we believe that parenting in the online world is very similar to parenting in the offline world. It is about having regular conversations with your children about the fundamentals of consent, respect, honesty and trust, which apply equally online as they do offline. We try not to bombard parents with the fact that they need to know all the technology; they

just need to sit down with, and engage with their children, see how they are interacting with the online world and help guide them through that process.

Parents need further support on the technical capabilities, particularly for younger children, such as parental controls and filtering in their homes, but there is also an overreliance on this being a parental issue when it involves ISPs. Sky has default-on filtering for the likes of pornography. Why are all ISPs not doing that? It safeguards the most vulnerable in our society; for parents who have multiple adversities, who are unable to cope with their own lives, let alone the online life of their children and young people. Equally, it could be a marriage between schools and parents. Schools need to be aware of parents' concerns in the online space and offer information to parents on what they are discussing in schools. Resources should be provided, not necessarily by schools themselves, to complement the advice and information that children get in the school setting back at home.

Q22 Baroness Bonham-Carter of Yarnbury: That moves on to how effective existing legislation is and where you feel that should go. I am going to ask you about sexting, which is obviously a big problem, and whether you feel that existing legislation is appropriate or whether we need to beef it up.

Dr Julia Fossi: There has been sexting guidance for schools outlining the activity and the risk assessment that takes place.[274] Equally, the police have set up new guidance for police officers. They have developed Outcome 21, which ensures that children and young people who have engaged in the consensual sharing of youth-produced images would not necessarily have it rest on their record. We are moving into the right space. For that specific topic, people are definitely acknowledging that children and young people are naturally curious. They will test out their sexuality. Rather than frame it as, "You must never do this activity", highlight the risks involved and take a well-balanced view as to whether you should take part in it. Fundamentally I will not stop repeating issues of consent, respect and trust, which are the kinds of elements that can often get lost in some of the conversations—the impetus is placed on the individual who shared the image, not necessarily the person who shared it more widely—and take that more holistic approach.

Baroness Bonham-Carter of Yarnbury: Finally on sexting, is the NSPCC aware whether there is a difference between the effect on boys and on girls, and the way boys and girls behave over this?

Dr Julia Fossi: The research highlights that girls tend to be asked more for those images, but recent statistics from the Internet Watch Foundation show that there are equal numbers of boys sharing. The difference is that girls, because of the proximity of the parts being shown, tend to show their face, whereas boys show their genitals and are not easily identifiable. They can equally say, "That's not me". There are differential impacts, but it impacts on both.

Baroness Bonham-Carter of Yarnbury: Do the girls tend to be victims more, as it were? Are the boys showing off?

[274] Dr Fossi later elaborated that Sexting Guidance has been released for schools, outlining the pressures and motivations that children face in relation to sexting – and providing schools with a risk assessment and process for dealing with sexting cases.

Dr Julia Fossi: It is so nuanced. I do not think we can make broad generalisations. Boys feel equally harassed and pressured, and also pressured to show their manliness in wanting to have those images and requesting them from girls.

Q23 Baroness Kidron: I just want to ask a couple of things on age groups. One of the things about the internet, as we are discovering, is that it does not treat children as children but as adults. Of course, not everyone under the age of 18 is at the same developmental stage. As a group we have become very interested in the stages of childhood and what might be appropriate at different times. I will ask you a question about governance, but before I do I will ask for your perspectives on the nature of the technology—perhaps something about compulsion and things that you think are inappropriate for young people of different ages, which you touched on in your opening remarks. It would be great if you would say something about the different age groups and where you feel technology interacts with them in ways that might be problematic.

Ms Vicki Shotbolt: It is an incredibly difficult question to answer because it is so new and because the generations coming through are experiencing it almost for the first time. One of the things I find really quite depressing is the increase in questions we have had from parents about tech tantrums: about much younger children for whom the device has become the thing that causes the big arguments. It used to be vegetables but not any more; it is taking the device away. There is a very legitimate question to be asked about how long for and at what age is it sensible to give a child a device. I do not think we know the answer to that. That is what makes it so difficult. There are fantastic resources on an iPad for a three year-old, so I would never criticise a parent for making the best use of that technology, but there is an issue about that uniquely individual device that is so engrossing being given at that very young age.

Moving on, the debate now is whether the default age for social networking should be 16, and there is the children's rights discussion about whether a child has a right to access the internet from the age of 13 without parental consent. All that says to me is that it is confusing and unclear, and we are not focusing on what is in the best interests of the child. My view is that it is not in the best interests of the child to expect them to sign up for terms and conditions they are unlikely to understand at the age of 13 without any parental oversight at all. I do not see how that can be appropriate in the online world, with all its dangers and complexities, if it is not appropriate in the offline world.

So, for me, there are some key points. There is the toddler question: the question of how we guide parents towards what is sensible for those very young children. What do we do about the point at which we accept that it is all right for a child to be online without any parental oversight, and at what age do we say, "Fair enough, you're old enough now to sign those terms and conditions and go and have fun"? For me those points feel like at aged 13 and 16. At 16 you should be old enough to do that. I say that thinking that I might hide under the desk because we do not know the answers to those questions. I am mindful of that.

Dr Julia Fossi: Absolutely. No proper research or impact assessment has been done looking at the cognitive, neuropsychological and developmental impact the online space has on children and young people. That is urgently needed so we

can provide the resources in an age-appropriate way for children and young people. Our research, in particular the research that we carried out with the Children's Commissioner for England on the impact of online pornography, shows that children and young people are accidentally stumbling across this material. They are not actively searching for it. The fact is that it impacts them negatively however they see it, but the fact that children are as likely to stumble across pornography as they are to search for it highlights that there is absolutely a need to protect children in this space from adult materials.

Children can be affected by a variety of things. Our contacts from Childline and research carried out by EU Kids Online highlight that children and young people are negatively impacted by news content. They get really upset. The difference in the online space is that "inadvertent popping up". They use a social-networking site to chat to friends, then on the side-lines there is a news article, an image, or an advert for pornography that pops up that they are not expecting but have to deal with there and then, with no context or anybody around them to help them understand where that has come from.

Baroness Kidron: Building on that—I understand that you do not have answers to the questions and that the research has not yet been done—what would be the road by which we would work out what sort of governance we needed for the under-18s? You are both talking about things that cannot be avoided, even if you are educated as a parent or a child. We would be interested in knowing what path you would take in looking at a different kind of governance. What would you like to see in place?

Ms Vicki Shotbolt: At the risk of sounding draconian—that is not my default position by any stretch of the imagination—I think that up to the age of 16 we should expect parental consent. That would be my default setting. Let us start from an assumption that, if you are a minor, you ought to be getting parental consent in some form or another. Beyond that, we need research. We need to understand the impact of technology on young people's cognitive abilities and to have some evidence-based policy-making around what is and is not appropriate at different ages. In the absence of that, I do not think that we can just wait and say, "We don't know and therefore it is all right not to expect parents to give their consent". Only parents are in a position to judge how mature their child is or how comfortable they will be in the environment they are asking to join.

Baroness Kidron: You are talking about parental consent, but I am asking about governance of the online space. Do you think that other people in that space also have a responsibility to provide services that are appropriate to the development of the child? I suppose I am interested in that as well.

Ms Vicki Shotbolt: A kind of online ecosystem for children has been built.

Baroness Kidron: That children are using?

Ms Vicki Shotbolt: Indeed. Yes, I absolutely think that other people have a responsibility, but without regulation at this stage I do not think that we are going to see that ecosystem change. I had a teenager with me when I was having a conversation about Snapchat. Someone said, "People have really misunderstood it. It was created to be 'delete by default' but we never promised that it would always be 'delete'. We just said that it was more like a real live conversation. There might be people who choose to record your real life conversation, but we do not encourage them to do that". The teenager with me

in the room said, "That's outrageous, because it was sold to us as 'delete by default'. It was sold to us as something that would instantly disappear". It is at that level of development that we need to say, "That's not all right. You have to be transparent".

Dr Julia Fossi: Parity of protection in the online space can apply. Models exist in the offline space for gambling, for television and cinema certification - that can also be applied in the online space. The Government need to give a clear direction that age verification regulation is needed to safeguard children and young people. As I said originally, it is a case of extending those powers to all aspects of child protection. We have the ICT Coalition principles on child internet safety, and UKCCIS has developed guidelines on best practice. Let us start enforcing those in the governance structure of a regulator, specifically looking at child protection.

The impact that online space is having is relatively unknown. The NSPCC research on pornography shows a desensitisation impact. The more often children view pornography, the less shocked they are at seeing it and the more they are sexually aroused. That is shaping boys' perception of things that they want to try out, and girls are really worried about what is expected of them within that space. That can be magnified across the board to all issues that children are concerned about, such as violent content and harassment. We are seeing an increasing number of children contact Childline about the sexually explicit content that they are being exposed to online. They are experiencing sexual grooming and live streaming. All these things are happening more often. We have got to a critical stage where something needs to be put in place. Let us expand the powers of the regulator that the Government will be introducing. Let us protect children and young people. Let us provide minimum standards and age-appropriate filtered experiences. Children have a right to use the internet, but they need to use it safely. We ensure that children cannot access or buy alcohol in shops, but they can buy it online through an online delivery service. There needs to be absolute parity of protection.

Q24 Lord Allen of Kensington: Can I turn to the issue of trust? Ofcom research shows that 20% of 12 to 15 year-olds absolutely trust the information they get on the internet, whether through search engines or on sites. I am interested in asking a question from two perspectives. First, from the parent's perspective, is that a concern for parents? Are the children placing too much trust in the information they are getting? Secondly, from a child's perspective, what impact does that have on their forming views, prejudices, opinions and so on in later life? It would be fascinating to look at this issue from both those perspectives. Vicki, you might like to pick up on that.

Ms Vicki Shotbolt: It is a completely fascinating question. I fear that I am about to repeat myself and say that, again, we do not know the answers to some of those questions because we are still dealing with the first generation coming through. We did some research on the impact of the internet on young people's mental health. We asked whether people would take advice that they saw online. We asked it of young people and of the professionals around young people. The professionals—a percentage in the high 80s—thought that young people would unquestioningly take the advice that they saw online, whereas the figure for young people was about 40%. So perhaps we underestimate young people's thoughtfulness about the content that they see.

On the other hand, they are on the receiving end of a tsunami of information—there is a vast amount of information—and helping them to navigate their way through it and develop critical reasoning skills is really challenging. We recently ran a project looking specifically at radicalisation and extremism. We talked to parents about how their children were being engaged in extremist views and how the level of debate was incredibly sophisticated. It is happening in their social networks—powerful arguments are being put across to these young people. Parents are simply not equipped to challenge some of the assertions that are being made by sophisticated groups. So I think it is making young people more vulnerable. I do not know that it is necessarily about trust; I think it is about their ability to put an appropriate level of faith in the information that they read and then to be able to contrast it with more reliable information. However, there is a real gap in the area of more reliable information. You used to be able to watch the BBC and would pretty much know that what you saw was true. Now, they are getting their newsfeeds from Facebook, and they have no skilled editors to make sure that what they receive is truthful. That is a real concern.

Lord Allen of Kensington: Is it also a concern for parents, who are saying that they are worried about it because they do not have the tools to be able to address it?

Ms Vicki Shotbolt: I would say that they are challenged by it, but I do not know whether it is true to say that they are worried about it. Parents tend to think, "Where did that come from? Why are you suddenly thinking that that is God's honest truth?" Parents need other facts and information to be able to challenge that and to encourage their children to think in a slightly more open way.

Lord Allen of Kensington: On that point, Dr Fossi, would you treat it in the same way as you would do in the real world: getting children to talk about it? Is that something that you would encourage?

Dr Julia Fossi: Yes. Children have a right to explore different viewpoints. They should not be isolated and put in a completely walled garden, but it needs to be carried out in an age-appropriate way. There is also the question of the transparency with which these companies operate. I think we would all benefit from understanding a bit more about the algorithms that are used and what information is put forward. Again, that is something that an online regulator could ascertain, using self-audits and the reporting of functions across the board.

Ms Vicki Shotbolt: At the risk of slightly disagreeing with the NSPCC, it is a massive ask to say to parents, "Just treat it like you would the offline world", because it is not like the offline world. A parent 30 years ago would not have been faced with detailed questions about the behaviour of a terrorist group in Syria. These are sophisticated propagandists delivering messages to young people who are interested in them and have a right to hear them, but parents need the same sophisticated information to challenge it. At the moment, they are not there.

The Chairman: I see that we have 10 minutes to go and we are exactly half way through our questions. This is the Chairman not keeping you in order. We will have to speed up a bit.

Baroness Bonham-Carter of Yarnbury: It seems to me there is one group of people we are missing out: people between the parents and young children who have grown up with the internet and have learned, like a certain lady in Canada, that it is not very good to put explicit photographs up and so on. I just wonder whether there is a generation that is there cautioning the younger generation.

Ms Vicki Shotbolt: I do not think it is happening. We have an amazing opportunity there, because we have a group of young people aged 17 to 25 who have lived with it and grown up with it. They are quite wise about it—in many ways wiser than the parents we deal with. That is a resource we should unleash.

Q25 Baroness Benjamin: I congratulate both of you on the sterling work that you have been doing over the last two decades or so. Thank you. I think you have brought up this subject quite a few times in questions and in answers, but many parents feel inadequate when it comes to educating their children about online issues and modern technology. We all know that PSHE—personal, social, health and economic—education in schools can cover these issues and threats. In your view, is enough guidance and advice available to parents to enable them to educate and inform their children, or to protect them from inappropriate content?

Ms Vicki Shotbolt: On the very specific question of protecting them from inappropriate content, a lot of information is available. The information issue that we have is of quality. There is a lot of information out there and it is very difficult for parents to figure out what is reliable information and what they should listen to.

Dr Julia Fossi: Advice is available to parents about inappropriate content. The difficulty is that it is everywhere; it is on advertising and music videos. For parents there is a specific challenge if you are looking at it just online. The NSPCC's argument is that it has to be both; there is no distinction for children in these worlds and there should not be for adults. Having spoken to some groups of parents—and there is some research out there—even within the older generation there are lots of people who are brilliant on the internet and understand the issues. "Digital natives" is a dangerous term, because it makes parents feel immediately disempowered. Issues of consent, respect, honesty, trust, what is right, what is wrong and what kind of behaviour you should have, apply equally online and offline. That is a discussion that any parent could and should be able to have. More could probably be done in the advice and information children are given in schools, and having age-appropriate, fun and engaging material in the online space, whereby both children and parents engage after school.[275] There is a dearth of resources in that space, so let us use the online space positively. Let us develop that material so that parents and children can discuss these issues together in a safe environment.

Baroness Benjamin: I know of a parent whose four year-old was sexually abused by a 10 year-old. When the parent spoke to the parent of the 10 year-old boy about what had happened, the parent was in denial. They were not aware of what this 10 year-old boy was watching. You said that a lot of material is available, but obviously there is a problem with parents not understanding it

[275] Dr Fossi elaborated: "There needs to be resources that are available online that children and parents can engage with together after school on these issues."

and not accessing it. What can be done to improve the development of communication about the resources available for parents in denial?

Ms Vicki Shotbolt: Of all the questions you asked, this is the one that makes my heart beat faster. We have a really urgent need for a proper parenting strategy in the UK. It is not about having more information for parents—there is tons of information for parents—but about having proper support for parents; working with parents on their parenting skills, guiding them through the information, explaining it to them and helping them to overcome the very natural response "It would not be my little boy". That is what every parent would say when faced with the reality that their child had done something awful. There used to be a requirement for every local authority to have a parenting strategy. That fell away. It needs to come back. Every school should have a parenting co-ordinator, every local authority should have a parenting strategy and every parent should have access to parenting support to help them make sense of all these complicated issues.

Baroness Benjamin: Through your experiences, are you aware of whether parents are aware of the effect on the mental and physical well-being of their children who are watching inappropriate material? Are parents worried about this?

Ms Vicki Shotbolt: I would have to say no, on balance. The concerns that parents present to us are either after the event—something has happened and they are trying to pick up the pieces—or they are worried about the things that are immediately impacting on family life, such as screen time, in-app purchases and unexpected bills. It is not the long-term effects of some of these issues on their young people. To be fair to parents, that is often because they are just too busy getting through the day job, getting their kids fed, getting them to school on time and doing all those things. Generally, they are in denial. What is quite troubling is that the direction of travel for parents' behaviour seems to be quite a curious one. We have done some research asking parents how many photos they share of their children. The average five year-old will now have 1,500 photographs shared by their parents. Parents are creating digital footprints for their children well before their children are in a position to give consent. Parents do not seem to be becoming more thoughtful and involved; they seem to be becoming a little less cautious.

Dr Julia Fossi: The majority of our contacts on the NSPCC helpline are from parents after an event. As Vicki said, it is after something has happened and they contact us for advice and information. We carried out some research relating to sexting on the kinds of information and advice that parents would like. There was an overwhelming response from parents saying that they desperately want this information. They look for it from the police and the school, in the form of leaflets. There is a desire on the part of parents to have that material in those formats. We shared that research in the hope that other organisations, such as schools and the police, will start developing content as well as ourselves.

Q26 Lord Gilbert of Panteg: Can I just pick up on that last point? You talked quite a bit about challenges that parents face, their anxieties, the role of schools and what parents are looking for. What more could schools do with parents to help them understand the risks, but also the opportunities, of the internet for

children, to understand what their children are doing and how they deploy their digital skills in school? What does best practice look like when schools are working very effectively with parents to take on those risks and explore the opportunities?

Dr Julia Fossi: Best practice is a 'whole-school approach'; whereby schools engage with children and young people themselves, ask them what their concerns are and what they would like to talk about, get parents in and then develop policies and structures with teachers, parents and children together, using best-practice guidelines for schools on their policies and provisions. Equally, it is not the sole responsibility of schools. Research highlights that teachers are also unaware of this. It is about the provision of guidelines for schools, whereby they are given information and research to highlight risky behaviours to be able to spot abuse, to have effective risk-assessments where they can identify children who are vulnerable, and then have a package whereby they work with parents, where appropriate. Teachers also need guidelines about where engaging with a parent might not necessarily be the best approach. It is working with experts in the field and with the police to develop those guidelines, which are then applied in the school setting.

Baroness Kidron: I am interested in the way the conversation is going. It is partly us and your responses, but parents, schools and teachers are overwhelmed. However, the people whom we do not seem to be reaching are the providers of the services and information. Earlier you mentioned Snapchat and the false promise. I would love you to say something about designing for children in the first place so that the terms and conditions are appropriate. I think you said, Vicki, that they are inappropriate—that the providers are carrying inappropriate content. It is not just a case of inappropriate content; the whole world that you are describing seems overwhelming. There is a third party in the picture, is there not? Could you say a bit about that?

Ms Vicki Shotbolt: Perhaps we are saying less about that because it is so difficult to figure out how you can start to influence those services. What is really unfortunate about the online world is that it is incredibly easy to take advantage of young people and their needs and desires. It is often young people who are designing the products and services, so they plug into what young people want to do without necessarily thinking about what is in young people's best interests. It is hard to see how you would shape the market to make it better for people to create good content for young people and have their needs front of mind. Instead, what people are currently asking is, "What will be attractive to young people and how can we get vast amounts of people on to the service?" That is why it is young people who have developed the gambling model, and it is a young company that has created it and made it possible.

Without a level of compulsion—whether it is through regulation or not I do not know—I am at a bit of a loss as to how you make services be designed for children.

Dr Julia Fossi: As I said before, it is about having minimum standards and a code of practice applied in the online space. That information needs to be passed down to university courses, so that child protection is front and centre in the development of anything in the online and technology world. We already have best practice guidelines, so let us apply them and make them mandatory for all sides. These things are designed by 21 year-olds. The feedback that I have often

been given is that it is very difficult for the developers of the apps. They have to get them to market and only when they are popular do they have the money to look at child protection issues. That should absolutely not be the case. It needs to be front and centre. A third of internet users are children. We know from our NetAware research that 98% of children who are under the age that they should be use these sites because there is no effective system of age verification on the sites. However, rather than restrict children, let us develop these online spaces and apps with children in mind. Let us co-produce them with children and young people, looking at their needs and issues. We should put them at the forefront because they are the next generation. They are the ones who will be using them the most. Let us put them at the heart of the issue.

Ms Vicki Shotbolt: Having been slightly melancholy about our chances, I guess we should celebrate YouTube Kids. At least there is a sign there. People banged on about the fact that YouTube was not really a suitable space for younger kids, so Google have come up with YouTube Kids. So maybe some of the bigger providers are starting to hear what we are saying, but I still think it is a challenge.

Dr Julia Fossi: To my mind, with the regulator and minimum standards, consistency of provision would be applied—it would be mandatory. You would not have only one or two sites that were suitable for children and young people.

Q27 The Chairman: To finish, as we have gone a bit over the time, you alluded to the legislative measures or action that might be taken by government and indeed by Parliament along the way. Could you summarise where you think we as parliamentarians should be going and where legislation might lead us? What key things would you like us to take away?

Ms Vicki Shotbolt: I will start because I am going to be predictable and say that first and foremost we should look at proper parenting support. I think that we need to reintroduce the notion of having structured parenting support. That would impact on the quality of support that schools can give. At the moment we tell schools that they should be working with parents, but we are giving them no skills or support to do that. That would be a really positive step. My second ask is that we look at the age at which a child can sign up to different services and who carries the duty of care. Who is responsible for that child when they use an online service? Ultimately we have to have some form of regulator that can enforce some minimum standards and ensure that online services have a duty of care or that they share that duty of care with parents because they ask for parental consent.

Dr Julia Fossi: Mine would be expanding the powers of the regulator to have a clear and accountable oversight function, consistent with that of other UK regulators. I would also include building on self-regulatory principles, and ensuring that children and child protection are the heart of the designs in the online space. Having a code of practice and minimum standards would go an enormous way towards ensuring safety and providing age-appropriate filtered experiences for children and young people in the online world.

The Chairman: That was brilliant—a very tight summary. Thank you very much for that, and that you both for a really useful session for us. It was tremendous. Thank you both for coming in.

Ms Vicki Shotbolt: Thank you for such interesting questions. It was a big hike around all the issues of online safety.

Ofcom – written evidence (CHI0051)

Section 1

One Page Summary

1.1 Ofcom welcomes the opportunity to contribute to the Lords' Communications Committee inquiry into Children and the Internet.

1.2 Our submission provides details of Ofcom's roles and responsibilities relating to online child protection. These include Ofcom's extensive research into children's online access and use; participation in some specific initiatives to address particular online risks; and our responsibilities for regulation of certain video-on-demand services.

1.3 Ofcom conducts regular, detailed research into media use, attitudes and understanding among children and young people aged 3-15, as well as the ways parents seek to mediate this use. Conducting this research is a responsibility placed on Ofcom by Section 14 (6a) of the Communications Act 2003. Sections 2-4 of our response set out the most relevant findings from that research.

1.4 Ofcom has recently participated in two initiatives to address specific online risks. We recently monitored the roll-out of family-friendly network-level filtering, details of which are set out in section 5.

1.5 Ofcom is also a member of the Executive Board of the UK Council for Child Internet Safety (UKCCIS), which include a variety of stakeholders from industry, charities and the Government to discuss and find solution to a variety of online safety issues. As part of our membership of UKCCIS we chaired the UKCCIS social media working group, providing guidance for creators of interactive services for children. Details of this work are also set out in section 5.

1.6 Ofcom also has a limited direct regulatory role in protecting children online through our regulation of adult content and hate speech on notified video-on-demand services, details of which are provided in section 6.

Section 2

How children are going online

2.1 Our response to the inquiry begins by setting out the relevant findings from our research into children's media use, drawing primarily on the following studies[276]:

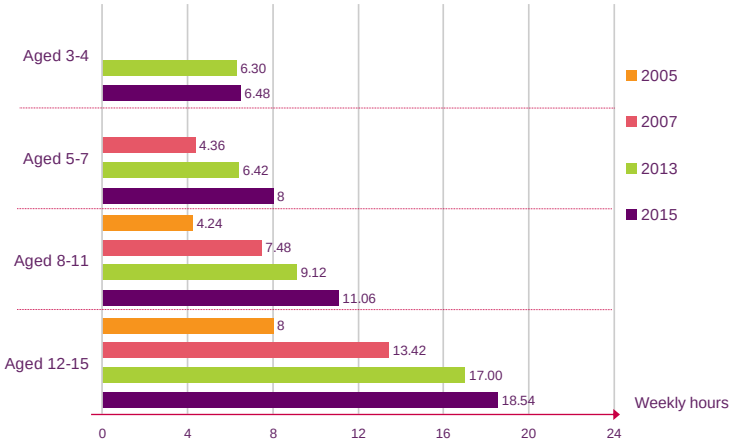
- *Children and Parents: Media Use and Attitudes, 2015.* An annual quantitative research report into the use and understanding of media among children aged 3-15 and the ways in which their parents' seek to mediate that use; and
- *Children's Media Lives: Year 1 findings*, 2014 and *Children's Media Lives: Year 2 findings*, 2015. Reports setting out the findings of Ofcom's qualitative, longitudinal research study, interviewing the same 18 8-15 year olds every year between 2014 and 2016.

2.2 To provide context to our response we first provide some background on how children are going online.

2.3 Thirty-nine per cent of 3-4s, 67% of 5-7s, 91% of 8-11s and 98% of 12-15s went online at home or elsewhere in 2015.

2.4 The amount of time children are spending online is increasing. As shown in Figure 1.1, in 2015 it ranged from 6 hours and 48 minutes a week for 3-4s to 18 hours and 54 minutes for 12-15s. For 8-11s and 12-15s time online has more than doubled in a decade.

Fig 1.1 Time spent online by age: 2005, 2007, 2013 and 2015



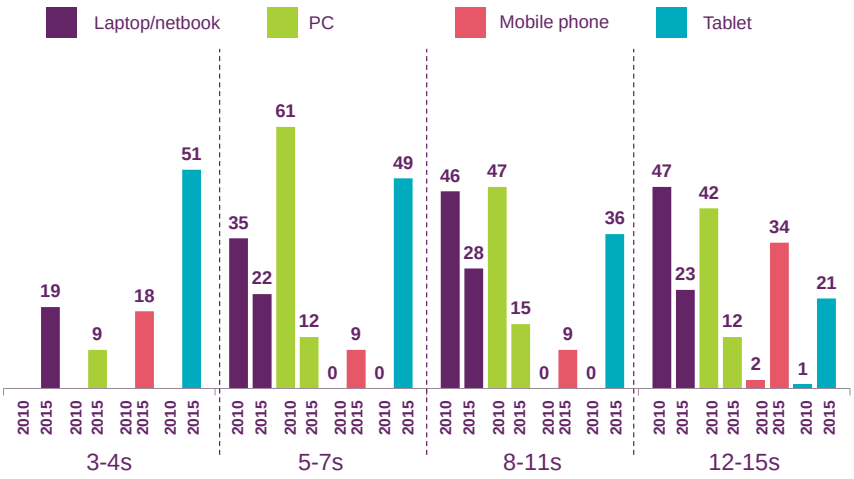
QP25A-B– How many hours would you say he/ she spends going online on a typical school day/ on a weekend day? (spontaneous question, single coded)

276 All our research can be found at www.ofcom.org.uk/medialiteracyresearch

Base: Parents of children aged 3-7 who use the internet at home or elsewhere and children aged 8-15 who use the internet at home or elsewhere (VARIABLE BASE).

2.5 Children are increasingly likely to use portable devices to go online. In 2015 tablets were the device used most often for going online for all age groups except 12-15s, who mostly used their mobile phones. In 2015 one in ten 5-15s only went online using a device other than a desktop or laptop (Figure 1.2).

Figure 1.2 Device 'mostly' used by children to go online at home (2010) or at home and elsewhere (2015), by age[277]



QP24 – And when your child goes online at home or elsewhere, which device do they mostly use? (prompted responses, single coded).

Base: Parents whose child ever goes online at home or elsewhere aged 3-4 (262) or 5-15 (1176 aged 5-15, 260 aged 5-7, 441 aged 8-11, 475 aged 12-15).

2.6 The internet is therefore increasingly central to children's lives. They are spending more time online, and are more likely to be doing this on portable devices. The next sections will set out the benefits and risks of this increased use.

277 No data is available for 3-4s in 2010.

Section 3

Children's online media use - the benefits and risks

3.1 This section sets out the benefits and risks to children identified in Ofcom's research.

Benefits

3.2 Half of parents of 3-4s who go online (51%) and nearly two-thirds of parents of children aged 5-15 (65%) agree that the benefits of the internet outweigh the risks.

3.3 The benefits identified in our research include: education and skills, entertainment and creativity, and for older children, opportunities for social interaction and identity formation.

Education and skills

3.4 Qualitative research conducted by Ofcom found that parents see the internet as an invaluable homework and learning resource for their children. They also felt that gaining proficiency in using the internet would be critical to their children's future prospects.[278] Many of the children in our qualitative research were using technology for homework as well as to enhance their learning in school.

Entertainment and creativity

3.5 Children in our qualitative research were also using the internet for entertainment and creativity. This included using it to enhance their personal interests or passions. For instance Robert, aged 14, was accessing a wide range of websites, podcasts and news sources to expand his knowledge and understanding of football; Brigit, 16, was using Pinterest and YouTube to enhance her crafting skills and Nadia, 10, was having Arabic lessons via Skype.

3.6 The internet, and YouTube in particular, was also used to expand children's creative activities, with, for instance, a number of the children watching video tutorials for drawing and craft projects.

I got this app called Fun2Draw. It teaches you to draw different animals and fruit and things. I think I was just bored one day. I do them every day. Then the other day I found they have YouTube videos too so now I watch them too.

Josie, 11

---

278 *Parents' views on parental controls: findings of qualitative research,* 2012, http://stakeholders.ofcom.org.uk/binaries/research/research-publications/childrens/oct2012/Annex_1.pdf

3.7 Some games also offered considerable scope for creativity, particularly Minecraft which many of the children played in 'creative mode', engaging in extensive design and construction.

Social interaction and identity formation

3.8 As children get older the social elements of the internet become more important.

3.9 In 2015 34% of 12-15s who go online agreed that they find it easier to be themselves online than when they are with people face to face. This is supported by academic research which finds that internet communication may be especially advantageous for shy or socially marginalized children, enabling them to practice social skills without the risks associated with face-to-face interactions.[279]

3.10 In 2015 nearly a quarter of 8-11s who went online (23%) and three-quarters of 12-15s (76%) had a social media profile. The numbers were lower for younger children: 2% of parents of 3-4s and 3% of parents of 5-7s who go online said their child had a social media profile. The qualitative research found that while social media does bring risks (see below), the social interaction it offers was highly valued by the children and social media profiles were used as a way of expressing and developing the children's identities.

Risks

3.11 Children's attitudes to, and understanding of, the concept of risk, and how it relates to the benefits they perceive of being online, change as they grow. A summary of children's attitudes to risk as they develop, produced as part of Ofcom's support of the UKCCIS working group on social media[280], is attached at Annex 1.

3.12 The online risks faced by children in our research include exposure to potentially harmful content and risks created by online contact. In addition, the complexity of the online environment makes it more difficult for children to develop critical understanding.

Potentially harmful content: parents' concerns

3.13 In 2015, 25% of parents of children aged 5-15 who go online were concerned about the content of the websites their child visits (25%). Twenty three per cent were concerned about their child seeing content online that encourages them to harm themselves (23%).

---

279 See for example "Adolescents and the Internet" Nathalie Louge, Cornell, 2006, and "Relationship formation on the Internet: What's the big attraction?" McKenna, Green, and Gleason. Journal of Social Issues, 58, 9-31 2002. and "Adolescents on the net: Internet use and well being": Subrahmanyam and Linht 2007.

280 For detail on this work please see section 6.

3.14 In our qualitative research the range of content that concerned parents was broad and included: violence; sexually explicit content; swearing; horror films and other 'scary' content; content that presented ideas and topics they didn't want their children to know about yet, for instance war or death; and content which might encourage emulation of risky behaviour.

Potentially harmful content: children's concerns and experiences

3.15 In 2015 12% of 8-11s and 8% of 12-15s who go online said they dislike seeing things that are too old for them and the same proportions said they dislike seeing things that made them feel sad, frightened or embarrassed. When we combine these two categories 19% of 8-11s and 13% of 12-15s said they disliked at least one of these.

3.16 In 2015 11% of 8-11s who go online, and 16% of 12-15s, said they had seen something that was worrying, nasty or offensive in the last year.

3.17 In 2015 both 8-11s and 12-15s were most likely to cite their parents, along with other family members, as the people they would tell if they saw something online that they found worrying, nasty or offensive (88% of 8-11s and 78% of 12-15s). For 8-11s this is followed by a teacher (18%) and for 12-15s by a friend (28%). However, the number of 8-11s who said they would not tell anyone if they saw this kind of content went up between 2014 and 2015, from 2% to 5%.

Potentially harmful contact: parents' concerns

3.18 The internet enables contact with known and unknown people which may expose children to harm, either as recipients of abusive messages (cyberbullying) or in allowing them to communicate or share information with unknown people, including adults who may seek to harm them (online grooming).

3.19 In 2015, 32% of parents of children aged 5-15s whose child goes online said they were concerned about their child giving out personal details online to inappropriate people and 21% were concerned about whom their child may be in contact with online. Twenty eight per cent were concerned about cyberbullying and 20% were concerned about their child sharing inappropriate or personal photos or videos with others online.

Potentially harmful contact: children's concerns and experiences

3.20 In 2015, fewer than one in ten 12-15s (7%) said they had added people as 'friends' to address lists or contact lists whom they have only had contact with online, unchanged since 2014.

3.21 In 2015, 4% of 12-15s had sent a photo or video of themselves to someone they'd only had contact with online, unchanged since 2014. A few of the participants in the qualitative research also knew of situations

where girls had sent nude or revealing photos of themselves to others at school, but none had been involved themselves.

3.22 In 2015 we asked a new question about contact via online games. Four per cent of 8-11s and 15% of 12-15s say they chat with people they don't know when playing games online. This can be via text or using a headset. Four per cent of all 8-11s and 7% of 12-15s have experienced somebody being mean, rude or abusive to them, and 2% of 8-11s and 1% of 12-15s say they have been upset by this.

3.23 Our qualitative research found that social interaction in games was mostly between real-life friends. Children showed little interest in talking to strangers online. For those that did, the conversation was typically about the game itself. In-game etiquette discouraged conversations straying into more personal territory.

3.24 Our quantitative research found that 9% of 8-11s and 12-15s in 2015 said they had been bullied in the past year. This was most likely to have been in person, with 6% of both 8-11s and 12-15s saying they had experienced this. Bullying via text message or on social media was less common, with 1% of 8-11s saying they had experienced each of these kinds of bullying, rising to 4% of 12-15s. Two per cent of 8-11s and 1% of 12-15s said they have been bullied through online games, and 1% of 12-15s via photo message or video, or via telephone calls[281].

3.25 However, our qualitative research suggests that children are often subject to abuse and peer pressure on social media and via mobile phones, but are unlikely to call this bullying. For instance, several children reported receiving rude, insulting or racist comments on their social media profiles or as a result of 'selfies' they had posted, but downplayed these incidents, insisting they were not bothered by them.

3.26 The high levels of use of social media for contact with friends and peers also had some downsides. The girls in the research felt considerable image-pressure around their online presence, while among some of the boys there was a perceived need to 'act tough', exacerbated by a tendency to use large group-chat functions on social media (e.g. Facebook messenger, WhatsApp), the more removed nature of which gave boys more confidence to test boundaries and 'show off' among their friends.

Critical understanding

3.27 Critical understanding is a way of describing the skills and knowledge children need to understand, question and manage their media environment. This is important if they are to get the benefits it has to offer, and avoid the risks. Critical understanding covers a wide range of knowledge and skills. The following measures provide an indication of the ways in which the complexity of the online environment can make exercising critical understanding difficult for children.

---

281 In most interviews for the quantitative research the parent is present. While we take steps to allow the children to answer privately, this may result in some under-reporting.

3.28 Children are more likely than in 2014 to think that various kinds of online information are "always true". Between 2014 and 2015 the numbers of 8-11s and 12-15s who visit news websites or apps and who answered that all the information on these sites is true increased (23% vs. 12% for 8-11s and 14% vs. 8% for 12-15s). There was also an increase in the number of 8-11s who say this for sites used for used for school work or homework (28% vs. 20%) and among 12-15s, who say this for social media sites or apps (9% vs. 4%).

3.29 Less than one in six 8-11s and a third of 12-15s in 2015 were able to correctly identify advertising displayed in online search results. In 2015, children aged 8-15 who used search engine websites were shown a picture of the results returned by Google for an online search for 'trainers'. Their attention was drawn to the first two results at the top of the list, which were distinguished by an orange box with the word 'Ad' written in it. Despite this labelling, only a minority of 8-11s (16%) and 12-15s (31%) correctly identified these sponsored links as advertising.

3.30 Less than half of 12-15s who go online in 2015 were aware of paid endorsements by vloggers (47%) or personalised advertising (45%).

Children's understanding of risk

3.31 Children's critical understanding skills are also related to their ability to understand online safety messages. Our qualitative research found that the children in the sample could repeat the safety messages learned from school and parents and explain what they were and were not supposed to do online. However, they did not always understand the reasons behind those messages. This meant they did not apply them consistently in different circumstances or contexts.

Section 4

Parents' approach to mediation

4.1 Parents have an important role to play in helping to manage the risks of children's internet use. Our research provides details on the ways in which parents are mediating this use.

Parents' confidence in managing their children's internet access

4.2 In 2015, 80% of parents of 3-4s and 76% of parents of 5-15s who go online agreed that they know enough to help their child to manage online risks.

4.3 However, between 2014 and 2015 there was a decrease in the number of parents who said they trust their child to use the internet safely, from 56% to 44% among parents of 3-4s and from 83% to 78% among parents of 5-15s.

Parental mediation of their child's internet access

4.4 In 2015 more than half of parents of 3-4s (58%) and 75% of parents of 5-15s who go online said they had looked for or received information or advice about how to help their child manage online risks, an increase from 48% for 3-4s and 70% for 5-15s in 2014. The most common sources of information, among parents of 5-15s, are the child's school (53%), followed by friends or family (40%).

4.5 Over nine in ten parents in 2015 mediated their child's use of the internet in some way, using a combination of approaches including:

- using technical tools;
- regularly talking to their children about managing online risks;
- supervising their child; and/or
- having rules (about access to the internet and/or behaviour while online).

4.6 The majority of parents whose child went online at home or elsewhere (96% of parents of 3-4s and 94% of parents of 5-15s) used at least one of these approaches; 18% of parents of 3-4s and 38% of parents of 12-15s used all four. A very small minority of parents (4% of 3-4s and 6% of 5-15s) did not mediate their child's internet use in any of the ways mentioned above, rising to 12% for parents of 12-15s.

4.7 The technical tools asked about in the research included:

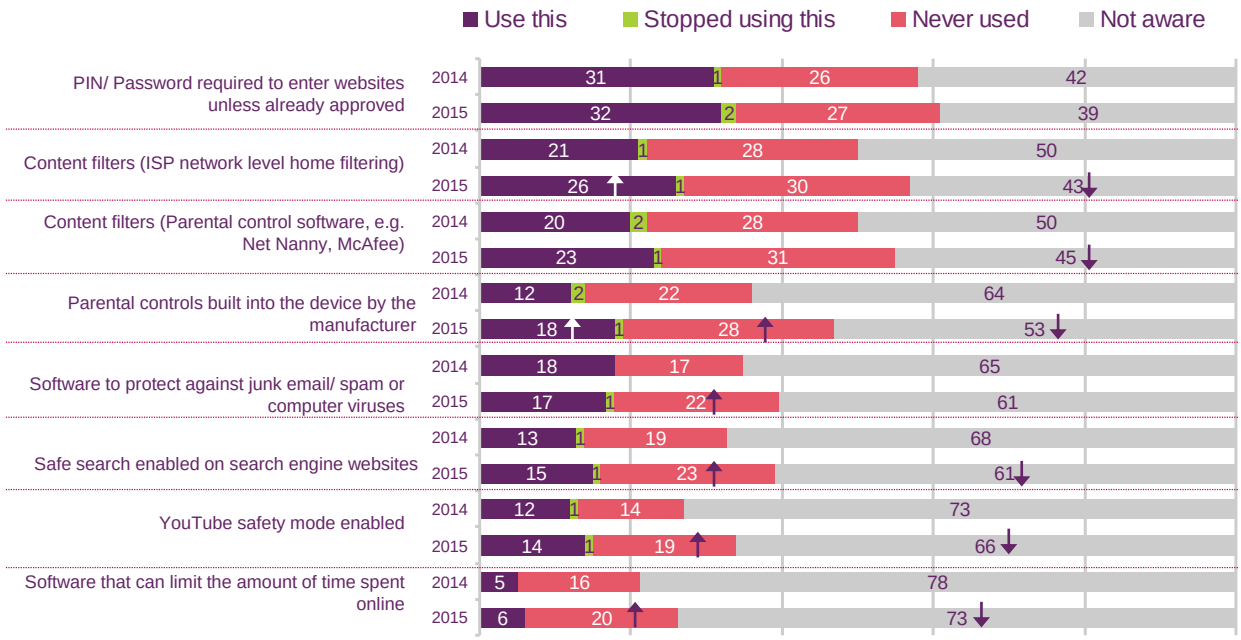
- Content filters in the form of home network-level filtering, provided by the broadband internet service provider (e.g. BT, TalkTalk, Sky and Virgin Media) which apply to all the computers and other devices using the home broadband service.

- Content filters in the form of parental control software set up on a particular computer or device used to go online (e.g. Net Nanny, McAfee Family Protection, Open DNS FamilyShield). This software may be from a shop, the manufacturer or the internet service provider.
- Parental controls built into the device by the manufacturer – e.g. Windows, Apple, Xbox, PlayStation etc.
- PINs/ passwords required to enter websites, unless already approved.
- Safe search enabled on search engine websites, e.g. Google.
- YouTube safety mode enabled to filter inappropriate content.
- Software that limits the amount of time spent online.
- Software to protect against junk email/ spam or computer viruses.

More than half of parents of 3-4s (56%) or 5-15s (57%) use any of these eight tools, with use lower among parents of 12-15s (50%) compared to 5-7s (62%) or 8-11s (61%).

4.8 In 2015 the most widely used of these tools were: PIN/password controls; content filters provided by the Internet Service Provider (ISP); and parental control software set up on a particular computer or device (Figure 1.3).

Figure 1.3 Use and awareness of technical tools among parents of 5-15s who have home broadband and whose child goes online: 2014, 2015



4.9 Among parents without technical tools in place, the top three reasons for not using each are consistent: around half of parents of children aged 5-15 prefer to talk to their children and use other methods of mediation; four in ten say they trust their child to be sensible/ responsible; and around two in ten parents say it is because their child is always supervised or there is always an adult present.

Awareness and take-up of content filters

4.10 Use of content filters provided by the ISP is of particular interest, given the recent joint initiative between government and the major UK ISPs to offer network-level home broadband filtering, also known as family friendly filtering, to all their customers (discussed in more detail in section 5, below).

4.11 Our research shows that awareness and use of home network-level content filters provided by ISPs increased among parents of children aged 5-15s between 2014 and 2015 (see Figure 1.3, above). Among parents of 5-15s with home broadband, whose child goes online, awareness increased from 50% to 57% and use increased from 21% to 26%. There was no change in awareness or use for parents of 3-4s, 65% of whom were aware and 25% of whom used (not charted).

4.12 Parents were also more likely in 2015 than in 2014 to say these tools were useful. Almost all parents of 5-15s who used ISP network-level filters thought they were useful (97%), an increase since 2014 (93%), and about three-quarters thought that they block the right amount of content (77%).

Section 5

Ofcom's participation in initiatives to manage online risks

5.1 Ofcom has recently participated in two initiatives to address specific online risks: monitoring the roll-out of family-friendly network-level filtering and chairing the UKCCIS social media working group, providing guidance for creators of interactive services for children. This section provides a summary of these two initiatives.

Family-friendly network-level filtering

5.2 On 22 July 2013 the then Prime Minister announced an agreement that the four major Internet Service Providers in the UK (BT, Talk Talk, Sky and Virgin Media, or the ISPs) had agreed to offer family-friendly network level filtering to all new customers by the end of December 2013 and to all existing customers by the end of December 2014. The ISPs made a commitment to offer an "unavoidable choice" to all customers as to whether to implement family-friendly network-level filtering.

5.3 In his speech the Prime Minister also asked Ofcom to report on the roll out of the filtering by the ISPs. We did this in a series of reports from January 2014 to December 2015282.

What is network-level filtering?

5.4 Filters block access to websites and internet services which raise potential concern, or pose a risk of harm to children. Every filter:

- categorises content according to specific editorial criteria; and
- restricts access to content in the desired categories.

5.5 Network level filtering goes beyond device level blocking. Device level blocking, where content is blocked on the basis of software on an individual's computer, has been available from the ISPs for some time. Network level filtering is intended to cover all devices in the home in one go, using the home's internet connection provided by the ISPs. Further details are available at Annex 2.

5.6 The ISPs committed to offering this to their customers through a series of measures and communications between 2013 and 2015. They confirmed that their network level filtering would cover websites and any other internet services using standard http protocols and ports. BT, Virgin Media and TalkTalk acknowledged that many mobile apps would not be covered by their filtering services, while Sky indicated that its filter would cover some apps as well as web browsing. Details of the editorial categories blocked are included in Annex 2.

---

282 *Internet Safety Measures: Strategies of parental protection for children online.* A series of reports looking at the roll out and take up of network home broadband filtering. Available at: http://stakeholders.ofcom.org.uk/internet/?a=0

How have customers responded to the roll out of network level filtering?

5.7 The roll out was in two phases, the first was to all new customers joining the ISPs after 2013, and the second to existing customers. The Government set deadlines for those two rollouts, for new customers by the end of 2013, and existing customers by the end of 2014.

5.8 By the end of June 2015 take up of family friendly network-level filtering among both new and existing customers stood at the following levels, as reported by the ISPs[283].

- BT: 6%
- Sky: 30-40%
- Talk Talk: 14%
- Virgin Media: 12.4%

5.9 The ISPs continue to offer family friendly network-level filtering to both new and existing customers.

Potential limitations of network-level filtering

5.10 There are a number of potential limitations to the use of family-friendly, network-level filters, including:

- they cover content but don't address the risks of online contact, so children may still be at risk from grooming and from online bullying and peer pressure;
- they cover children when online via their home Wi-Fi network, but not when children are accessing the internet via 3G and 4G (although in this case they may be covered by the MNO's filters, which are default on so are likely to be on the majority of phones used by children), via public Wi-Fi or via potentially unprotected wireless networks at friends' houses;
- some children could get round the filters, although this is technically complicated and the numbers in our research who say they know how to do this or have done this are low: 10% of 12-15s said they knew how to unset filters or controls to use certain websites in 2015 and 1% said they had done this; 6% said they knew how to use a proxy server to access certain sites or apps and 1% said they had done this; and
- there may be over or under blocking of certain sites.

5.11 As a result of these potential limitations Ofcom also encourages parents to talk to their children about the risks. Our research showed that in 2015 one in four parents of online 3-4s (25%) and 65% of parents of 5-15s said

283 Some of the differences in take-up of family friendly filtering will be due to the profile of the ISPs customer base, with some ISPs having a higher proportion of families.

they talk to their child at least every few months about managing online risks.

The UKCCIS guide to Child Safety Online for providers of Social Media and Interactive Services

5.12 Ofcom is a member of the Executive Board of the UK Council for Child Internet Safety (UKCCIS), which brings together government, industry, law enforcement, academia and charities, working in partnership to help keep children and young people safe online.

5.13 In December 2014, government asked Ofcom to Chair the UKCCIS Social Media Working Group to refresh the existing UKCCIS policy and good practice guidance for social networking providers. Ofcom engaged with stakeholders from the UKCCIS Board, the wider social media industry, academia and the voluntary sector to produce a practical guide.

5.14 The guide is based on six key areas identified by the ICT Coalition, a European Policy body focused on child safety online, and on UKCCIS members' existing best practice.

5.15 To accompany the guide the working group is supporting a 12 month outreach plan targeted at smaller and start-up social media companies to promote a culture in the online content industry of "safety by design".

The Guide

5.16 The Guide sets out research evidence on children's vulnerability online to risks, and the business case for protecting users and brands from damaging online content. It is published on the UKCCIS website[284] and contains detailed advice on:

1. **Managing content**: helping services understand if their content is suitable for their target age range, and if not how to limit access to content with age verification and identity authentication solutions.

2. **Parental controls**: making sure parental controls are easy to use and understanding how parental controls on other devices or services might interact with their website or app.

3. **Dealing with abuse/misuse**: covering the setting and enforcing of community standards, through rules and reporting.

4. **Dealing with child sexual abuse content and illegal contact**: drafted in conjunction with CEOP and the IWF, this provides advice on creating a standardised function for users to report this kind of content, and using a specialist team to review and escalate material to the appropriate channels for investigation.

284 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/517335/UKCCIS_Child_Safety_Online-Mar2016.pdf

5. **Privacy and controls**: drafted in conjunction with the Information Commissioner's Office, this focuses on the privacy needs of children and advises on limiting how much data is collected and published and ensuring informed parental consent is obtained for younger children to help avoid bullying and grooming.
6. **Education and awareness**: encourages services to educate users about safety as part of the experience on their platform.

Section 6

Ofcom's role in regulating video-on-demand

6.1 The UK has long sought to restrict access for children to types of content which it considers may be harmful to children. In addition to Ofcom's responsibilities around broadcast television and radio content, Ofcom also has regulatory duties relating to certain kinds of online content, notably adult content and hate speech on notified video-on-demand services. These are set out below.

Video-on-demand content

6.2 The Communications Act 2003 Part 4A makes provisions for the regulation of UK-based on-demand programme services (ODPS), often known as video-on-demand services, available online. This regulation does not cover all video-on-demand services, but only those ODPS whose principal purpose is the provision of programmes, the form and content of which are comparable to programmes normally included in television services, and which meet other criteria set.

6.3 Ofcom regulates all non-advertising content[285] on ODPS. All ODPS must ensure certain minimum standards are met, including rules that, "if an on-demand programme service contains material which might seriously impair the physical, mental or moral development of persons under the age of eighteen, the material must be made available in a manner which secures that such persons will not normally see or hear it".

Restricted material

6.4 Ofcom has always adopted a precautionary approach to its interpretation of the wording of the Act and included R18[286] material (or material equivalent to content classified in that category) as "material that might seriously impair" and ensured that it must be held behind access controls to prevent minors from accessing it.

6.5 This approach was confirmed by the Audiovisual Media Services Regulations 2014[287] which termed such content *specially restricted* material, and described this as any material that in video form has, or would, receive an R18 certificate, and any other material that might seriously impair the physical, mental or moral development of people under the age of 18.

---

285 The Advertising Standards Authority is our co-regulator in relation to advertising content on ODPS.

286 There is no requirement for material being provided on an ODPS to be classified by the BBFC, but Ofcom is required to have regard to the BBFC Classification Guidelines when determining whether material on an ODPS is R18-equivalent. The R18 content classification is a special and legally-restricted classification primarily for explicit works of consenting sex or strong fetish material involving adults.

287 http://legislation.data.gov.uk/cy/uksi/2014/2916/made/data.htm?wrap=true

Prohibited material

6.6 The regulations also introduced a duty for the regulator to ensure that ODPS do not contain any *prohibited* material.

6.7 Prohibited material means any material which has been rejected for classification by the video works authority (in the UK's case, the BBFC) in a video form, or that would be rejected for classification if it were submitted in video form.

6.8 All material on ODPS, including still images and other non-video content, is subject to these requirements. The rules for specially restricted and prohibited content are published in Ofcom's Rules and Guidance [288] under Rules 11 and 14.

Content access controls

6.9 Ofcom's interpretation of the requirement that people aged under 18 'will not normally see or hear' such material is that for all specially restricted material there should be in place an effective Content Access Control System ("CAC System") which verifies that the user is aged 18 or over at the point of registration or access, by the mandatory use of technical tools for age verification. Each time a user returns to the service, they will either be required to recomplete the age verification process or use an alternative security control such as a PIN or a password.

6.10 Ofcom issues guidance on which technical tools may be acceptable for age verification purposes including:

- Confirmation of credit card ownership or other form of payment where mandatory proof that the holder is 18 or over is required before issue.
- A reputable personal digital identity management service which uses checks on an independent and reliable database, such as the electoral roll.
- Other comparable proof of account ownership which effectively verifies age. For example, possession and ownership of an effectively age-verified mobile phone[289]. Ofcom does not regard confirmation of ownership of a Debit, Solo or Electron card or any other card where the card holder is not required to be 18 or over to be sufficient verification.

---

288 http://stakeholders.ofcom.org.uk/binaries/broadcast/on-demand/rules-guidance/rules_and_guidance.pdf

289 'Mobile phone' here refers to the SIM card rather than the physical handset. For a phone to be effectively age-verified the account holder must have presented proof of identity and age (for example driving licence or valid passport) to the mobile phone operator. An effective CAC system must establish that the owner is the person attempting to access content – for example by demonstrating possession of the phone and awareness of the attempted access. As with other age verification methods, mandatory security controls such as passwords or PIN numbers may be used for subsequent access to the service.

Enforcement

6.11 If Ofcom records a breach or breaches of the Rules, it may consider that the breach justifies consideration of the imposition of a statutory sanction[290] on the ODPS provider.

6.12 As material on an ODPS will often remain available for viewing on-demand for a long period, there may be an ongoing risk of harm where material remains available which potentially involves incitement to hatred based on sex, religion or nationality, or involves potential harm to children. In such circumstances, Ofcom will expedite its processes to ensure prompt compliance.

6.13 Ofcom has imposed financial penalties on the services 'Playboy TV'[291], 'Demand Adult'[292] and 'Strictly Broadband'[293] after these services provided R18 equivalent material without adequate measures in place to ensure that those under 18 would not normally see or hear it.

UK Commercial Broadcasters Association Voluntary initiatives

6.14 In 2015 the UK Commercial Broadcasters Association (COBA) issued a statement indicating that all its signatory members would ensure that the 'catch-up' video on demand content they provide through television platforms meets the same or comparable child protection standards as for their broadcast services. As this content is largely identical to the on demand content they provide on their own websites, COBA signatories have effectively reproduced the broadcasting standards parents have become accustomed to for their online on demand content. This is a voluntary initiative, above and beyond the requirements of the legislation, which Ofcom welcomes.

290 http://stakeholders.ofcom.org.uk/binaries/broadcast/on-demand/rules-guidance/Revised_sanctions_procedures.pdf
291 http://stakeholders.ofcom.org.uk/binaries/enforcement/vod-services/Playboy_TV_Sanction.pdf
292 http://stakeholders.ofcom.org.uk/binaries/enforcement/vod-services/Demand_Adult.pdf
293 http://stakeholders.ofcom.org.uk/binaries/enforcement/vod-services/Strictly-Broadband.pdf

Annex 1

How children and their attitude to risks evolve throughout childhood

Below is a summary of information produced through UKCCIS working group on Social Media on the development of children from 3-18: how they see themselves, their priorities, their behaviour online and their attitude towards risk (Source: Dr. Angharad Rudkin, Chartered Clinical Psychologist, University of Southampton).

3-5 year olds

Overall development:

- They can put themselves in others' shoes, but they are still quite fooled by appearances.
- Beginning to learn that there are social rules to follow.
- Starting to build up friendships but peer pressure remains low.

Key online activities

- Entertainment, particularly games and TV.

Attitudes to risk

- They may be unaware of risks.

6-9 year olds

Overall development

- Play is mainly pretend/role-play, moving towards greater rule-based reality play.
- Becoming socially more sophisticated; the need to fit in and be accepted by the peer group becomes more important
- Learning how to manage their thinking and their emotions. Learning about the complexities of relationships; if they can't manage these it can lead to alienation, bullying and loneliness.
- At around 7, they undergo a significant shift in thinking to more order and logic.
- They are now frequent users of the internet but with limited information on staying safe online, which may make them vulnerable.

Key online activities

- Entertainment and fun – games, films, TV, video.
- Communications largely with family only.

Attitudes to risk

- Largely compliant with messages from school/home – although if risks aren't explained clearly, they imagine their own explanations.

10-13 year olds

Overall development

- Moving towards more adult ways of thinking but still not making decisions the way adults would.
- Very aware of social pressure and expectations; will change aspects of themselves in order to fit in and be accepted by peers.
- Friends are becoming more important.
- More aware of what's 'cool' or not, including brands.
- Girls show a decrease in self-esteem as they compare themselves to others around them.

Key online activities

- Communications with friends; games (for boys), gossip, TV/films, shopping.
- Open communication across a range of sites.
- Visual communication becomes key.
- Development and honing of self-image.

Attitudes to risk

- Developmentally, the strong desire for immediate rewards triggers risk-taking behaviour.

14-18 year olds

Overall development

- Underdoing significant neuro-psychological changes, leading to differences in the way they perceive emotions and make decisions.
- Developments in the pre-frontal cortex may contribute to the increase in risk-taking behaviour seen during adolescence.
- Mental health difficulties such as anxiety and depression can intensify.
- Still have difficulties realising that others can have a different perspective, so may find it hard to work out interpersonal problems.
- Adolescence is a time characterised by idealism, with a tendency towards all-or-nothing thinking.
- Highly dependent on peers for a sense of wellbeing.
- They need to feel as if they are part of a group – yet also want to be viewed as unique.
- Can appear to shun adult influence but still require clear boundaries and support from parents and teachers.

Key online activities

- Communications with friends; games (for boys), gossip, TV/films, shopping.
- Open communication across a range of sites.
- Visual communication now vital and the 'currency' of likes and ratings is very important.

Attitudes to risk

- More settled within peer groups.
- Beginning to get better at the risk/reward equation.

Annex 2

How network level filtering works

Generally, filters block sites in specific editorial categories by identifying the locations of potentially undesired content either through the site's web addresses (URLs) or domain name. Certain sites, such as sites run by charities relating to child safety and sexual health, are whitelisted, and cannot be blocked[294].

The table below summarises the different editorial filtering categories offered by the ISPs. Each ISP allows their filtering categories to be customised by users.

Content	BT	Sky	TalkTalk	Virgin
Alcohol	✓	**X**	✓	**X**
Crime, violence and hate	✓	✓	✓	✓
Dating	✓	✓	✓	✓
Drugs	✓	✓	✓	✓
File sharing	✓	✓	✓	✓
Gambling	✓	**X**	✓	✓
Games	✓	✓	✓	✓
Hacking	✓	✓	✓	✓
Nudity	✓	**X**	**X**	✓
Pornography	✓	✓	✓	✓
Sexual education	✓	**X**	**X**	**X**
Social networking	✓	✓	✓	✓
Suicide and self-harm	✓	✓	✓	✓
Tobacco	✓	**X**	✓	**X**

August 2016

294 For more detail see http://stakeholders.ofcom.org.uk/internet/?a=0.

Ofcom – oral evidence (QQ 79-86)

Tuesday 1 November 2016

Watch the meeting

Members present: Lord Best (Chairman); Lord Allen of Kensington; Baroness Benjamin; Baroness Bonham-Carter of Yarnbury; Earl of Caithness; Lord Gilbert of Panteg; Baroness Kidron; Baroness McIntosh of Hudnall; Lord Sherbourne of Didsbury.

Evidence Session No. 6 Heard in Public Questions 72 - 86

Examination of witnesses

Tony Close, Director of Standards; Lindsey Fussell, Consumer Group Director, Ofcom.

The Chairman: Thank you very much indeed for joining us, Lindsey Fussell and Tony Close. I am going to ask you to introduce yourselves and tell us a little bit about yourselves and where you are coming in on this question of children and the internet. I will start with you, Lindsey.

Lindsey Fussell: Yes, of course. I am Lindsey Fussell. I am the consumer group director at Ofcom, and in this context I look after Ofcom's market intelligence and market research functions through which we conduct most of our media literacy research, including into children's internet use.

Tony Close: My name is Tony Close. I am Ofcom's director of content, standards, licensing and enforcement. I look after a broad range of the enforcement areas of Ofcom's work related to television, radio, video on demand and any work that we have in relation to internet protection and audience safety.

The Chairman: Great, we look forward to your contributions, starting with a question from Baroness Kidron.

Q79 **Baroness Kidron:** I wanted to ask a couple of questions. The first is very general, just for those who have not read your submission in its entirety. Could you tell us the high points—what you think is important about the changes in the media use of young people?

Lindsey Fussell: Of course. I will start by saying that our written submission drew on the 2015 research and our qualitative and quantitative research into children's internet use. In the next couple of weeks we will publish our 2016 reports, so in answering this question I

might draw on some of the updated information if that would be helpful.

Baroness Kidron: Fantastic.

Lindsey Fussell: Of course, you will have the reports shortly anyway. So, three points. Looking at our 2016 research, I suppose the high point is that children's internet use continues to increase across all age groups from three right through to 17, typically by about 75 to 90 minutes a week. If you like, the proportion of children using the internet has not particularly changed but the amount of time continues to grow. As a result—and I imagine this may catch some headlines—children from the age of five to 15 are now spending more time online each week than they are watching television, and that is the first time that we have observed that trend. It is particularly driven this time by an increase in eight to 11 year-olds going more online than watching television. That is the first thing.

The second point that we note is that the growth of portable devices among children continues to rise with increasing child ownership and usage of both tablets and smart phones to access the internet. From the qualitative research, what we see from that is perhaps an increasing division of children accessing child-orientated content on those kinds of devices on their own and television increasingly being more of a sort of family-orientated viewing activity than perhaps it has been typically in the past where we have seen children watching a lot of child content on television as well.

The use of portable devices obviously has a number of implications, some of them quite interesting. Clearly, it does, I would say, increase some of the risks around children accessing the internet on their own, less on the laptop in the family living room, and that having some implication for the level of supervision. From wider research, it also has some implications for children developing the necessary digital skills, which you tend to get through using laptops for the future world of work and so on, which we can explore if you are interested.

The third point I wanted to make—I am sure we will talk quite a lot about some of the risks of the internet for children—is that it is probably worth saying that about two-thirds of parents continue to say that they think the benefits of the internet outweigh the risks and that their children achieve a good balance between online and offline activity, if I can put it that way. Children themselves increasingly see the internet as a crucial part of the way that they live. They do not necessarily make a distinction between online and their broader activity in their world. They see that as a critical part of their lives. I will stop there and give you an opportunity to ask any particular points.

Baroness Kidron: That is very helpful. I wanted to bring you to something that may or may not be considered a risk. It is not traditionally on the list, but the evidence that you put forward about critical thinking is a bit show stopping: that one in five young people think that if it is listed it must be true. A very similar proportion do not even think about whether anything that comes up on a search engine is

true. Does that give you any cause for concern? Secondly, do you think that we need to act—and who might need to act—more responsibly and perhaps delineate what information is for, such as for advertising, and what the source is?

Lindsey Fussell: Yes, I agree. It is a really important issue. I think it is a source of concern that as children's internet use grows—although there is some evidence, which I will touch on, that they are becoming savvier about the internet—there is quite a distance to travel. We have seen some evidence that far smaller numbers of children—and we are now down to quite a small percentage of children—believe that everything they read on social media is true. Children are now much more sceptical about social media generally, and there is some awareness among particularly older age groups about things like personalised advertising on vlogging sites, which they typically access a lot.

We definitely see some evidence that children are becoming savvier, but the type of evidence that you are talking about remains the same. Only a minority of children across all age groups, although the older children get the savvier they get generally, can still identify a Google ad even though it is in an orange box with "ad" at the top. Similar proportions of children to those you were talking about still think that what they get on search engines is likely to be true. Our qualitative research is quite interesting. We find that children often believe there is some kind of authority figure behind search engines who somehow selects those that are most accurate, which is quite an interesting perception.

I think all that points to the fact that there is a distance to travel here. Clearly, there is a regulatory aspect to this that the Advertising Standards Authority take and they have done some things. I know they banned a recent makeup demonstration video for not making clear the links to sponsorship. I do think that a lot of this is less about specific delineation and more, frankly, about increasing children's understanding through education, discussion with their parents, and so on. As I say, from our research, even where the advertising is reasonably clearly delineated, children do not always pick up what that signifies.

Tony Close: Would you mind if I add one point? It is really crucial, because what this is about is building children's resilience online and building their critical thinking powers. I am a member of UKCCIS. Ofcom is represented on the UKCCIS board, and UKCCIS has recently begun a programme of work looking at children's resilience online, what that means and how you might go about improving it. It is at a very early stage, but I think it will be a really fruitful piece of work. I think the Committee will be interested in its findings.

The Chairman: Very much.

Q80 **Earl of Caithness:** Could I take you on to on-demand programme services and your role there? Are there particular difficulties in

regulating this, and do you think that the Communications Act 2003 is now out of date and needs a revision?

Tony Close: That is a great question. Ofcom has been looking after video-on-demand regulation for a few years now, and at the beginning of the year we brought day-to-day regulation of video-on-demand in-house for the first time. It had previously been part undertaken by a co-regulatory arrangement, but we decided that it was a good time to take charge. Our experience is that it is a pretty effective system. VOD services, on-demand services, tend to know what the rules are. There are good levels of compliance within the sector. When there is not compliance, when people breach, we have a good set of tools to take action. We have fined errant providers and we have suspended services, and that has been appropriate. We have directed services to change the way they are behaving, with good results.

One area where it is quite difficult is deciding who is going to be regulated. The scope of video-on-demand regulation is not the clearest situation. It can be difficult to determine who is in scope of regulation and who is out of scope of regulation, and I think that is mainly caused by the fact that is a fairly nascent industry. It is an industry that is undergoing change, and some of the services within the industry that are regulated or are not regulated are very different in character. You have things that are obviously video-on-demand that are like television and should be subject to regulation, but then you have many more niche services where there is a query over whether or not they should be regulated.

Another aspect of scope is determining whether or not services are established in the UK, which is a crucial part in determining whether or not they will be regulated by Ofcom. That can sometimes be very difficult. I do not think that can necessarily be fixed by changes to the Communications Act, but it is a challenge and I think it will remain a challenge for some time.

Earl of Caithness: Can I take you on to a more European context than what we have just been discussing? That is the EU's audiovisual media services directive. As you know, the Commission is thinking of changing that. Do you think that the proposed changes are beneficial? Are they going to help in your role? Could you also enlighten the Committee as to what your thinking is for the future? In two and a bit years' time we might be free of Brussels. How is Ofcom going to work then? Are we going to follow religiously what they are doing across 22 miles of English Channel, or are we going to go our own way?

Tony Close: I will answer both of those in order. The second half is a very difficult question, so I will answer the first half first. On the AVMS directive—sorry, I should check—I am assuming you are particularly interested in the changes that it is proposing around video-on-demand regulation.

Earl of Caithness: Yes.

Tony Close: The revised AVMS directive on video-on-demand regulation makes a couple of proposals. One is to remove some of the

current constraints on who should and should not be regulated. There is the removal of certain important terminology such as "TV-like", which has the potential to increase substantively and substantially the number of services that might fall within the scope of regulation, potentially further increasing the very tricky judgments that I just spoke about. The second, and perhaps more important, is the proposal to extend some form of regulation to video-sharing platforms, a significant proposal within the directive.

Our position is that the overarching objective is a good one. It is difficult to argue that it is not a good thing to ensure that children are protected when they are online, particularly when they are consuming content on video-sharing platforms. It is difficult to argue that it is not a good thing to try to limit race hate and other forms of hate speech online. My worry about the proposal is twofold. The first is that they largely replicate some of the good practice that many of the larger service providers and video-sharing platforms already do on their own, and to that extent there is a degree of gold-plating or unnecessary regulation potentially.

Another potential issue with the proposal as it is currently drafted is that it might also place quite a significant burden on national regulators. For example, I do not know how easy or appropriate it would be for a national regulator to consider specific individual complaints from members of the public about content that is shared on a video-sharing platform. I am not sure in coming up with the proposal whether or not the Commission did a great deal of research on the numbers, the resource burden that might be involved. I do not know whether the team and I could have to consider hundreds of complaints a year or whether it could be hundreds of thousands, if not millions, of complaints a year. I think that is a challenge.

You asked about Brexit. Ofcom, you will be not be surprised to learn, has no specific view on Brexit. I would say, though, that when the Government and policymakers are thinking about how they manage the impact of the UK leaving the European Union they should put at the heart of their thinking consumers and the communications sector—the second biggest sector in the UK behind financial services, I think, so incredibly important for us—and ensure that we have the tools available, perhaps through new or amended domestic legislation, to carry on doing the job that we currently do under the European framework, including the AVMS directive.

Baroness Bonham-Carter of Yarnbury: I may be in completely the wrong territory, so I apologise to everyone. What powers of regulation do you have over video that is embedded in news pieces?

Tony Close: For example, on a newspaper website?

Baroness Bonham-Carter of Yarnbury: Yes, on a news website. It is just I had a very unpleasant experience coming across something that I did not want to look at. I did not see it, I am glad to say, but I am not quite sure how that content is regulated.

Tony Close: I would like to be able to give you a really simple answer, but I am afraid that there is no very simple answer. In deciding whether or not something falls within the video-on-demand regulated space, you have to assess the characteristics of the service as a whole, which means looking at the broad balance of content that it is offering, seeing how much is text, how much is video, whether or not it is provided as a service for the principal purpose of providing consumers with video-on-demand. That leads to some very finely nuanced judgments on a service-by-service basis. It could mean that one particular very text-heavy site—just pick any national newspaper that has a significant web presence but also lots of video—falls outside of regulation because of the balance of text and video, but another that has a slightly different balance of text and video might very well fall inside the sphere of regulation.

Baroness Bonham-Carter of Yarnbury: Obviously, this is something that children can come across quite easily.

Tony Close: Yes, potentially.

Q81 **Lord Allen of Kensington:** Can I turn to filtering? Somebody came to the Committee and basically said that Ofcom merely asked the ISPs to inform it of their take-up levels. My question is: should that take-up be monitored? Should that be part of what Ofcom would do? Should we be looking at the ISPs being accountable for both the quality and the volume of take-up, and, frankly, is that desirable and/or enforceable?

Tony Close: That is a great question. I have had the pleasure of leading three reports for Ofcom on ISP family-friendly network-level filtering. We published three of them over the last few years looking at the rollout and take-up. Also, independently of that process, we monitor reported and claimed awareness and take-up by parents themselves rather than just relying on the numbers given to us by ISPs. We have seen year-on-year increases in both the awareness of filters and the take-up of filters by parents—or certainly the claimed awareness and claimed stated take-up by parents—to the extent that, even absent information given to us directly by the ISPs, our own research tells us that around two-thirds of parents are aware of network-level filtering, what it does and how it works, and a third of parents across the UK state that they also use it in some form or another. That roughly matches some of the figures that we have been given by ISPs as part of the report preparation process, so we are fairly confident that they were telling us the truth.

Our research also says that ISPs have been fairly successful in raising awareness through things like their Internet Matters campaign, a collective campaign on behalf of all the major ISPs that they put quite significant funding into. They have been successful in rolling out filters absent any existing external monitoring or external oversight. In those circumstances, and as we see a continued success with take-up, I would query whether there is currently a requirement to have an external monitoring or an external enforcement programme. I think if we saw a tailing off of take-up or even a decrease or some concern

over lack of awareness or ineffectiveness, perhaps it would be a question worth asking. At the moment, there is a very positive story to tell about network-level filtering and what ISPs have done.

Lord Allen of Kensington: I was interested in your report at point 5.8 about the differential between 6% and 40%. Your footnote said that it was because of the demographics of the various ISPs. That seems a massive differential, and frankly I am surprised that you say that it can be explained by the differential of the customer base. I have two questions. First, have those at the top end, which looks like Sky, done something different to the others, and are there lessons to be learned there? Secondly, do you think we should have default-on filtering?

Tony Close: I think they might be inextricably linked, those questions, so do you mind if I provide one answer?

Lord Allen of Kensington: Yes.

Tony Close: The first thing I would say is that although it cannot be the only reason, the nature of your customer base is an important factor in determining the extent to which people will take up filters. If you have a customer base that has more parents with young children than another ISP, you are probably going to see an increase in take-up of filters. But let us be clear: the two ISPs that have had the most success with take-up—if success is measured by take-up—are those that have adopted a default-on process. I think it is fairly clear, based on behavioural economics, that people are much less likely to opt out than they are to opt in. Of course, it is a small set of data, but I think the default-on in these circumstances has indicated that it drives take-up.

Does that mean that everyone should have default-on? I do not know. There are still differences in the customer base, and I think it should be appropriate for ISPs to decide how they tailor their products depending on who their customers are. Not everyone will have the same results as Sky. It is Sky that had the most results with default-on. Sky has a very family-focused customer base, and if you are an ISP and you know that you have a slightly older customer base who are less likely to have young children in the house, you might well start annoying or infuriating your customers if you make it default-on.

Baroness Kidron: One of the things that we are looking for is trying to create an ecosystem in the world that is good for children. If it puts a few adult customers out, that is a minor commercial consideration versus taking care of children. We know that opt-out works hugely better than opt-in. Is there not a cultural or social argument that we take care of our young for possibly taking that line of inquiry?

Tony Close: I would not disagree, and I think the facts tell their own story. Default-on does drive take-up. It is as simple as that.

The Chairman: But you are not going to do anything about that knowledge?

Tony Close: Ofcom is not the regulator of internet filters. We have had the pleasure of working with the ISPs to monitor the take-up and are

really pleased to be able to witness the positive impact that we think it is having on the child protection debate in the online sphere. There is a question for the ISPs themselves whether or not other ISPs want to follow suit with Sky, whether or not they think that the benefits outweigh the risks to their customer base. It is also for policymakers and for Parliament to decide.

Baroness Benjamin: Do you think there should be legislation?

Tony Close: I do not know whether there is a case for legislation. Based on what we have seen, based on the solid uptake of parents, even with ISPs that do not have default-on, I do not know whether the case is there or not, but other people will have a different view.

Baroness McIntosh of Hudnall: Can I ask a very dumb question to pull this thread a little further? If you have a default-on system and it is universal, how difficult is it to switch it off?

Tony Close: If you know it is on, it should be fairly easy to switch off.

Baroness McIntosh of Hudnall: But if you are going to be annoyed by it, it will be because you know it is on. If you are not annoyed by it, why do you care?

Tony Close: Yes, absolutely.

Baroness McIntosh of Hudnall: I understand that this is not entirely your issue, but just as a matter of interest it feels to a relatively uninformed bystander as though this is making rather heavy weather of what is, in the end, a fairly simple issue.

Lord Allen of Kensington: If it is universal, you tell your customers, "When you get your kit, it is on, and here are the three things that you need to do, fairly simply, to take it off". If we had legislative change, would that move us forward substantially? In terms of new kit, you would also need to address whether they need to do it with their existing customer base. I know from an ISP perspective that is more difficult technically, but it is not enforceable either, provided that you communicate with the customer.

Tony Close: Apart from agreeing with you all, I think the facts tell their own story. Default-on drives uptake. It is a factor in driving uptake, but you cannot argue with the numbers.

Lindsey Fussell: It may be worth adding that having to switch my parental filters back on, having just changed provider, even if you want them on, engaging with the system is a good idea because most filtering systems will have different levels within them and different decisions to take. Of course, I absolutely accept that you may well want to have a basic level as a default-on system, but as a consumer, to be certain that you are blocking what you want to block and not blocking what you do not want to block—and most parents think the filters are getting blocking right—a certain level of engagement with the filter is a good idea to make sure you get that right.

Q82 **Lord Sherbourne of Didsbury:** Can I broaden out the question about

parents trying to manage online safety for their children? Paragraph 4.4 of your submission is packed full of statistics, and I am trying to understand what they mean. In particular, can you deduce from the huge amount of research you have done what proportion of parents do not know what to do? I could not work it out myself.

Lindsey Fussell: What our research indicates, and I accept as charged the statistical heavy nature of it—

Lord Sherbourne of Didsbury: It is not a criticism. I am trying to work out, as I said, how many parents either do not know where to get information or do not have the information and so are bereft of being able to do anything to help.

Lindsey Fussell: We see evidence that parents are accessing a huge wealth of information about this and are actively in increasing numbers talking to their children about it. The latest research indicated that about 85% of parents said that they had spoken to their children about internet safety in the past year. Interestingly, 95% of children said that they had discussed internet safety. That is interesting, because sometimes children and their parents do not tell us the same results in these circumstances.

Lord Sherbourne of Didsbury: Can I interrupt? On that, the children may know much more than their parents.

Lindsey Fussell: Indeed. I was going on to say that we see that parents use a variety of methods in helping their children access the internet and stay online, and that includes discussion rules, filtering that we have just been talking about, and supervision. We see parents saying increasingly that they are using all of those.

This year, for the first time, we asked parents where they got their information from and we gave them a selection of 10 places as to where they got information from about the internet and their children. You will not be surprised that their children themselves did feature on that list, but we see that most parents are turning to schools and to various other what they see as trusted sources, which can be family and friends but also information on websites and so on. I think there is some really good information out there. Tony has referred to Internet Matters, which I think is a great campaign that brings together a real wealth of information. We also work very closely with a charity called Childnet, which does a great job at getting more resources out to schools and to parents.

I think it is one of those things that for parents is not perhaps front of mind every day. They do not sit there and think, "Today I am going to find out about child online safety". They do not go to a single place and say, "I am going to educate myself". They use a wealth of information and a wealth of sources to pick up what they feel they need, and they talk to their children. They apply different rules for their children on an iterative basis rather than, "This is the week I am going to talk to them about it". I do not think we see much evidence that parents do not know where to turn for information. While undoubtedly there are some parents who are not yet talking to their children as much as others,

there is evidence that in increasing numbers parents do talk to their children on a very regular basis about internet safety.

Lord Sherbourne of Didsbury: I understand that whole range of different sources that parents go to. Would it be helpful if there was one place where you could direct parents? Rather than hoping that they will find their way—and obviously the majority do find different sources, schools and family and so on—if there was a central information place that could be signposted when people buy kit and so on, what would be the downside of doing that?

Lindsey Fussell: I am not sure there would be a significant downside. I think we would probably say that the evidence suggests that it is probably not where people would necessarily turn. It is perhaps just not the way people access information now. They do not turn to a single place that they see as trusted, even if it is a government website or something like that. People tend to use a range of sources every day—the people they talk to, the things their children tell them when they come back after an online safety chat at school and so on—to gather information and ideas about what to talk to their children about and what rules to apply in their internet usage. I certainly do not think there would be any harm in more central gathering, but I am not sure that we would necessarily see parents turning to it in droves.

Lord Sherbourne of Didsbury: Do I infer that one of the best things to do would be to encourage schools to do more and more?

Lindsey Fussell: Certainly our research suggests that over half of parents of school-age children in increasing numbers will look first to schools for information about online safety and then, as I say, from family and friends, from internet service providers and on down the list.

Baroness Kidron: May I quickly ask about the quality of information as well as the availability of it? One of the things we are discovering is that there seems to be a huge emphasis on content, on bullying and on certain aspects of safety, but the sort of knowledge that may be an algorithm might not be neutral—the sorts of things we were talking about right at the beginning—

Lindsey Fussell: The critical thinking, yes.

Baroness Kidron: —or, indeed, that when your app refreshes your GPS automatically goes on so everybody knows where you are, those sorts of things that have huge implications on safety are very poorly represented in the whole gamut. Would you like to comment on the quality and range of what is available as well as the multiple sources?

Lindsey Fussell: Yes, that is a fair comment. Probably a lot of child safety online started, quite naturally, with concerns about content, online bullying, hate speech and that kind of thing, which we have talked about and which children might see, and about safety and children sharing personal information about themselves and explaining to children that people are not always who they see on the internet. All those concerns are entirely natural and probably first spring to mind for parents and tend perhaps to attract the most media coverage.

I think it is fair to say that they have potentially swamped some of the more important information on critical thinking. Certainly, some of the work that we have done with Childnet and others is increasingly exploring fact sheets and other things that we provide to schools, and we need to talk to young people about that kind of critical thinking in a much broader way, recognising advertising and the sharing of personal data in a much less overt way than has been done previously. It is fair to say that that is a space where more could be done to encourage greater understanding.

Baroness Kidron: Is Ofcom willing to look into advertising some of that?

Tony Close: Maybe not advertise but—

Baroness Kidron: I do not mean advertise. I am referring to the extent.

Tony Close: Yes, absolutely. I think we probably do it already with varying degrees of success. I mentioned our role on the UKCCIS board earlier. In addition to being a board member and leading a number of the groups, we also provide all the information and all the media literacy work that we do in this area, including our work on critical thinking—and you are right, there is not a lot of other information out there—to the evidence group and try to ensure that it is socialised with the kinds of industry players and non-industry players that have a direct relationship with children and with parents. I do not know how successful that process is at the moment, but it is certainly something that we are working on.

Baroness Benjamin: Do you think that is the reason why more parents are engaging with finding out more information about how to keep their children online? Why are there suddenly more and more parents being proactive?

Lindsey Fussell: Obviously, it is difficult to say, but I would guess that it is driven by the increasing amount of time that children are spending online in a way that is perhaps less visible to their parents. As I say, the switch from more traditional TV viewing into access to the internet via portable devices is encouraging more parents to feel that they need to take an active interest in what they are doing and to talk to their children rather than relying on perhaps more active supervision at all times.

Tony Close: I think it is worth adding that our own research on parents' resilience or parents' critical thinking or understanding of the risks of the internet indicates that over the last few years we have seen more parents using the internet more often to do more things and that there is an increased awareness of the risks of the internet. I was quite startled about four or five years ago to see some of our research that showed that parents thought that television was more dangerous for their kids than the internet. That is not the case now. I think it is that level of awareness that plays a role in driving parental engagement.

Q83 **Baroness Benjamin:** I spent some time at Ofcom, and I have heard it

said that Ofcom always shies away from regulating the internet, but you have announced that you will be working with the Information Commissioner's Office to regulate the internet of things. Does this indicate a change in policy to greater intervention in the regulation of the internet in the UK? Perhaps you could tell us what internet of things means.

Tony Close: I am going to begin with an apology. Neither Lindsey nor I know a great deal about the internet of things. There are lots of really bright people at Ofcom and many of them know about the internet of things, but we do not really. I will do my best to provide part of an answer. If you are not happy with my answer—and I suspect that I will not be able to cover it in sufficient detail—I will commit to ensuring that we will ask someone who knows what they are talking about back at Ofcom to provide you with the relevant information and the relevant answer.

The starting point for my answer is, no, I do not think this signals a change in our attitude towards being the internet regulator. I think it indicates that we think that we can play a crucial role helping people who are the primarily responsible organisation, such as the ICO, when it comes to data privacy issues online. We can help them with our resource and our understanding of the internet, the technology and the issues facing consumers. We can collaborate with them, the Government and other agencies to ensure that they come to good outcomes for consumers.

Our formal regulatory role in relation to the internet of things is probably quite limited. We are very interested in ensuring that it does not have a potentially negative or dangerous impact on the management of spectrum, for example, but has a clear regulatory role in ensuring that our management of spectrum on behalf of the Government is not impacted upon by wireless devices that facilitate the growth of the internet of things. I do not think that in and of itself is a signal that Ofcom is ready to change its tack and become the internet regulator, but we are absolutely ready to ensure that we can help people do a great job protecting consumers in relation to the risks associated with the internet of things but also to ensure that people understand the benefits as well.

Baroness Benjamin: Why do you not feel you can be the regulator of the internet? What sorts of challenges do you think that will bring that you will not be able to cope with?

Tony Close: That is a really big question. Being the regulator of the internet is not just one thing. The internet is many things. Ofcom currently regulates 2,000 television and radio services that span the globe. Ofcom regulates fixed telephony, mobile telephony, the airwaves, the post, and we are just taking on the BBC, which will be the most significant cultural change and change to our remit since we began 13 years ago. My fear about being the regulator of the internet in any guise is that it fundamentally jeopardises our ability to carry out all our other duties with a degree of effectiveness that I think everyone round the table would expect us to. I think it is as simple as that.

Baroness Benjamin: Do you have anything to add?

Lindsey Fussell: No, not at all. I think it is a huge issue, but if, as Tony said, you want us to provide more information specifically on the internet of things we are very happy to do that.

Baroness Benjamin: I think it would be helpful to us to know what the internet of things means and whether it feeds into our concerns on children. We need to drill down to find out if people can infiltrate into an area where they should not be by hiding behind these sorts of things. That is what I am trying to get at.

Tony Close: Do not get me wrong; the obvious issue, certainly for us and for you, with the internet of things is the data privacy issue, which has a particular child focus. Nobody wants an environment where people are able to snoop on children, abuse the trust of children and use, analyse and distribute their data in a manner that is unsavoury. The Information Commissioner is the existing regulator for data in that sphere. What we would hope to do is help them carry out a great job in regulating privacy of data.

Baroness Benjamin: How will you be helping them?

Tony Close: I will come back to you with an answer.

Baroness Benjamin: Yes, because we are really interested to know. This is not flippant but something that we really need to understand. We need to understand the role that you will play and what the internet of things means, because it is a broad picture and if people do not look at this it can be harmful to children.

Tony Close: I am happy to commit to providing more information on that.

The Chairman: More to follow.

Q84 **Lord Gilbert of Panteg:** We look forward to that information. Could I turn to social media? From your evidence, do you have a view as to whether the age limit for signing up to a social media account should be 13 or 16? In any event, is it an academic question? Is it in any way enforceable? We have just heard from the BBC, which does an amazing job of monitoring how young people engage with them through other social media platforms, but it is massively labour intensive. It is very intense monitoring and moderation. Is there any other route for either enforcing or monitoring the use of social media by young people?

Lindsey Fussell: Perhaps I will say a bit about research and what that indicates, and then I will hand over to Tony to talk about regulation and enforcement.

The first thing to say is that latest research indicates fairly stable but with some increase in children's social media use. Around a quarter of eight to 11 year-olds and around three-quarters of 12 to 15 year-olds have a social media profile. Facebook is still the most likely one, although we see increasing use of Instagram, Snapchat and so on. Quite interestingly, we did a bit more work on this this year and it is not

a flat curve. There is a very sharp uptake of social media at certain ages, particularly at 10 and around the 12-to-13 mark. The 12-to-13 mark certainly indicates that that 13 year-old barrier is quite well understood. The 10 mark is perhaps somewhat harder to decipher.

The qualitative research suggests that many children, whether they are under or over 13, are signing up for these sites with parental knowledge, so not necessarily all of this is going on without parental consent. I think that indicates that the 13 year-old limit or cap is quite well understood—and certainly sites like Facebook do a lot to try to enforce it—but also that children themselves see social media as an increasing part of the way they interact with others. I suppose what we see now is increasing use of group chat services, and children will talk about that as the way they talk to their friends, do their homework, live their lives. In other words, what you are regulating is perhaps quite a lot more about behaviour and culture than something that is a bit more rules based. Tony, you might want to say something about regulation.

Tony Close: Could you be a bit more specific about the regulation or enforcement aspect of the question?

Lord Gilbert of Panteg: I am thinking about whether organisations that engage with young people through social media are heavily moderating. The BBC told us that they moderated very heavily and if they have an inkling, I think they said, that somebody is under the age of 13, then they do not engage with them through social media. You just mentioned Facebook. At what point is the enforcement in place? Is it at the point of sign-up? Do they have any due diligence process or is it through moderation and deriving an inkling that somebody is under the age of 13?

Tony Close: My understanding of the practice is that it varies significantly from provider to provider. Facebook is probably an example of best practice, although it does a lot of its quality assurance, to put it another way, through moderation. A number of other service providers are not as proactive in probing the consumers that use their services. The BBC is obviously a great example of a socially conscious organisation that will go to great length to ensure that they are not interacting with people under the age of 13.

I am struggling with imagining what an enforcement or regulatory regime might look like. I think it would have to attach to the protocols or principles of practice that you have in place as opposed to a monitoring or enforcement of your specific interactions with the millions of individuals that you might have on your service. I am not sure what an effective enforcement regime would look like, but I know that there are models of great practice out there. Facebook is one, the BBC is another. It is not universal, but a number of social media providers could learn from their peers.

Lord Gilbert of Panteg: Is that an area that you would explore—educating providers in the gold standard that you say is provided by the BBC, Facebook and others?

Tony Close: It is an area that we have had a bit of experience of recently and we have had the privilege to be involved in. Last year I think it was—it may have been the year before—the then Secretary of State asked us to lead a specific working group on best practice guidelines for social media providers, which enabled us to get lots of social media providers around the table, and people with an interest in child safety online in particular, to come up with a set of principles and guidelines that represented best practice, borrowing heavily from some of the really good practice out there but also coming up with what we think is a consensus of what represents good practice.

Having published those guidelines for social media providers, we have spent the last year finding novel ways to hit start-ups, new services, services that have not already got the systems in place to ensure that they are properly moderated, to ensure that they are dealing adequately with young customers, to socialise those best practice guidelines, to ensure that people build them into their business case when they start thinking about a social media business. There are lots of great examples out there and there are lots of great examples of not so good practice that people can learn from as well.

Baroness Kidron: I am sorry to pick up on this, but the stats show a quarter of eight to 11 year-olds, who are clearly under the age of 13, and then however many others. We are talking about millions and millions of children who are under 13 regularly with a Facebook account, with or without their parents' permission, yet Facebook is the gold standard. I am hugely sympathetic to Ofcom for not wanting to get into this space because it is so enormous and the capacity argument is pretty enormous. But we are then left with ICO with the data, you with a little bit of the education, and millions and millions of children using these services—I do not know whether it is illegally or at least services to which they are not supposed to be signed up—and no regulatory presence. I am just curious that we are selling Facebook as the gold standard, there is no regulatory presence because of capacity, and it is all rather haphazard. I am not saying whether anything is right or wrong here; I am just beginning to grasp a picture that seems unsatisfactory. Obviously, you cannot fill the gap if it is not your responsibility, but I am interested to know from you whether you are prepared to say there is a gap. This seems a yawning gap, to my level of understanding.

Tony Close: Am I prepared to say that there is lots of good practice out there? It is not always well co-ordinated and it is not perfect, absolutely. More needs to be done to ensure that not just social media providers but more online platforms, more online providers, behave in a consistent manner in the interests of their customers. Absolutely, lots more needs to be done. While I describe Facebook as the exemplar or gold standard, they do so many good things. They are not perfect, but they do so many good things to ensure that their customers—

Baroness Kidron: No, I recognise that they do some very good things and are absolutely brilliant about bullying, for example. I understand that, and I am not anti-Facebook at all. I am just interested how they

can be an exemplar if they have tens of millions of underage users. That is just a bit difficult for me.

Tony Close: No, I appreciate that. My final point would be that they are not perfect, but they try hard to ensure that they have decent guidelines in place and that consumers understand what they can expect from Facebook. There are social media providers out there and other online providers that do not really bother to do that. They do not have the presence or size of Facebook and they can learn from them. I feel as though I have mentioned Facebook too many times now. There are other fabulous social media providers.

Baroness Kidron: No, and to be fair I am not interested in Facebook either. I am just saying that there is a gap of provision or regulation for the millions of children who are using things under age. That is a much bigger issue, not one or the other service.

Lindsey Fussell: It is probably worth saying that we ask children whether they have a social media account. I am not suggesting, by the way, that none of those children have Facebook, but some of them will say yes when what they mean are the types of accounts that are reasonable, that are effectively very heavily constrained spaces that are suitable for children under age, and many of them would certainly probably say that their mum or dad had agreed to them using either that site or one of the other sites. I guess from a Facebook perspective, or indeed any social media site, that if parental consent has been given and they go on to moderate and try themselves to pick out anybody who is under the age of 13, it is quite hard to know what extra provision they could put in place to try to prevent children who are under the age signing up to those sites.

Lord Gilbert of Panteg: Are you aware of any really powerful moderation tools—the BBC depends very heavily on human moderation—that are enabling providers to identify potential under-13 year-olds using their platforms?

Tony Close: I think the providers themselves would probably be better placed to explain the technology behind it, but it is worth saying that many of them still rely on banks and banks of human moderators, which is obviously not without its faults.

The Chairman: Do you not have any idea what proportion of the three-quarters of 10 to 12 year-olds who have social media accounts have had parental consent for them?

Lindsey Fussell: No, we do not. I should say that the three-quarters actually referred to all the children—the 11 to 15 year-olds—which will obviously encompass a good proportion of children who are 13 and over.

Baroness Kidron: Might I suggest to Ofcom that they count to 13 next year?

Lindsey Fussell: Yes.

Baroness Kidron: I am not even in particular favour of the COPPA law that says 13 or of banning children. I am just saying that if that is what is in place, should we perhaps count to that place?

Tony Close: That is a good point.

Lindsey Fussell: We certainly can look at that.

Q85 **Baroness McIntosh of Hudnall:** I think some of what I wanted to ask has been covered one way and another by the way the questioning has gone in the last 10 minutes. What I am hearing—please correct me if I am wrong—is that Ofcom, for perfectly sensible and understandable reasons, is continuing to shy away from the notion of having any explicit regulatory role in relation to these platforms and a number of other things to do with the internet. But I am also hearing you say, "We know there is lots of good practice out there and we are trying to get people to talk to each other so that that good practice can be disseminated". That is "regulation-lite" to say the least, but it does imply that you recognise that you are in a very good position to provide an overview of practice that can be shared. You may want to challenge me about that, but I am not going to let you this second. However, it has been put to us by more than one witness that Ofcom should have the power to regulate in the sense of requiring online platforms to reveal their working practices so that it can be verified that they are transparent and that the practice is as good as it can be. I sense that you do not want to have to do that, and I understand why but, leaving aside the resource issues, is it desirable and can it be achieved?

Tony Close: Okay, I will leave aside the resource issues. I find myself in this odd position. Each day I come in and I am responsible and deeply committed to ensuring that different constituencies of people are protected from bad things. That is my job and that is the job of all the people who work with me. That is their noble purpose each day when they come in. I do not want to come across as flippant or not conscious of the significant risks to the most vulnerable in society presented by the internet, but I find myself cast in that role as we have the discussion today.

I am not going to talk about resource, but I am going to talk about a couple of things. The first is that although Ofcom is not and does not want to be the regulator of social media or the broader internet, that is not to suggest that providers in this area are wholly unregulated. That often goes unspoken. There are a significant number of constraints on their behaviour, not all relating to child internet safety, but some of them are linked. They are subject to data protection provisions. They are often investigated and the subject of successful investigations. They are subject to a number of obligations relating to otherwise unlawful content, not just copyright but child abuse images and other unlawful content. They proactively engage on a voluntary basis with a range of agencies that all have a role in ensuring that some kind of consumer good or protection for the most vulnerable is achieved.

It is not just that they have good practice in place. It is that they are, in fact, also bound into a number of obligations. They are not

unconstrained, swirling around wildly causing untold damage to people, and if they were I think the case for regulation would be much stronger. It is in part because they are constrained, there are checks and balances on their behaviour and they proactively engage on a voluntary basis to ensure better outcomes for kids and other vulnerable consumers that I do not think the case for regulation is as strong as it would be. That is why I do not think that Ofcom should regulate it, because I just do not think the case is there.

Baroness McIntosh of Hudnall: By the way, I hope you do not go away feeling that you have been cast in the role of somebody who does not take this seriously—on the contrary. If I have understood what you just said, you not only do not think Ofcom should regulate, you think that it is not necessarily a good way forward to think of any further regulation in this area.

Tony Close: At the moment, yes. At this time, based on my understanding of the existing constraints placed on these providers and their willingness to engage and submit themselves to further constraints and good practice, I do not think there is a very, very strong case for regulation in this area at the moment.

Baroness McIntosh of Hudnall: You are saying that there is a significant quantum of good will, which is already operating to moderate some of the harms that might ensue?

Tony Close: Yes.

Q86 **The Chairman:** We are more or less out of time. I will try a couple of quick questions in case you have something very significant to add to the excellent presentations you have made already. Some people have told us that, in respect of its age verification provisions, the Digital Economy Bill should give a regulator, not necessarily you, the power to require that access to non-compliant sites should be blocked. How do you react to that?

I will throw you the other question as well. Either or both can take one or the other. What about the famous EU net neutrality regulation that we keep hearing about? Could that have an impact on content?

Tony Close: It is helpful. They are linked questions and I will tell you why. You will not be surprised to learn that we do not want to be the regulator of age verification for a range of reasons, but we do recognise that at the heart of this proposal is a rock solid foundation, a public policy objective to protect the most vulnerable in society from harmful sexual material. Again, that must be a good thing. We are also really pleased that the BBFC, a very trusted partner of ours with a great deal of experience in content assessment and working in the online arena, has agreed to play a crucial role in this. I think that is a really positive step.

There are some challenges with the scheme as it is proposed. We responded publicly to the Government's consultation earlier in the year, and we pointed out that, for example, the scheme does not require ISPs

to block on a firm statutory footing. If ISPs were to take any action blocking non-compliant sites, they would do so on a voluntary basis. That is quite tough to enforce, but it also puts ISPs in quite a tough spot. I think you might have heard from ISPs about the legal difficulties they think they would face if they were to undertake voluntary blocking to secure compliance in this area: that it would raise issues in relation to net neutrality. I think we agree with the points they have raised. A big challenge with the current proposals around age verification centres on the ISP's role, which neatly leads me to your other question.

The EU regulation on net neutrality limits the circumstances in which ISPs can block content. What it does not do, though, is render ineffective many of the other excellent measures out there at the moment. It does not impact on the network-level filtering that we have been talking about today. The reason why we think it does not impact on that is because at its heart consumers are provided with a choice in relation to network-level filtering. They are able to turn them off or turn them on, so it does not suffer from the same net neutrality problems as a broad and mandated blocking program does.

The Chairman: That is a helpful and very clear response, thank you. Lindsey, any final comments from you?

Lindsey Fussell: No. Thank you very much. We are delighted that this review is taking place. It is a really broad-ranging review, but it covers, as we have been discussing, some hugely important issues that we are interested in. We will publish our research in a couple of weeks, but we obviously very much look forward to seeing your report as well.

Tony Close: Thank you very much.

The Chairman: Great. Thank you both very much indeed. Do not worry, we feel you are very much on the same side as we are in all that we are doing. Thank you for coming.

Ofcom – supplementary written evidence (CHI0060)

The Internet of Things

This note contains further information the Committee asked Ofcom to provide on the following topics:

- definition of the Internet of Things;
- what work Ofcom has undertaken in this area; and
- any potential risks for consumers and children

What is the Internet of Things?

The Internet of Things (IoT) describes a range of devices, including everyday objects, that are connected to the internet and can share data to provide a range of new and innovative services and new ways to use devices.

The IoT is an emerging area and has the potential to bring significant benefits to citizens and consumers across a number of sectors, including smart cities, transport, healthcare, utilities, agriculture, manufacturing and consumer electronics.

In contrast to conventional Internet access, where individuals use a network connection to access content, the IoT involves devices that are able to connect and interact with one another via the Internet.

Examples of how IoT is already working or may soon work in specific sectors are:

- Healthcare: remote monitoring of an individual's health to improve recovery from illness, track fitness levels, treat illness, encourage a healthy lifestyle and reduce hospital costs.
- Transport: collecting information from vehicles to improve traffic flow, allow drivers to avoid traffic accidents and provide information for better vehicle design.
- Utilities: connecting a wider range of household, office and industrial equipment to enable their use of energy to be monitored and potentially changed, with implications for cost-saving and reduction of utility bills.
- Smart Cities: a range of technologies and applications can be used to address some of the on-going challenges faced by cities and communities. For example, connecting public transport and infrastructure, including parking spaces, could make it easier to provide better information on congestion and transportation options.

Ofcom's work that relates to the Internet of Things

Given these potential benefits, Ofcom has been following the development of the IoT sector.

As a first step in informing our own thinking on the subject, in 2014 Ofcom commissioned and published research[295] on IoT application characteristics and their potential impacts on spectrum.

In July 2014 Ofcom published a Call for Input[296] which aimed to:

- identify potential barriers to growth and innovation in the IoT sector;
- seek views from stakeholders and consumers on what role Ofcom might potentially play in helping overcome these barriers.

In January 2015, following our Call for Input, Ofcom published a statement[297] which identified four key issues related to successful future development of IoT services, some of which fit within our existing duties and others were where there is potential for Ofcom to play a collaborative role. These were:

- **Spectrum:** Ofcom is responsible for the management of spectrum in the UK including radio spectrum used by wireless IoT devices. In March 2016 we published a statement[298] which sets out that, in the short and medium term, there is likely to be sufficient licensed and unlicensed spectrum available for IoT use, but we will remain vigilant in this area.
- **Network security:** Ofcom has a duty to ensure that appropriate measures are taken to prevent and minimise the impact of incidents that affect the security and resilience of communications networks some of which may be used by IoT devices.
- **Numbering:** Ofcom remit includes the management of telephone numbers, some IoT devices might use these numbers to identify themselves on the network.
  Data privacy: Ofcom has no specific duties with respect to data privacy, which instead falls within the remit of the Information Commissioner's Office (ICO). However, we see a role for ourselves as a collaborator and facilitator in this area, working with the ICO, Government, and other regulators and stakeholders in relation to the secure collection, sharing and analysis of personal or commercially sensitive data.

Most recently, Ofcom has commissioned a study on the technological progress being made in IoT and how the surrounding market is developing. The outcome of the study is expected to be published in the first half of next year.

---

295 https://www.ofcom.org.uk/__data/assets/pdf_file/0040/68989/m2m_finalreportapril2014.pdf
296 https://www.ofcom.org.uk/__data/assets/pdf_file/0014/29012/iot-cfi.pdf
297 https://www.ofcom.org.uk/__data/assets/pdf_file/0025/38275/iotstatement.pdf
298 https://www.ofcom.org.uk/__data/assets/pdf_file/0029/78563/vhf-iot-statement.pdf

Potential risks for consumers and children

IoT applications may be applied to a large number of previously unconnected consumer and non-consumer devices (watches, washing machines, cars, baby monitors, etc) that are able to communicate, share data with one another, and in some cases perform actions in a remotely controlled way (e.g. switching the heating or the lights on and off before arriving home).

If not properly secured, the data shared by IoT devices have the potential to reveal information about their owners to others or be controlled by others without their owner's knowledge or consent. For example, a 'smart thermostat' could reveal whether someone is at home or not; or an IoT connected child's toy or baby monitor could provide information about the children in the home.

To establish future consumer trust about the use of IoT services and the security of their personal information, they will need to be made sufficiently secure from malicious third party attack. These security issues are not new and already exist in many other sectors. In this instance it is the ICO that is primarily responsible for upholding the data privacy of individuals. However, it will be important for the IoT industry to develop appropriate solutions to these issues. Ofcom will continue to help support and promote industry led initiatives aimed at improving the security of IoT services, devices and networks.

Ofcom also intends to continue to work closely with the ICO to help ensure that consumers can easily understand the types of data that will and will not be shared by IoT devices and services they use.

November 2016

Parent Zone – written evidence (CHI0011)

1) Introduction

Parent Zone specialises in providing support to parents grappling with the challenges of parenting in a digital age**.**

Our mission is to make the internet work for families. We represent parents on the executive board of the UK Council for Child Internet Safety and reach over 2million parents a year through initiatives like www.parentinfo.org (our free newsfeed service for schools delivered in partnership with CEOP), *Digital Parenting* magazine (in partnership with Vodafone), and *Parenting in The Digital Age*, the first parenting programme designed to help parents take their offline parenting skills online.

Through our research, parent services and work with schools, we have an in depth understanding of the difficulties parents face as they try to support and guide their children through and in online spaces.

Our response reflects the concerns parents have raised with us as well as covering the areas in which we hold specific expertise.

2) Risks: A legal abyss

The internet throws up new social problems and amplifies old ones. It has changed family life profoundly, with parents facing a multitude of challenges, many of which they feel ill equipped to respond to. These challenges are exacerbated by the fact that the internet treats children as adults from the age of 13.

For parents, this means they are routinely excluded from the interactions their children have with online services and are powerless to intervene should problems arise. Parental consent is not sought unless a platform is specifically designed for children under the age of 13 and therefore, the responsibility for children using services falls into an abyss.

Services have no special duty of care towards children, and parents have no legal status online in relation to their children's accounts. It follows that parental responsibility for children's online behaviour is at best unclear.

3) Risks: Parental authority under challenge

In our report *The Digital Family*,[299] 54.9% of parents told us that the internet made it harder to set boundaries for their children. Add that to the legal responsibility vacuum and you create a toxic mix that is leaving children at risk.

---

299 *The Digital Family: Three stories about where we are in 2015*, Geraldine Bedell, October 2015: https://parentzone.org.uk/system/files/attachments/DF%20Report_FINAL2016_0.pdf

Managing those risks falls to parents, schools and young people themselves. In our research, 49.8% of parents have had to have conversations with their children that they hadn't expected to have – about pornography, violent extremism, self harm and a raft of other troubling issues.

Parents feel these conversations are being thrust upon them when their children are too young to understand. Nearly two thirds of parents felt their children were exposed to explicit sex too early because of the internet, and 61% felt their children were addicted to their devices.

The picture isn't just one of parents who are trying hard to respond to the new challenges of digital parenting – there are also parents who don't get involved, leaving their children to navigate risk unsupervised, and an unknown number of parents who actually don't know which risks their children are taking.

The only people who actually know which risks children take online are the services themselves, and that information is never made public.

4) Risks: The fear of risk itself

This contributes to one of the most insidious risks for children, that of parental nervousness about allowing them to explore and discover online. Allowing children to take managed risks is an important part of growing up, but parents cannot feel confident letting their children take managed risks online when appropriate standards and legal safeguards are not in place. **Children are at risk of spending their time in walled online gardens missing the opportunities the internet could offer.**

5) Risks: The difference between risk and harm

In talking about risk, we need to be clear that it is different to harm. The potential for unmanaged risks to turn into actual harms appears to be high, although figures are not available. We do not know how many children take risk and therefore we cannot assess how often it turns to harm.

NSPCC research[300] points to a steady increase in harm to children that includes an online element. It seems likely that allowing children to navigate high-risk environments without proper legal protection or informed parental supervision is contributing to this increase.

6) Risks: The ones that worry parents

It is worth touching on the less dramatic risks of children using services that are fundamentally not designed for them, because it is these risks that worry parents. The commercialisation of childhood, the wholesale capturing of children's data and excessive screen time – these are the daily worries of a

---

300 *How Safe Are Our Children?* NSPCC, 2016: https://www.nspcc.org.uk/services-and-resources/research-and-resources/2016/how-safe-are-our-children-2016/

modern parent. One of the many queries to our digital parenting help service offers a snapshot of the type of concerns we hear.

> 'The internet exposes my 10-year-old to things I don't think she should be watching, like tutorials on make-up. It's all too easy to find, too much in your face, not what you should be doing at 10.'
>
> *Christina, mother of daughters aged 5, 10 and 15*

7) Risks: The danger of focusing too much on risk and harm

Focusing exclusively on risk and harm is also a mistake. Parents are embracing technology for their children because they recognise the importance of digital skills and believe technology is a significant benefit to their children and their family. This belief is well founded. Our research with the Oxford Internet Institute[301] showed that only two factors were positively correlated to building online resilience – one was 'good enough parenting' and the second was a child's own level of digital skills and confidence.

If the fundamental role of a parent is, as Diana Baumrind suggests,[302] to raise a child 'that is socialised to the society they are growing up in', then parents are right to recognise the need to raise children who can flourish in a digital world.

The jobs market children are being prepared to enter is likely to look very different to the one we experience today. A 2013 study by the Oxford Martin School[303] suggested that 47% of all jobs in the US are susceptible to automation.

Our own research with young people found that 71%[304] were either very or quite interested in a career in IT, with only 4% anticipating a career that involved physical activity. Getting the balance right between protecting children from online risk whilst preparing them for a digital future is a critical.

At present, there appears to be a significant disconnect between these two priorities.

8) Which platforms are children using?

Children have redefined the term 'early adopters'. Their desire to find new and emerging services, to create their own online ecosystems and to stay ahead of the digital trend curve means that any attempt to identify the platforms children use risks missing the point.

---

301 *A shared responsibility, building children's online resilience*, Dr Andrew Przybylski, 2014: http://parentzone.org.uk/article/building-childrens-online-resilience

302 New directions in socialization research, Baumrind, Diana, 1980

303 *The future of employment: how susceptible are jobs to computerisation?* Carl Benedikt Frey and Michael A. Osborne, 17 September 2013: http://www.oxfordmartin.ox.ac.uk/downloads/academic/The_Future_of_Employment.pdf

304 Girls in ICT, April 2016: http://parentzone.org.uk/article/girls-reluctant-follow-careers-it-%E2%80%93-and-it-gets-worse-older-they-get

The fact is that children are using a multitude of platforms. With well over 1 million apps available and an estimated 100 billion worldwide downloads of apps,[305] the environment children inhabit online is too complex to reduce to a list.

What we can say is that children use all of the internet. Whether they access it via apps or websites, via 3 or 4G, public or private WiFi, they explore it all.

This includes familiar names like Facebook, Snapchat and Instagram, but it also includes places that fewer adults understand, including services like Putlocker, a site that facilitates free streaming of movies and TV programmes, and VPNs (Virtual Private Networks) that facilitate anonymous surfing and, more crucially for young people, the ability to bypass filters.

One of the most famous VPNs – Hide My Ass – was created by a 16-year-old to enable him and his classmates to get around his school filters. The company was purchased by AVG Technology in 2015 for £40million. AVG acquired a user base of 2 million for its investment. Ironically, AVG is a company that sells filtering products to parents and schools.

9) The darker side of the net

Young people are also visiting places many adults – including parents and teachers – don't know exist.

Anonymous flirting sites like Omegle – a service with the tagline 'Talk to Strangers' – present specific and very obvious risks to children. The darker, less ethical parts of the internet, expose children to increased risk of cyber crime, inappropriate advertising, popups and contact from people who do not have their best interests at heart.

The online gaming platform Steam has an age rating of 13. It allows players to enjoy an enormous range of online games and buy virtual assets including 'skins' for their virtual weapons. Steam links to 'Skin Gambling' sites like CSGOLotto which allow young people to gamble with these virtual assets. The gaming platform that facilitates this activity requires users to confirm they are 13 or older. It is clearly and unequivocally facilitating underage gambling with virtual assets that can cost up to thousands of pounds.

These services appear to be operating with impunity – or certainly without the scrutiny they deserve.

We need to take care that our increasing efforts to filter the internet for children do not result in children moving to encrypted services and less savoury parts of the web in attempts to bypass adult restrictions. We also need to ensure that in tackling the familiar risks and services, we are not ignoring new and emerging ones.

---

305 *Internet Society Global Internet Report 2015 - mobile evolution and development of the internet*: http://www.internetsociety.org/globalinternetreport/assets/download/IS_web.pdf

10) Which platforms are children using? Sometimes dangers lurk in plain sight

However, it is not simply the less scrupulous parts of the internet that are putting children at risk. Sometimes it is the familiar services that lull parents into a sense of absolute security. The risks of using social media, gaming platforms and live video chat services like Skype and Facetime are often forgotten by parents. Their familiarity and seeming ubiquity make them appear almost child friendly. Parents confidently teach their youngest children how to use Skype to chat to Grandma or stay in touch with a parent working away from home. But any service that allows children to interact with people online in real time carries some risk.

Person to person, live, unmoderated video chat can be high risk, and when parents teach their children how to use these services they should also be teaching them safety information with as much care as they teach road safety.

Parents need to understand that children can be persuaded to share sexually explicit images and personal information that can be used to bully or harass them on these services.

One of the barriers to parents having the right conversations is the industry's unwillingness to provide transparent data on the harms children experience on different services.

Parents have no way of knowing which sites or services they need to be aware of. It is rather like some playgrounds having play equipment that children routinely fall off. It is unfeasible in the offline world that such a playground would be allowed to continue without some warning information for parents.

In the digital world, services have no requirement to offer transparency about risk or more usefully, harm. In 2015, the IWF conducted research looking at youth produced sexual content online.[306] In doing so they were able to identify the services that were being used to create and share these images. **The fact that they chose not to share this crucial information outside of their members was a missed opportunity.**

11) Future harms

If the business model of the internet is advertising, it has been said, the business model of the internet of things will be insurance. As our bodily interactions with the world are monitored and our moods assessed (in 2014, for example, BA pioneered a 'happiness blanket' which measures passenger contentment through neural monitoring), it is not difficult to imagine the potential consequences for children. Will a child's digital footprint become an even more intrusive record of their life, with the potential to influence not just future university and job prospects but also their future life insurance and credit rating? If so, steps should be taken now to ensure that their data has special protection.

---

306 *Emerging Patterns and Trends Report: Youth-Produced Sexual Content*, IWF, March 2015

The right to be forgotten and the GDPR are positive steps, but this piecemeal approach to protecting children is not entirely satisfactory. A more comprehensive review that includes updating the Data Protection Act is worth exploring.

Developments in age verification, monitoring software and facial recognition make this challenge both pressing and complex. **We need a child-focused data protection review for the digital age.**

12) Supporting parents. The role of industry, schools and the urgent need to do more

If raising a child takes a village, then raising a child in a digital world requires a global effort.

Parents have for some time been the focus of attention and as a result they are being overwhelmed with information about specific risks – often through the lens of the tabloid press – with very limited access to parenting support.

Helping parents to develop parenting skills that are adequate to the task of raising digital citizens is vital. We have a crisis that should be dealt with as a public health issue and the response should involve multiple stakeholders.

Government has a role, schools have a role, industry has a role and specialist parenting support organisations have a role. Success will only be achieved if the correct role is played by each sector. Industry can and does play a vital part by improving the information they have available on their own services for parents and providing parents with tools to ensure that they can choose family-friendly settings for their technology.

Industry is often uniquely placed to partner with organisations to bring together parenting expertise with the insight and technical understanding tech companies have. *Digital Parenting,* a free magazine for schools produced by Parent Zone and Vodafone, is one example of a meaningful partnership that has reached over 4million parents since its launch in 2010.

By contrast, initiatives which allow the industry to control the message and select the information parents receive is akin to allowing the fizzy drinks industry to run the national obesity campaign or the powdered baby milk industry to run the breastfeeding campaign.

Equally, government cannot dodge responsibility. Significant progress was made to ensure parents received the support they needed under the previous Labour government. Every local authority was required to have a parenting strategy.

A government department led on parenting work and significant investment was made in the creation of the National Family and Parenting Institute. That infrastructure has now gone.

Parenting has lost its voice in government at a time when it needs it most.

Perhaps it is because of this vacuum that 70% of parents say they turn to their child's school for support and information. The burden this places on schools, already struggling to deal with the impact of technology on the children in their care, is unacceptable given the lack of funding for parent support in schools.

13) Regulation

An ever changing digital world is not easy to regulate. That should not mean that the regulations that protect children should be left in a pre-digital state. The GDPR has led to an important conversation about the age at which children should be allowed to use services without parental consent. This is a debate that should be explored in full with due regard for the legal capacity of a child to agree to terms and conditions on a site and the consequences of parents not being required to give parental consent.

It is time for the *Children's Act* and *Working Together to Safeguard Children* guidance to be reviewed to consider whether a legal duty of care could be included to ensure that services that identify a child experiencing harm are required to report that child to the appropriate authority. **Online services have a unique window into children's lives. It cannot be right that they are allowed to look through that window, observe a child experiencing harm and have no legal duty to do anything with that information.**

14) Children's wellbeing

In March 2016 we published a report titled *The Perfect Generation*.[307] The report asked young people about their experiences of the internet and its impact on their mental health. Young people shared nuanced and thoughtful views about the internet and its impact on their wellbeing. They did not regard it as 'separate' or even 'a thing'. Rather it was woven through their lives as a utility and its impact linked to mood, resilience and maturity.

There were very stark discrepancies between what professionals thought about the internet and what young people told us. 44% of professionals thought that the internet was bad for young people's mental health, compared to 28% of young people. Worryingly, 84% of teachers told us they lacked the resources they needed to deal with issues effectively. It was also clear that young people are rejecting traditional sources of help, including those offered by online children's services and children's charities. This generation of digital natives prefer to access support from their friends and from anonymous online communities. They want support where they are – in forums, on games and in social networks - not from structures that were designed in a pre-digital age. **There could be an important role for industry in responding to these new support needs.**

---

307 '*The Perfect Generation': Is the internet undermining young people's mental health?* Rachel Rosen , 17 March 2016

15) Conclusion

The UK has led the world in online safety. UKCCIS provides a model for collaborative working that should be celebrated. The first phase of internet safety has passed. It is now time for the next phase. We need to bring our legislation into the digital age, develop proper digital parenting support and address the fact that children require the same special protections online as they rightly enjoy off. We need to achieve these things whilst protecting children's digital right to roam.

Driving parental fear is not the answer. Nor is seeking a technical silver bullet. We need fundamental protections so that parents can allow their children to enjoy the internet and children can continue to benefit from the extraordinary opportunities it provides.

15 August 2016

Parent Zone and NSPCC – oral evidence (QQ 18-27)

Transcript to be found under NSPCC

Professor Andy Phippen, Plymouth University – written evidence (CHI0045)

About me

1. I am a Professor of Children and Technology at Plymouth University, a research partner with the UK Safer Internet Centre, a member of the South West Grid for Learning's online safety group and the advisory council for the Open Rights Group. My work is almost entirely quantitative in nature and I have spent the last 10 years talking with children and young people of all ages about how digital technology impacts upon their lives, with a specific interest in changing norms and legitimisation as a result of online interaction. Specific areas of focus in this time have been around sexting, pornography, gaming, social media, privacy and data protection.

Response to the Inquiry Questions

2. I very much welcome this inquiry and the committee's interest in the area of children and the Internet. However, I can't help feel that this submission is similar to others I have submitted to other Parliamentary inquiries in recent times yet from a policy perspective I see little change – the focus is still on service providers to "do more" while the harder issues that might have a significant and profound impact upon the lives of children, for example, an up to date and compulsory relationship and sex education curriculum that acknowledges the role digital communications play, are largely ignored (or rejected).

3. Clearly digital technologies have had a profound impact upon this generation of children and young people – the majority of my conversations with young people are positive with them viewing Internet technologies as having a constructive impact upon their lives. However, there are also clearly risks and I have spoken to many children who are the victims of what we might refer to as "cyberbullying" and also other negative influences – such as early sexualisation, unrealistic expectations of sexual performance and body image, performance anxieties, legitimised aggressive and homophobic language and exposure to risk of grooming.

4. Most concerning for someone who works a great deal with children and young people is that with all of these potential risks, I hear that they have few opportunities to discuss these issues in a school setting. As a result end up developing their own strategies for what is acceptable and unacceptable and coping strategies – a reflection of modern society is certainly the view by many young males that the way to express interest in a potential partner is to send them an image of their genitals.

5. Yet we risk playing "chase the technology" if we continue to focus upon platforms and not behaviours. While it is clear that presently the main platforms of choice for young people are things like Snapchat, Instagram and YouTube, as well as various gaming platforms, this will change over time –

children and young people are often early adopters to new platforms and services and will use them in unpredictable and disruptive ways. However, the potential risks associated – for example harm from abuse, grooming, data and personal privacy, exploitation and coercion – remain similar to what we were looking at 10 years ago.

6. A focus upon service provision and technology does not get to the root cause of risky behaviour – for example, sexting manifests as a result of cultural norms, technological facilitation and the social currency of popularity. The harm that can result from sexting (such as the redistribution of images and resultant abuses, breakdown of trust and infringement of privacy) results from a lack of respect of boundaries, failure to understand consent, and a lack of empathy between abuser and victim. There is nothing platform specific about this, it is about behaviours. Prior to digital technology we had Polaroid cameras used for similar reasons – all the digital technology does is make it easier to self-generate and distribute. However, the indecent "selfie" is not a creation of the Internet.

7. I am in no doubt that we are, at present, failing children as far as education provision around the Internet and its 'safe' use. In my experience of exploring online safety curricula in schools it is clear that the lack of guidance while at the same time placing greater expectation, from safeguarding policy and inspection framework, to "do something" around online safety results in schools implementing ad hoc curricula from a weak knowledge base. That is not to say all schools fail – I have seen some excellent curricula that encompass online safety and risk issues across the curriculum, but equally I have seen many where teachers are trying their best without any support or guidance. A lot of the time with pressure as a result of reactionary demands from senior management who need to something/anything in place due to impending inspection). I have, on more than one occasion, been invited into a school to talk to the children there "because we've got an inspection soon as we need to say we've done something".

8. Parental education is more of a challenge and while I have seen a great deal more effort by service providers in recent times to provide a lot of information about their services, issues around safety, clear and effective reporting routes, and effective take down policies, there is a very important public education issue around making parents realise that this is something they need to know about. When working with charities who deliver parental information sessions around online safety, I have seen poorly attended (in some cases non-attended) sessions – it seems that for many parents their view is that schools should be attending to child development in this area. Compounded with this issue is the belief by that children should be monitored in the home, have their conversations intercepted by "safeguarding" software, have their movements tracked in order to be reassured about their whereabouts, and be subjected to mobile phone "spot checks" to make sure they're "safe" – all of these things have been described to me by children I have spoken with. The reliance upon technology to do a parenting role is concerning and can be detrimental to the rights of the child.

9. Returning to the role of the service providers and media companies, as I have already mentioned, I have seen a great deal of improvement in what is provided by these companies, and they are far more responsive to the needs to protect children who use their services. However, the focus on these companies as the sole stakeholder responsible for child safety seems somewhat concerning. By placing the focus (and finger of blame) on the service providers, others who might do more (for example, those defining education policy and educators themselves) are being absolved of responsibility. I have lost count of the number of times I have been told in a primary school that because children in their care shouldn't be on social media due to the 13 years old age restriction, they don't need to educate them on such. Yet the fundamental issues around risk and harm from social media (arising from thing like peer abuse, cyberbullying, grooming and privacy issues) are certainly things that can be addressed in a primary curriculum without any need for technology specifics.

10. If we are to consider the position of legislation and regulation in this area, it is a patchwork at best, with, again, an overreliance upon technology to solve what are, essentially, social problems. We have seen in recent years an expectation (backed up with a threat of regulation) on service providers to provide the filtering of content on internet connections in the home. More recently, we have seen growing regulation that places an expectation on schools to monitor children's' internet access to ensure they are "safe" and not accessing anything that is potentially "harmful". We have also seen policy to "ensure" age verification on pornography sites. All of which suggests that if we can get the technology "right" we can ensure children are safeguarded from the sorts of threats afforded by high use of Internet technologies.

11. However, even if these technologies worked perfectly (and the Open Rights Group's Blocked project highlights that almost 20% of the Alexa's 100,000 top Internet sites are blocked by at least one service provider filter in the UK) they will only ever be successful in preventing access to specific forms of content, whereas children and young people constantly highlight that upset, harm, and risk come as more from the behaviour of others than seeing "inappropriate" content. That isn't to say that children should access pornography whenever they wish – clearly there is much evidence to highlight the potential harm this causes. However, to think that filtering the UK's internet will solve this problem is extremely naïve.

12. In our rush to ensure children are "safe" online, we risk a dystopia where young have limited access to relevant and valuable information (for example, sexual health, relationships advice, information about gender and sexuality), increasing erosion of the privacy, and a failure to meet their rights to an education that is fit for purpose and one they are calling for.

13. For example given the growing expectations on schools to monitor children's internet access and use, with little guidance on what to do which incidents are discovered, consider the following scenario – a teenager, with concerns around sexual health, uses a school computer to look us something about a sexually transmitted disease. The school monitoring system, as a result of the keywords used in the search term, will intercept this. As a result, school

monitoring systems will be informed. What happens next is entirely dependent upon the school, there is no guidance in safeguarding regulation for what the incident response should look like. Potentially a school, with fear of a poor inspection as a result of being seen to be weak on monitoring, could see fit to raise this, entirely innocent and potentially helpful and informative, search with senior management who might then decide to call in the child's parents. At what point does this scenario place the best interests of the child at the centre of the response, or have any cognisance of their rights?

14. If we wish to ensure that this, and future, generation of children and young people can use the Internet safely, positively, while reducing the risk of harm or upset (because we are never going to stamp out risk), we need to move away from chasing technology and develop education that goes beyond prohibition, understands that technology merely facilitates behaviour, address root causes of issues. And we need to provide it in such a manner that allows safe and supportive environments for them to ask questions, and get answers, about growing up in our massively connected society.

September 2016

Philip Powell, Emily McDool, Jennifer Roberts, Karl Taylor, Department of Economics, University of Sheffield – written evidence (CHI0008)

THE EFFECT OF SOCIAL MEDIA USE ON CHILDREN'S WELLBEING

1. Summary

1.1. Our evidence is concerned with question (1.i): *What risks and benefits does increased internet usage present to children, with particular regard to social development and wellbeing*? This research was generated as part of an Engineering and Physical Sciences Research Council (EPSRC) funded project on 'digital empathy'.

1.2. We focus on one important aspect of children's internet use, the use of social media or social networking. We estimate the effect of children's online social networking on their subjective wellbeing. We use a large sample of 10-15 year olds from the UK Household Longitudinal Study, and estimate the effect of time spent chatting on social websites on a number of alternative outcomes which reflect how these young people feel about different aspects of their life, specifically: school work, school attended, appearance, family, friends and life as a whole.

1.3. Our results suggest that spending more time on social networks reduces the satisfaction that young people feel with all aspects of their lives, except for their friendships, where the effect is positive. Spending an hour a day chatting on social networks (the average time in our data) reduces the probability of being completely satisfied with *life overall* by approximately 14 percentage points.

1.4. Looking at the different aspects of life, the largest effects are for satisfaction with *family* and *school attended* and the smallest effects are for *appearance* and *school work*.

1.5. We explore three explanations for our results. We find some support for *social comparisons* and *cyberbullying* explanations, but no support for the theory that time on social networks has an adverse effect because it detracts from time spent doing other beneficial activities.

2. Background

2.1. Childhood circumstances and behaviours have been shown to have important persistent effects in later life. One aspect of childhood that has changed dramatically in the past decade is the advent of social media, or online social networking. Young people are heavy adopters of social media; today's teenagers are the first cohort to have grown up with online social networking. An ONS survey in 2015 revealed that, in the UK, 92% of 16 to

24 year olds use online social networks[308]. Along with teenagers, younger children are also increasingly users of social media; while most sites stipulate a minimum user age of 13, few require any validation, and a survey for the children's BBC channel (CBBC) found that more than three quarters of 10 to 12 year olds have social media accounts[309].

2.2. A lot of the existing evidence on the effects of social media use comes from small selective samples from outside of the UK, so it is difficult to generalise this to children in the UK. In contrast our evidence comes from a large representative sample (n = 3971) of children from across the UK.

2.3. Much of the existing evidence establishes an association between social media use and wellbeing but is not able to claim that the relationship is causal. Associations can be misleading as they may be driven by other factors. Our method comes as close as possible to establishing a causal effect.

3. Where our evidence comes from

3.1. We use a large secondary data source, the UK Household Longitudinal Study (UKHLS), often called the *Understanding Society* survey. This is secondary data, meaning that it was not collected specifically for the purposes of studying children and social media use.

3.2. UKHLS is a study of 21st century UK life and how it is changing. It captures a wide range of information about people's social and economic circumstances, attitudes, behaviours and health. It is funded by the Economic and Social Research Council (ESRC) with additional funding from a consortium of government departments.

3.3. UKHLS is a representative sample of over 40,000 households across the UK; the same individuals and households are interviewed in each wave. Five waves of data are available; starting in 2009-2011 (wave 1), which provided data on over 50,000 individuals. In wave 5 (2013-15), over 41,000 individuals were interviewed. All adult members of each household are interviewed along with children in the households aged 10 to 15 years old.

3.4. Our data is from children interviewed in waves 2 to 4; data comes from a face-to-face interview and a self-completion questionnaire. We also make use of information from the adult interviews so that we can include household and family circumstances in our analysis. Our analysis uses a sample of 3,971 children, providing 6,788 observations between waves 2 to 4 of UKHLS.

3.5. The outcomes are measures of *domain satisfaction*; children are asked *how they feel* about different aspects of their life, specifically: *school work*,

---

308 www.ons.gov.uk/ons/guide-method/method-quality/specific/business-and-energy/e-commerce-and-ict-activity/social-networking/index.html

309 www.bbc.co.uk/news/education-35524429

school attended, *appearance*, *family*, *friends* and *life as a whole*. The possible responses are on a 7-point scale ranging from 1 = not happy at all, through to 7 = completely happy. Average satisfaction is highest for *family* (6.35) and lowest for *appearance* (5.18).

3.6. The main explanatory variable is obtained by firstly asking: *Do you belong to a social web-site such as Bebo, Facebook or Myspace*? 77% of respondents answer 'Yes'; they are then asked *How many hours do you spend chatting or interacting with friends through a social web-site like that on a normal school day*? The responses are: 1 = none (13.1%), 2 = less than an hour (43.7%), 3 = 1-3 hours (33.9%), 4 = 4-6 hours (7.0%), and 5 = 7 or more hours (2.3%).

4. Methods

4.1. We use regression analysis to estimate the effect of the time that children spend chatting on social media on their satisfaction with the different domains of their life, controlling for other variables that are also expected to influence this satisfaction.

4.2. The main control variables are: children's characteristics (age, sex, race, number of close friends, hours spent watching television, educational aspirations, and other behaviours, such as truancy and smoking); parent and household characteristics (parental employment and education, single parents, household income, housing tenure, other children in household, propensity to eat evening meal with family); area characteristics (urban area, local unemployment rate).

4.3. Our estimation method is designed to deal with some important methodological issues (see below), so that we get as close as we can to estimating a causal effect of social media use on wellbeing, rather than simply establishing an association.

5. Results

5.1. Our results show that spending more time on social networks reduces the satisfaction that young people feel with five of the six aspects of their lives (school work, school attended, appearance, family and life overall). In contrast it has a positive effect on the satisfaction with their friends.

5.2. The quantitative interpretation of our models is hard to summarise because our main explanatory variable (time spent chatting on social networks) and our outcome variables (how the children feel about different aspects of their lives) are measured on ordinal scales. Here we interpret the effect on the outcomes evaluated at the mean time spent chatting on social networks, which is approximately 1 hour per normal school day.

5.3. Spending an hour a day chatting on social networks reduces the probability of being completely satisfied with life overall by approximately 14 percentage points. This is three times as large as the estimated adverse effect on wellbeing of being in a single parent household (4.6 percentage

points) and is also larger than the effect of playing truant (10.3 percentage points).

5.4. Looking at the different aspects of life, the largest effects are for satisfaction with family and school attended, whilst the smallest effects are for appearance and school work. In contrast an hour spent chatting on social networks increases the probability of being completely satisfied with friends by 9 percentage points.

5.5. Looking at boys and girls separately reveals some differences. For boys there are adverse effects on satisfaction with school work, school attended, appearance and life overall. For girls there are adverse effects on school work, school attended, family and life overall. Surprisingly increased time on social media does not reduce girls' satisfaction with their appearance, but for girls there is a strong positive effect on satisfaction with friends that is not there for boys.

6. Why does social media use affect children's wellbeing?

6.1. We explore three theories that help to explain why social media use may have a negative effect on young people's wellbeing. These theories draw on research from both economics and psychology, and it is likely that they are not mutually exclusive.

6.2. *Social comparisons*: increased social media use is linked to more frequent social comparisons with others; these comparisons are more likely to be negative in direction, given that the material people choose to present online represents selectively idealised versions of their true lives. We explore the effects of time spent on chatting on social media for children with high vs. low self-esteem (using a psychological measure called the Rosenberg self-esteem scale). There are more adverse effects for those with lower self-esteem, which provides some support for the social comparisons theory as those with lower self-esteem are more prone to make negative social comparisons.

6.3. *Finite resources*: extensive time spent on social media encroaches on other activities known to be beneficial for wellbeing, such as face-to-face socialising, sports or exercise. We explore the effects of time spent on chatting on social media for children with high vs. low participation in other activities (such as going to the cinema, watching sport, or 'hanging out' with friends). There are more adverse effects for those with higher involvement in other activities, which is contrary to what this theory suggests.

6.4. *Cyberbullying*: young people who spend more time on social networks have a greater chance of being the victim of cyberbullying. We explore the effects of time spent on chatting on social media for children who report being bullied (this is general experience of being bullied, not cyberbullying per se) vs. those who say they are not bullied. There are more adverse effects for those who report being bullied, which provides some support for the cyberbullying theory. Interestingly, for those who report being bullied,

more social time on social media increases their satisfaction with their friends.

7. Methodological issues – the econometric estimation

7.1. An important methodological issue relates to the direction of causality of the relationship between wellbeing and social media use. We have stated here that social media use is an input and wellbeing is an output, but it can also be argued that causality may go in the opposite direction because children with lower levels of psychological wellbeing may choose to spend more time on social media. It is also possible that there is a 'third variable problem'; meaning that there are factors not included in our analysis (for example loneliness or introversion) that drive both social media use and wellbeing. Failing to account for these factors may result in misleading estimates of the effect of social media use on wellbeing.

7.2. We attempt to deal with the 'third variable problem' in two ways. Firstly, we have a very rich set of control variables which account for children's characteristics (such as age, sex, siblings, number of close friends, other activities), family and household circumstances (such as income, parental employment and education, single parents, housing tenure and propensity to eat evening meals together) and characteristics of the local area (such as whether it is rural or urban and the local unemployment rate). Secondly, we use an estimation technique that controls for time invariant individual characteristics that we cannot observe (like personality traits).

7.3. To deal with the problem of direction of causality, we use an instrumental variables (IV) approach. An instrument is a variable that only affects the outcome measure (wellbeing) via its influence on the main input (social media use). We use information on local area broadband speeds and mobile phone signal strength published by Ofcom. The basic premise here is that the quality of internet connection should have no direct effect on how young people feel about these specific aspects of their lives (once we control for other key influences such as household income and the local economy) but will only affect them via its influence on time spent online; empirical tests support the validity of this IV strategy.

7.4. Our estimation method is also designed to deal with two important features of the data; firstly, the outcome measures (how young people feel about various aspects of their life) are not continuous; they are measured on a 7-point ordinal scale. Secondly, we have repeated measures from some children who appear in more than one wave of the data.

Funding Acknowledgement: This research is part of a project funded by the UK EPSRC research grant EP/L003635/1 Creating and Exploring Digital Empathy (CEDE).

18 August 2016

PSHE Association - written evidence (CHI0005)

Introduction

1. PSHE education is a non-statutory curriculum subject that teaches pupils in English schools the knowledge, skills and attributes they need to keep themselves safe, to stay physically and emotionally healthy and to prepare for future life and work. The PSHE Association is the leading national body for the subject, a charity which supports teachers with guidance, resources and training on PSHE education. We also lead the campaign for high-quality PSHE education in all schools in England.

2. PSHE education lessons cover safe internet use, as well as addressing the impact that the internet has on sex and relationships, mental wellbeing and other issues. Lessons tackle issues ranging from the risks of sharing sexual images, to the impact of cyberbullying, to the critical consumption of media, helping young people to develop the skills to make safe choices. These lessons compliment the school computing curriculum, which focuses predominantly on the technical elements of use of technology, such as coding.

3. We welcome this inquiry. Children and young people are growing up in a time of rapid technological and social change, which brings tremendous opportunities as well as substantial risks. It is important that education ensures pupils are able to negotiate new, emerging and hitherto unanticipated dangers and opportunities. While our submission focuses largely on the risks rather than the benefits of the internet, we believe that education ultimately plays a positive, facilitating role in ensuring that children and young people gain the most out of the internet by learning how to use it safely.

Summary

4. There is a strong consensus that schools have an important role in educating children and young people to keep themselves safe from online and offline risks through. While both parents and teachers alike may feel daunted by the 'latest trends' and rapid technological change, it is important not to overstate the novelty of the challenges the internet presents. Lessons can address issues related to online safety, from online pornography and the sharing of sexual images, to accessing extremist content by building skills to help pupils manage risks, think critically, resist peer pressure and foster healthy relationships – all of which are just as applicable to offline contexts.

5. Yet, worryingly, PSHE education lessons, through which these issues are taught, is increasingly being squeezed off school timetables. This means that many pupils miss out on education which could help to keep them safe online. The most recent Ofsted review of the subject has stated it is 'not good enough', pointing to the serious safeguarding implications of

failure to teach many of these issues, while the Commons Education Committee says the situation is "deteriorating".

6. While more guidance for schools would be welcome, this will not address these gaps in provision. The low priority given to PSHE education directly stems from its non-statutory status. We therefore recommend that Government make PSHE education compulsory in all schools to ensure that all children and young people leave school with the ability to make the most of the opportunities that the internet offers, safely.

What risks and benefits does increased internet usage present to children? (with particular regard to i) social development and wellbeing; ii) neurological, cognitive and emotional development iii) data security

7. The benefits of increased interest usage come with a range of attendant risks including access to sexually explicit, or otherwise harmful or distressing content, as well as extremist content. There are also risks associated with children and young people's interaction with others online, ranging from the potential of online grooming for abuse and exploitation, to the dangers of sharing sexually explicit images. There are concerns that these materials could affect both the emotional wellbeing and social development of children and young people.

8. Concerns have been raised about the effect that increased access to online pornography may have on young people's perceptions of 'normal' sexual behaviour. A joint survey undertaken by The Children's Commissioner for England and the NSPCC found that 94% of children aged 11-16 had seen pornography by the age of 14, many by accident. 39% of 13-14 year olds and 21% of 11-12 year olds said that they would like to copy some of the behaviour they had seen. Female respondents, in particular, worried that they would come under pressure to behave more sexually from partners who had viewed pornography; and worried that pornography was degrading or humiliating.

9. Additionally, depictions of the human body in pornography may distort young people's perceptions of their own and other's bodies. In light of this, it is in our view essential that pupils are taught about healthy relationships and consent, to teach them to think critically about pornography and be able to develop respectful relationships.

10. Children and young people are also vulnerable to accessing other harmful material online, including sites which promote eating disorders or self-harm; or which promote extremist views. It is important that children are taught skills to think critically about the information that they encounter online. It is also important to provide protective learning in relation to these issues to ensure that they know how to access sources of support, and are able to support their peers if they suspect someone is at risk.

11. Social media can have a significant impact on children and young people's emotional wellbeing and on their relationships with others, creating pressures to portray an 'ideal life' and allowing bullying which previously

would have ended at the school gates to continue offline. Research suggests that one in three children have been a victim of cyberbullying and one in four have experienced something upsetting on a social media site. It is essential that teaching helps pupils to build resilience to the potentially negative effects of social media, and construct strategies to manage their social media use and to critically evaluate what their peers post online.

12. Earlier this year, a Times investigation estimated that around 44,000 secondary school pupils have been caught sharing sexual images in the past three years and that over a third of cases involve children aged 12 or 13. There is a particular danger that images shared with a peer might then be shared on with a larger group of people, causing considerable distress to the victim. Additionally, children may not realise that they are committing a criminal offence when sharing these images: the law states that the sharing of sexual images of under-18s is a criminal offence, and in addition, some cases may fall under the scope of laws to tackle revenge pornography. Experts on child protection have also raised concerns about the opportunities the internet presents to perpetrators to groom children online, and in some cases to arrange to meet offline. Figures from the Child Exploitation and Online Protection Agency suggest that around a quarter of reports relate to online grooming. It is vital that all young people receive guidance on this issue, to help them understand the law, to keep themselves safe, and to challenge abusive behaviours within their own relationships.

13. Most of these risks cannot be entirely addressed through web filters. Young people have numerous options for accessing unrestricted content and many dangers relate not to specific technologies, but to how these technologies are used. For example, the use of image sharing apps can be benign or risky depending on the nature of the images shared. Given the profound benefits of internet access, a measured response is crucial. New Government safeguarding guidance on 'Keeping Children Safe in Education' aims to strike this balance, noting the importance of ensuring that "over blocking" does not lead to unreasonable restrictions as to what children can be taught. Instead, we believe that methods such as filters should be combined with education which builds children and young people's capacity to use the internet safely.

What roles can schools play in educating and supporting children in relation to the internet?

14. We believe that there is an overwhelming consensus across society that PSHE education in schools can play an important role in teaching children how to keep themselves and others safe, including from online risks. However, as we set out below, we believe that the Government must take action to make PSHE lessons compulsory in all schools to ensure that all pupils receive regular, high-quality lessons that help to keep them safe.

15. Schools have a duty to keep pupils safe under section 175 of the Education Act 2002 and schools' safeguarding duties on schools, as

outlined in statutory guidance *Keeping Children Safe in Education,* set out the expectation that schools keep pupils safe in school, as well as outlining ways in which schools can help pupils to stay safe outside the school gates. This guidance was recently updated to include more emphasis on school's role in providing preventative education.

16. There is widespread support for schools to play this safeguarding role. Statutory PSHE education is supported by 92% of parents, 92% of young people and 88% of teachers. A PSHE Association-YouGov poll of over 1,000 parents found that 87% believed schools should do more in relation to teaching children about the impact of sexting, with the vast majority favouring preventative education over punitive approaches such as calling the police or social services. Leading charities with significant expertise in this area, from the NSPCC and Barnardo's to Childnet have all argued for statutory PSHE education, to keep children safe from both online and offline risks.

17. There is also cross-party recognition of the importance of PSHE education in this area. The Commons Education Committee, in its 2014-15 inquiry into the subject, called for the Department for Education to make the subject statutory in order to keep children safe. More recently, the Chairs of the Education, Health, Home Affairs, and Business, Innovation and Skills Committees wrote a joint letter to the Education Secretary calling on her to make PSHE education statutory, noting that it could keep 'young people safe from abuse in many forms'. The Children's Commissioner, Chief Medical Officer and Public Health England and the national police lead for child sexual exploitation, Chief Constable Simon Bailey, have all given their support for statutory status.

18. Experts agree that effective online safety education cannot simply focus on technical issues such as firewalls and privacy settings, but must instead focus on issues which apply equally to offline spaces, focussing on pupils' relationships with others, their ability to recognise unhealthy or exploitative relationships; to respect others and develop positive relationships; as well as to appraise risks, resist peer pressure and make informed decisions. An expert panel report for the Department of Culture, Media and Sport, stated that education on pornography should have 'a core focus' on relationships, sexual and gender identities and consent; and the Child Exploitation and Online Protection Centre notes that "online safety is not primarily a technology issue but about behaviour, communication and relationships between people". The Committee has already heard similar oral evidence from the Childnet Chief Executive Will Gardner, that we must avoid focusing overly on the 'technical' aspects of cyberbullying, instead recognising that it is about relationships between individuals.

19. Given the importance of seeing online safety within this broader context, it is essential that lessons on online safety are integrated into a broader PSHE curriculum, that the novelty of challenges associated with internet use is not overstated, and that arbitrary lines are not drawn between the online and the 'real' world. The guidance we produce for schools, for

examples on teaching about consent, recognise both the online and offline dimensions of these issues, including specific lessons on issues like pornography and the sharing of sexual images, integrating these into broader teaching on consent, self-esteem, peer-pressure and gender and sexual equality. PSHE education lessons provide the ideal context in which to teach about these inter-related issues.

20. We have also published a review of effective prevention education with the Child Exploitation and Online Protection Centre, identifying principles of best practice for online safety education. Yet, while a body of evidence exists, there is a lack of awareness of best practice principles and a lack of resources or time to put them into practice in schools.

What guidance is provided about the internet to schools and teachers? Is guidance consistently adopted and are there any gaps?

21. We believe the challenge for schools is not principally due to a lack of guidance, but rather due to a lack of provision of lessons making use of the guidance which already exists. There are a range of sources from which schools can access information on teaching pupils how to stay safe, including online. These range from our own guidance documents, many of which are Government-funded and freely available; to respected organisations such as CEOP, Childnet and the NSPCC; to Government resources such as the Home Office's *Disrespect NoBody* campaign.

22. Significantly, statutory guidance for schools has fallen short of requiring schools to teach PSHE lessons. The 2015 Ofsted framework places greater emphasis on safeguarding but no requirement to provide teaching, and the Government guidance 'Keeping children safe in education' includes a reference to – but no requirement to provide - teaching and learning opportunities related to safeguarding children online and offline. Indeed, the trend in schools is to provide less time on the curriculum for teaching on issues like online safety, and for fewer teachers to gain training on delivering high-quality lessons. In the face of competing pressures, and the non-statutory status of the subject, PSHE education is systematically deprioritised.

23. Some have pointed to the inclusion of online safety within the computing curriculum as a step forward but we do not believe that the computing curriculum can reasonably be expected to accommodate a developmental curriculum which includes the learning we have described - including on issues such as healthy relationships, consent, self-esteem and mental and emotional wellbeing - that underpins effective online safety education.

24. Ofsted's most recent review of the subject found that provision was "not yet good enough" in 40% of schools, with particular weaknesses in safeguarding areas including domestic abuse, attributing this to insufficient training for teachers. Department for Education data suggests the proportion of school hours allocated to PSHE has declined by over 30% between 2011 and 2015. The decline in timetabled provision is compounded by this lack of teacher training, meaning that the quality of

lessons that are delivered can be variable. While there is good evidence-based pedagogy in this area, these principles are often simply not being put into practice.

25. Therefore, while further guidance would be welcome, we do not believe it is the central issue. Unless PSHE education is seen as a priority for schools, they are less likely to make use of the resources and training available to them. Prevention education can only be effective when the quality of provision is good enough to ensure that complex issues are effectively addressed. The patchy quality of teaching means that the time that is currently devoted to PSHE education is not being used effectively.

Conclusions and recommendations

26. We believe that the internet provides a host of opportunities and advantages to children and young people. In modern Britain, having the skills to use the internet effectively and safely is essential to thriving in work and life. However, there are a range of risks associated with children's internet use which go far beyond the 'technical' aspects of online safety. We believe that these are best taught through PSHE education. Yet, at present the subject is falling off the timetable in schools. While more guidance for schools is welcome, it is the low priority given to the teaching of issues related to children's ability to keen themselves safe online and offline that is the principal challenge.

27. The single most effective way to ensure that all pupils are taught PSHE education would be for Government to ensure that the subject is taught in all schools, including academies. This is the view taken by the Commons Education Committee, which notes that other measures are likely to be insufficient to address the deteriorating provision of PSHE education in schools. Making PSHE education a statutory subject would ensure that all teachers are properly trained in order to ensure lessons are taught effectively.

28. It is clear that pupils, teachers and parents support statutory PSHE education. Yet patchy provision continues despite the widespread support and importance of the subject in fulfilling schools' safeguarding duties. There is a clear case for the government to show leadership and take national action to reverse decline, and to publicly support schools to invest in curriculum time and teacher training. Making the subject statutory would have important knock on effects, beyond raising awareness of the importance of the subject among teachers and school leaders, including increasing investment in high-quality resources and training; and encouraging teacher training providers to devote more time to teaching the subject.

18 August 2016

Jennifer Roberts, Emily McDool, Philip Powell, Karl Taylor, Department of Economics, University of Sheffield – written evidence (CHI0008)

Written evidence to be found under Philip Powell

Dr Angharad Rudkin, Dr Dickon Bevington and Dr Henrietta Bowden-Jones – oral evidence (QQ 11-17)

Transcript to be found under Dr Dickon Bevington

Samsung Electronics – written evidence (CHI0029)

INTRODUCTION

1. About Samsung UK and Ireland

1.1. Samsung Electronics is a global leader in technology, employing 270,000 people across 79 countries.

1.2. Through relentless innovation and discovery, we are transforming the worlds of televisions, smartphones, personal computers, printers, cameras, home appliances, LTE systems, medical devices, semiconductors and LED solutions. We have the highest research and development spend of any technology company and have the second highest research and development spend across any industry worldwide.

1.3. Samsung has based operations in the UK for over thirty years and we regard the UK as one of the most important tech markets in the world. Over the years our presence and activity here has grown as we utilise the significant growth and investment opportunities.

1.4. The UK is also an important European hub for Samsung. Our European Headquarters, design and innovation centre and European R&D centre are based here.

2. Executive Summary

2.1. We welcome the opportunity to respond to this important consultation. At Samsung, we build devices which our customers, including children, use to access the internet. We have a limited ability to control how our customers use our devices, and what websites they choose to visit or what content they choose to upload or access, however, we do provide tools on our devices which allow parents to limit their children's exposure to the internet (highlighted in our response to Q3). Our viewpoint on this issue is therefore distinct from, for example, online platforms or social media sites which host online content, but we hope that the Committee will welcome our perspective.

2.2. At Samsung, we believe in the power of technology to educate and inspire and as our world becomes smarter and more connected, we want everyone, and particularly young people, to be able to take advantage of the opportunities that technology presents.

2.3. The internet offers children today an unprecedented variety of resources to explore, learn, and play. We believe that this represents a major boost to child development – technology use builds problem-solving skills and logical thinking; encourages creativity; and teaches teamwork and collaboration.

2.4. We recognise that there risks for children online, but we believe they can be most effectively addressed through education which builds a positive relationship with the internet. Samsung has established a series of digital education programmes in the UK which aim to teach children to use technology responsibly and equip them with the essential skills they need to thrive in an increasingly digital world.

2.5. Alongside these programmes, we are undertaking research to better understand the challenges and opportunities of using technology in the classroom and, more broadly, children's experience of the internet. Our interim findings are set out in this paper, but the key issues for Samsung are:

- Positive role for technology: Internet-enabled technologies in the classroom provide opportunities to strengthen problem solving skills and logical thinking; encourage creativity; and teach teamwork and collaboration. We therefore see major educational and developmental benefits to increased internet usage among children, provided this is accompanied by classroom-based education to teach responsible internet use.
- Teaching responsibility: Teachers felt that one of the greatest effects of the Samsung Digital Classroom programme had been on pupils' personal growth and maturity, both in the classroom and outside. We believe that this helps to tackle inappropriate internet use, such as online bullying and trolling.
- Supporting teachers: Many teachers are enthusiastic about using technology in the classroom, but they are held back by a lack of confidence using technology and they would like more training and clearer guidance. The Government should provide resources to address these barriers.
- Supporting parents: Many parents also lack confidence using online technology and do not have the knowledge to talk to their children about online safety. Samsung's Digital Families events demonstrate that engaging parents in their children's learning and internet use breaks down these barriers. We believe the Government should roll-out similar initiatives.

CONSULTATION RESPONSE

Risks and benefits

1. What risks and benefits does increased internet usage present to children, with particular regard to:
   i. Social development and wellbeing
   ii. Neurological, cognitive and emotional development,
   iii. Data security.

1.1. While we recognise that there are challenges related to management of children's internet use, at Samsung we believe that a positive relationship with the internet can be achieved through education. We have found, through our *Samsung Digital Classroom* programme as well as our other digital skills initiatives for pre-16s, that bringing technology into the classroom encourages the positive and productive use of technology, equips young people with essential digital skills, and helps to tackle problems such as online bullying and trolling.

1.2. Samsung welcomed the previous Government's commitment to improving digital literacy through the Computing Curriculum, which introduced mandatory computing lessons for 5–16 year olds. A major component of the course involves learning how to code, which of course we expect to have major benefits for companies like Samsung by inspiring many young people to follow a career in tech.

1.3. But the impact of technology use in the classroom is not limited to coding. It improves learning across the whole curriculum and the benefits will be felt across the whole of society. Technology strengthens problem solving skills and logical thinking; it encourages creativity; and it teaches teamwork and collaboration. Taken together, this represents a major boost to child development.

1.4. To better understand the impact of technology in the classroom, Samsung has been running a Digital Classroom pilot programme across the UK since 2013. There are now fifteen within primary schools located in the most underprivileged areas in every UK region; one at the British Museum; one at the Victoria and Albert Museum; and three with our charity partner, The Prince's Trust. In addition to providing a suite of devices and the training necessary to use them in the classroom, we are working closely with schools to assess the impact on teaching practice, attitudes to learning, and pupil performance.

1.5. The pilot is on-going, but the interim results show that:

i. 78% of pupils are now using a computer or tablet to search the internet on a weekly basis, up from 60% at the beginning of the year.
ii. More than 80% of pupils believe that the equipment has helped them in the classroom, particularly to carry out tasks set by the teacher,

talk about what they have learnt with the class, work with students in a team, compare facts, understand the information they have found, present and explain ideas, and work in a different style from their normal one.

iii. 86% of pupils think they've learned new skills; 76% that they work creatively; and 74% that they work better with classmates.

1.6. Specific examples from schools bear out these findings:

i. Independent learning: working with technology gives young people a real sense of independence and ownership of their own learning. Teachers said that the equipment has enabled more able pupils to explore subjects in greater depth, choose the device that best suits their learning needs and undertake independent extension learning.

ii. Creativity: some schools have focused on using technology to improve children's writing – an area where boys in particular often struggle. They have used apps and other digital activities to draw in reluctant writers, giving them quick feedback, creating a dialogue around their writing and building confidence. As a result, the pupils are more inclined to persevere with their general writing techniques and the quality of written work has improved, helping them to express themselves more effectively. Other schools use technology to introduce pupils to different media – such as audio and video – which they can use to create exciting work. This has not only helped them develop a range of creative skills, but, just as importantly, has given them the motivation and confidence to create new work and share it with teachers and peers.

iii. Collaboration: collaborative learning is based on the idea that learning is a naturally social act, and it is through talk and interaction that learning occurs. At our schools teachers have found that this open and collaborative approach has made pupils excited to share their work with classmates and helped to remove their fear of failure.

iv. Inclusion: technology has a disproportionate effect on children who need extra support and motivation, by making lessons more exciting and inclusive and creating new opportunities to learn and engage. One particularly disengaged boy has increasingly taken pride in his work, and, instead of distracting pupils, he is showing other children apps he has found or work he has completed.

v. Personal development: working with the equipment has given pupils a new sense of responsibility and maturity. Teachers felt that one of the greatest effects had been on pupils' personal growth and maturity, both in the classroom and outside. This is partly due to the pride they take in having responsibility for the equipment and being able to personalise it.

1.7. Overall, Samsung sees major educational and developmental benefits to increased internet usage among children, provided this is accompanied by classroom-based education to teach responsible internet use.

2. Which platforms and sites are most popular among children and how do young people use them? Many of the online services used by children are not specifically designed for children. What problems does this present?

2.1. N/A

3. What are the technical challenges for introducing greater controls on internet usage by children?

3.1. As a hardware manufacturer, Samsung has a limited ability to control how our customers use our devices, and what websites they choose to visit or what content they choose to upload or access. However, we do provide tools on our devices which give parents greater control over their children's internet use.

3.2. Our free 'Kids Mode' app for smartphones and tablets lets parents control the apps that their children can use, the videos, music and other content they can access, and how long they can use a device. A PIN code lock prevents a child from exiting Kids Mode and parents can choose how open or closed they wish the device to be to protect their children from inappropriate online content and limit them from using the device too much.

3.3. Alongside these security settings, the app has a simplified user interface that features large and colourful buttons designed for children, with controls that are uncomplicated but that give a wide range of options for children to explore. The app is packed with fun, educational games designed for children.

4. What are the potential future harms and benefits to children from emerging technology, such as Artificial Intelligence, Machine Learning and the Internet of Things?

4.1. N/A

Education

5. What roles can schools play in educating and supporting children in relation to the internet? What guidance is provided about the internet to schools and teachers? Is guidance consistently adopted and are there any gaps?

5.1. Samsung believes that schools have a crucial role to play in teaching young people essential digital skills and nurturing responsible internet use.

5.2. We are running a Digital Classrooms pilot scheme to better understand the impact of technology use in the classroom, the results of which are explored in detail in our response to Question 1.
5.3. We are also running a related project, the Samsung Digital Academy for Teachers, which focuses on training teachers in innovative ways of using technology in the classroom and supporting them with the new computing curriculum. It is based at Harborne Academy in Birmingham and it is estimated that this will improve the learning of over 14,500 students in the West Midlands.

5.4. Through these initiatives we have gained an insight into the challenges that teachers face using technology in the classroom. These fall into four priority areas:

i. Lack of confidence: the training on offer at the Samsung Digital Academy has been well received by teachers, with many returning subsequently for additional training. Many teachers lack confidence using digital technology in the classroom and implementing the computing curriculum – their enthusiasm for the training available at the Samsung Digital Academy indicates a clear appetite among teachers for guidance on how they should be using technology in the classroom. The Government should seek to build on existing initiatives, such as the Samsung Digital Academy for Teachers, to expand their impact.
ii. Lack of direction: Teachers tell us that there is an abundance of resources available for the computing curriculum, but they feel lost about which resources to pursue, or how to assess their pupils progress with the curriculum. In practice this can result in teachers attempting to try everything to see what works in the classroom, rather than systematically working through the key concepts and languages at the heart of the curriculum to build a base of knowledge. The Government should update the guidance for teachers on the computing curriculum and seek to provide an authoritative resource for how to teach the key concepts and languages in coding.
iii. Support for professional development: many teachers have been unable to take advantage of our training because their schools do not have the resources or the motivation to provide teaching cover. The Government should support schools that need to provide cover for a teacher attending off-site training.
iv. Disparity in teaching standards: there is an emerging discrepancy between pupils who have benefitted from high-quality teaching and those that have not. This becomes a particular issue when pupils transition to secondary school, as they may find they are not at the same level as their peers and their teachers will be required to teach a mixed-ability class. In this circumstance, those previously well-taught pupils might have to revisit concepts and languages they have already mastered, while those previously poorly-taught pupils will struggle to get up to speed. The Government should provide firmer

guidance on assessment to ensure all children reach the same standards.

5.5. Overall, Samsung believes that high quality teaching is crucial to the implementation of the computing curriculum. The teachers we meet through the Samsung Digital Classroom pilot and the Samsung Digital Academy for Teachers are enthusiastic about using technology in the classroom, but are held back by a lack of training or guidance. The Government can provide the resources to ensure that all teachers are well-equipped to deliver the computing curriculum to a high standard.

6. Who currently informs parents of risks? What is the role for commercial organisations to teach e-safety to parents? How could parents be better informed about risks?

6.1. Samsung recognises that learning does not stop at the school gate and parents have a crucial role to play in supporting their child's digital skills education. To better understand the barriers to parents participating in their child's learning, we held a series of 'Digital Families Days' where we invited parents to a Samsung Digital Classroom so their children could show them the work they have been doing and their parents could raise any thoughts or concerns.

6.2. The dominant feedback from parents who attended the Digital Family Days was that they see the benefits that technology brings to the classroom, and trust their children to use the internet responsibly, but many lack the confidence to support their children's learning.

i. 83% of parents we surveyed agreed that digital devices help their children learn new things and 81% agreed that developing digital skills is important for their children's future.
ii. 80% know what their children are doing online and 75% trust their children to use digital devices responsibly.
iii. The biggest barrier that parents face to encourage their children to make the most of digital technology is their own lack of confidence (19%), other pressures on their time (14%) and lack of familiarity with digital devices (14%).

6.3. However, we found that after attending the event, parents felt confident about their digital skills, for example talking to their children about staying safe online, supporting their learning at home, and setting parental controls on devices. They also had a better understanding of the role of technology in the classroom to boost their children's education and could see the relevance of coding and other digital skills for their children's future.

6.4. Overall, Samsung believes that parents need more support to be able to more fully support their children's learning. Although parents trust their children to behave responsibly online, it is crucial that they are equipped with the

knowledge to have open and informed discussions with their children to ensure they use the internet safely. Initiatives like the Samsung Digital Family Days close this gap in parent's knowledge and confidence by bringing them into the classroom, introducing them to the key opportunities and risks associated with digital devices, and engaging them with their children's learning. Samsung would support the wider roll-out of similar initiatives.

Governance

7. What are the challenges for media companies in providing services that take account of children? How do content providers differentiate their services for children, for example in respect of design?

7.1. N/A

8. What voluntary measures have already been put in place by providers of content to protect children? Are these sufficient? If not, what more could be done? Are company guidelines about child safety and rights accessible to parents and other users?

8.1. N/A

Legislation and Regulation

9. What are the regulatory frameworks in different media? Is current legislation adequate in the area of child protection online? Is the law routinely enforced across different media? What, if any, are the gaps? What impact does the legislation and regulation have on the way children and young people experience and use the internet? Should there be a more consistent approach?

9.1. N/A

10. What challenges face the development and application of effective legislation? In particular in relation to the use of national laws in an international/cross-national context and the constantly changing nature and availability of internet sites and digital technologies? To what extent can legislation anticipate and manage future risks?

10.1. N/A

11. Does the upcoming General Data Protection Regulation take sufficient account of the needs of children? As the UK leaves the EU, what provisions of the Regulation or other Directives should it seek to retain, or continue to implement, with specific regard to children? Should any other legislation should be introduced?

11.1. N/A

12. What more could be done by the Government? Could there be a more joined-up approach involving the collaboration of the Government with research, civil society and commerce?

12.1. A significant concern for Samsung is the Apprenticeship Levy. As set out in the response, Samsung supports the Government's drive to help young people to learn skills for the workplace and believes that an apprenticeship can be an effective route into life-long employment.

12.2. However, it is important that a new policy such as the Apprenticeship Levy achieves a number of central objectives:

i. The implementation of the levy must be careful not to lead to unintended and negative consequences on the investment in digital skills development and training much valued by tech companies and employees alike.
ii. The implementation of the levy must not crowd out other opportunities for tech companies to invest in talent development and allow flexibility in the methods that work for innovative business models in the tech sector.
iii. The levy must be appropriately designed to ensure the delivery of quality apprenticeships that are geared towards the high-value high-skilled jobs of the future.

12.3. UK technology businesses invest increasingly in training UK talent but, depending on the business, this training may target school children, apprentices, graduates, or professionals. It is vital that technology businesses are left to determine which types of investments in training best serves corporate needs. This is essential to ensure training efforts are geared toward the skills needs of the UK's digital economy and help learners gain sustainable long-term employment opportunities.

12.4. Digital and tech companies comprise knowledge-intensive roles which may be less suited to apprenticeships than roles in other sectors such as health and social care, construction, or retail. Therefore the implementation of the Levy, as currently proposed, will impose an overly rigid training regime which will be detrimental to our ability to train young people in the skills our business needs and risks undermining the successful digital skills programmes that we have developed in recent years.

12.5. The Levy is due to come into force in April 2017, but the details have not yet been finalised and the issues raised above have not been addressed. We would therefore urge the Government to delay implementation so these challenges can be overcome and business has enough time to prepare for this major shift in recruitment and training.

August 2016

Jenny Afia, Partner, Schillings - written evidence (CHI0024)

My background

1. As a privacy lawyer at Schillings – an international privacy and reputation consultancy – I help people in the public eye and their families reduce intrusions into their personal lives.

2. Schillings has been responsible for some of the leading privacy cases, including:

    a. Campbell v MGN Ltd[310], which established an individual's right to privacy under English Law.
    b. Murray v Big Pictures UK Ltd (for JK Rowling's child)[311] which established the law should protect children from intrusive media attention.
    c. Rocknroll v News Group Newspapers Limited[312] which considered how images from social media sites can be used by third party publishers.

3. I won Legal Week's Young Lawyer of the Year Award in 2008, am ranked as a leader in my field by Chambers & Partners and last year became Spears' Magazine's Reputation and Privacy Lawyer of the Year.

4. I am on the Leadership Council of 5 Rights[313], a civil society initiative which seeks to enable all children to access the digital world creatively, knowledgeably and fearlessly. I am also a member of the Children Commissioner's Task Force on Children and the Internet[314], formed to ensure children's interests are at the heart of the development of the internet and web-based technology.

About this submission:

5. In this submission, I respond to the following questions in the 'Call for Evidence' regarding *Legislation and Regulation*:

    a) **Q10.** What challenges face the development and application of effective legislation? In particular in relation to the use of national laws in an international/cross-national context and the constantly changing nature and availability of internet sites and digital technologies? To what extent can legislation anticipate and manage future risks?

---

310 [2004] UKHL 22.
311 [2008] EWCA Civ 446.
312 2013] EWHC 24 (Ch).
313 http://5rightsframework.com/
314 https://www.childrenscommissioner.gov.uk/news/new-children%E2%80%99s-commissioner-internet-taskforce-announced-help-children-they-grow-digitally

b) **Q12.** What more could be done by the Government? Could there be a more joined-up approach involving the collaboration of the Government with research, civil society and commerce?

Summary

6. In my view, existing English and Welsh laws are broadly and theoretically sufficient to provide protection for children's rights online. The key issue is that the laws are routinely ignored. I believe this stems from a lack of awareness as to what rights exist and some practical difficulties in applying those rights to children.

7. To address this challenge, a joined-up approach involving Government, civil society and commerce should be based around the principle that a child is a child until they become an adult, not until they go online.

8. Once this obvious but ignored principle is adopted, existing laws and commercial practices will be viewed differently, through the perspective of children. Practical changes are likely to flow. Two examples of such changes, regarding Subject Access Requests and Terms and Conditions, are suggested below.

Existing Laws

9. In July 2015 Schillings reviewed whether the "5 Rights" - namely the right to remove, the right to know, the right to safety and support, the right to make informed and conscious choices and the right to digital literacy – are reflected in English law. We regard the 5Rights as a useful tool to understand the existing rights of children and how they manifest online. They should be viewed against the backdrop of other international and national frameworks of children's rights; perhaps the most significant of which is the United Nations Convention on the Rights of the Child.

10. It was evident from our review that there is a great deal of legislation to protect and empower children online.

11. The following legislation was considered:

a) The Communications Act 2003.
b) The Copyright Designs and Patents Act 1988.
c) The Data Protection Act 1998.
d) The General Data Protection Regulation [in draft].
e) The Defamation Act 2013.
f) The Defamation (Operator of Websites) Regulations 2013.
g) European Convention on Human Rights.
h) Human Rights Act 1998.
i) The Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013.
j) The Consumer Contracts Act 2013.
k) The Consumer Rights Act 2015.
l) The Consumer Protection from Unfair Trading Regulations 2008.

m) The Computer Misuse Act 1990.
n) The Data Protection Act 1998.
o) The Electronic Commerce (EC Directive) Regulations 2002.
p) The Coroners and Justice Act 2009.
q) The Criminal Justice and Courts Act 2015.
r) The Criminal Justice and Public Order Act 1994.
s) The Education and Inspections Act 2006.
t) The Malicious Communications Act 1988.
u) The Protection from Harassment Act 1998.
v) The Video Recordings Act 2010.
w) The Education Act 2011.
x) The Minors' Contracts Act 1987.
y) Sale of Goods Act 1979.
z) The Unfair Terms in Consumer Contracts Regulations 1999.

12. Key findings from Schillings' review were that:

a) Children can ask search engines to remove links to information about themselves which is irrelevant, out-dated or otherwise inappropriate.[315]

b) Children have the right to privacy which includes privacy online.[316]

c) Children have the right to a reputation which includes the right not to be unlawfully defamed online.[317]

d) Children have the right to stop websites from publishing photos or images they have created in which they own the copyright.[318]

e) Parental consent would normally be required when collecting personal data from children under 12.[319]

f) Children have the right to find out what information any 'data controller' is holding about them, why it is being processed and who it is being shared with.[320]

g) Children have a right to know how and when their information will be used by an organisation operating online.[321]

---

315 *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González* (2014).

316 Article 8, Schedule 1, Part 1 of the Human Rights Act 1998.

317 https://www.justice.gov.uk/courts/procedure-rules/civil/rules/part21.

318 Section 96(2) Copyright, Designs and Patents Act 1988.

319 Part of the remit of the Information Commissioner is to educate UK citizens about data protection law, so the ICO generally provides easy-to-use guides to the rights and responsibilities of data subjects and data controllers under data protection law. All data controllers have an obligation to ensure that data protection policies are communicated in clear and plain language, particularly if the website (for instance) is targeted at a child. Examples of such guides are referred to in this section.

320 Section 7 Data Protection Act 1998.

321 In this sphere see also, for example, the Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013; and Electronic Commerce (EC Directive)

h) Children have the right to have their personal information stored online protected.[322]

i) It is illegal to harass a child online or via an electronic device.[323]

j) It is illegal to send grossly offensive messages to children or about them to third parties.[324]

k) It is an offence to use the internet or any electronic device to encourage or assist a child to commit suicide.[325]

l) The internet cannot be used to sexually exploit children.[326]

m) Children have the right to be protected against cyberbullying by their school.[327]

n) Children must be protected from exposure to depictions of violence, self-harm, criminal offences and sexual activity in online videos and games.[328]

o) Care must be taken when communicating marketing to children and young people.[329]

p) Particular care must be taken when broadcasting gambling advertisements or producing non-broadcast marketing communications about gambling to ensure that children or young persons are not harmed or exploited.[330]

q) Children can ask website operators not to subject them to automated decision-taking.[331]

r) On the whole, children cannot form contractually binding relationships before they turn 18 years old.[332]

Regulations 2002; Fair processing: https://ico.org.uk/for-organisations/guide-to-data-protection/?template=pdf.

322 Section 1 Computer Misuse Act 1990; Principle 7, Schedule 1 Data Protection Act 1998.

323 Protection from Harassment Act 1997.

324 Section 1 Malicious Communications Act 1988; Section 127 Communications Act 2003.

325 Section 59 Coroners and Justice Act 2009.

326 Section 1 Protection of Children Act 1978; Section 33 Criminal Justice & Courts Act 2015.

327 Section 89(2) The Education and Inspections Act 2006.

328 http://www.bbfc.co.uk/sites/default/files/attachments/BBFC%20Classification%20Guidelines%202014_0.pdf.

329 Rule 5 of the *UK Code of Non-Broadcast Advertising, Sales Promotion and Direct Marketing* (CAP Code).

330 Rule 16.1 CAP Code; Rule 17.3 BCAP Code.

331 Section 12 Data Protection Act 1998; Article 19 and 20 of the proposed General Data Protection Regulation.

332 Walter v Everard [1891] 2 QB 369; Section 3 Sale of Goods Act 1979; Chitty on Contract, 8-0003, p 757; Chitty on Contract, 8-015, p 762; *R v Oldham Metropolitan BC, ex p*.

s) Contract law protects children who cannot fully understand the significance and implications of a contract.[333]

t) Adult permission must be obtained before minors under 16 can buy complex or costly products.[334]

u) A person cannot mislead children about a product they are selling, or hide information from them.[335]

v) The online and app-based games industry must not exploit children's inexperience, vulnerability, credulity including by aggressive commercial practice.[336]

w) OFCOM has a duty to promote learning by children about using the internet.[337]

x) Schools are required to teach children about the internet.[338]

y) Children have the right not to be exposed to content on video on demand platforms which might seriously impair their development.

Application of the laws

13. The biggest problem arises not in the lack of laws but in how they are applied.

14. Based on my extensive experience in working with adults whose rights have been infringed online, I suspect children are often unaware of their rights. Greater awareness and education of the rights already in existence is critical.

Garlick [1993] 1 FLR 64; Section 3 Minors' Contracts Act 1987; Regulations 6 and 8 of the Unfair Terms in Consumer Contract Regulations 1999; Section 62(1). Consumer Rights Act 2015; Chitty on Contract, 8-052, p 779.

333 Section 9(1) Consumer Contracts Regulations 2013 (SI 1999/2083).

334 Rule 5.2.4 of the *UK Code of Non-Broadcast Advertising, Sales Promotion and Direct Marketing* (CAP Code).

335 Regulation 5 The Consumer Protection from Unfair Trading Regulations 2008; Regulation 7, The Consumer Protection from Unfair Trading Regulations 2008; Regulation 2 (5), The Consumer Protection from Unfair Trading Regulations 2008; Paragraph c of Schedule 2, Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013 (no. 3134); Regulation 6 (1) Electronic Commerce (EC Directive) Regulations 2002 (no.2013); Regulation 8, Electronic Commerce (EC Directive) Regulations 2002 (no.2013); Regulations 7 and 8, Electronic Commerce (EC Directive) Regulations 2002 (no.2013).

336 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/288360/oft1519.pdf.

337 http://stakeholders.ofcom.org.uk/market-data-research/other/media-literacy/.

338 s. 84 (3) Education Act 2002.

15. Further, existing legislation should be assessed from the fundamental perspective that a child is a child until they become an adult, not until they go online.

16. Applying this principle to our current laws highlights various practical difficulties which impact the application of the laws. To provide two examples:

    a. First, under section 9(1) Consumer Contracts Regulations 2013 (SI 1999/2083) children have a right to expect consumer information to be communicated clearly and comprehensibly. Yet the way in which Terms and Conditions are routinely presented for websites and apps is far from clear for children (indeed, even for adults). Consequently children are not able to provide informed consent before transacting with such companies.

    b. Second, under the Data Protection Act 1998, children, like adults, are entitled to make "Subject Access Requests" to find out what information a 'data controller' such as an online company holds about them. In theory, by submitting a written request a child can find out what, if any, personal data (such as photos of them, information about their hobbies) the organisation is processing, why it is processing the data, which organisations or people the data has been or may be given to and any available information as to the source of the data and to also be given a copy of the information containing the data. In most cases, the organisation needs to respond to the subject access request within 40 days.

    Yet the Subject Access Request must be accompanied with a £10 fee to reflect the organisation's costs of complying with it. This fee is likely to prove prohibitive for many children.

    I submit that the £10 fee should be waived when children make Subject Access Requests. This will transfer more cost to companies but in my view that is an acceptable expense in exchange for transacting with and collecting data about children. There is already precedent in the field of privacy law for according children's rights the highest priority in instances where there are competing rights.[339]

17. We are happy to provide further examples of practical difficulties in applying the existing legislation to children if the Inquiry would find them useful. As a firm, we have been troubled at how whole tranches of the law designed to protect children are routinely ignored by organisations and businesses that in other contexts pride themselves on compliance. The Inquiry may wish to ask representative businesses what practices they adopt to reflect the different status of children to adults when providing online services to them.

---

339 See for example *Re S*: [2003] WLR 1425 1451-1452.

18. Finally we welcome this Inquiry and in particular any changes to make legal rights practical as opposed to just theoretical.

26 August 2016

Sky – written evidence (CHI0038)

Inquiry into children and the internet

1 INTRODUCTION

1.1 Sky welcomes the opportunity to respond to the House of Lords Communications Committee's call for evidence into Children and the Internet. Sky is the UK's second largest Internet Service Provider ("ISP"), and we are proud of the record we have in taking responsibility in this area. We have led the industry by the actions we have taken to help our customers protect their families from inappropriate content, and designed products specifically for children to enjoy safely.

1.2 Development of the internet has been profoundly important, bringing immeasurable benefits to society. However, it isn't universally suitable for children and that is why we have taken a three pronged approach to safeguarding children when using the internet. First, we have designed products with children in mind to ensure they can enjoy safely internet delivered content without the risk of seeing inappropriate content. Second, we believe that education has a vital role to play, and as a leading media company we have used innovative ways to bring this to life. Finally, we have led the internet industry in creating easy to use filtering products that ensure the greatest proportion of our customers can use tools to help keep their families safe online.

1.3 We have **developed our products** to create safe ways for children to access the fantastic range of content designed for them. The most recent example of this is our newly launched Sky Kids app. The Sky Kids app offers the most loved children's TV shows, as well as new shows being produced by Sky specifically for children, all delivered over the internet. In developing Sky Kids app, Sky worked with 5Rights[340] and was driven by its principles to deliver a product specifically tailored for children. This involved working with children in the development phases to create a product that works for young people. The app has been designed with child safety at its heart and allows for parents to create profiles for each child, based on their age, to ensure age-appropriate content is curated on the home page. We have added other safety features including Sleep Mode so that parents can limit the time their children spend on the app. This allows parents peace of mind that the content their children are accessing via our products is appropriate and not harmful.

1.4 Sky believes effective **education** is at the heart of ensuring that children can use the internet safely and build resilience to face any problems they encounter. That's why in 2013, along with other major ISPs, we set up

340 http://5rightsframework.com/in-action/sky.html

Internet Matters which is an online information portal for parents, dedicated to providing information, advice and support for parents to protect their children online. We believe the government and other policymakers should strongly support initiatives such as Internet Matters, and should encourage broader industry engagement in education initiatives that help parents and children with online safety. Sky helps build resilience through our now well-established Sky Academy Skills Studio. This initiative provides schools with the opportunity to visit Sky to create TV news reports on subjects they're studying at school. Our module on online safety and cyberbullying is the most popular topic. We have the capacity to reach 24,000 young people a year, with studios at our central offices in West London and at our Livingston office in Central Scotland. Sky believes that educating children and building resilience is a crucial aspect of helping them use the internet responsibly.

1.5 Sky believes that providing our customers with the tools to apply secure internet **filtering** to home networks is a crucial aspect of child online safety. In July 2013 David Cameron, as the Prime Minister, set an objective to provide more protection for children when they use the internet. He outlined a number of measures he wanted ISPs to carry out, including the deployment of home network filtering by ensuring that both new and existing customers were encouraged to use the filtering.

1.6 Sky has led the way and has set out how we believe that the best approach is to automatically deploy our filtering for all our customers unless customers actively choose otherwise. When we deployed this model to our existing customers 70% kept some form of filtering deployed, with 62% electing to retain the parental controls element. These figures compare incredibly well to the opt-in approach we previously deployed, which saw take up rates of only 5-10%.

1.7 Due to the success of this approach and our continuing commitment to providing families with as safe as possible internet access, from July this year, we have been automatically switching on Sky Broadband Shield for all new customers the moment they activate their Sky Broadband. This means that the default filter has been set to our 13 age rating, so that sites unsuitable for anyone under that age will be inaccessible before 9pm, after which it will change to an 18 setting. The first time someone tries to access a filtered website, the account holder will be invited to amend the settings or turn it off entirely.

1.8 In July 2016 we launched a new service, the NOW TV combo, which combines broadband access with contract-free, on-demand pay TV. NOW TV broadband was launched as the first ISP with parental controls turned on automatically for all customers. Under the same system as Sky Broadband Shield, customers can turn off or configure the 'Broadband Buddy' parental controls by logging into their account.

1.9 We believe that our approach is the best way to help families to protect their children from inappropriate online content such as that contained in the scope of this inquiry. Automatic filtering will result in greater use of

home filters and greater protection of children from online risks, and Government and other policymakers should encourage industry to adopt this approach as it will result in a greater number of children being protected.

1.10 The Government has consulted on measures to introduce age verification for pornographic websites and has now brought forward legislation in the Digital Economy Bill[341]. We appreciate the challenges of regulating extra-territorial pornographic websites. Government's response to its consultation sets out that in relation to non-compliant websites, it intends to "*work with payments firms and ancillary companies to ensure that the business models and profits of companies that do not comply with the new regulations can be undermined*".

1.11 We note and welcome that "*the Government's clear position is that blocking of infringing sites [by ISPs] would be disproportionate, and would not be consistent with how other harmful and/or illegal content is dealt with ".* However we are concerned that as an ancillary service, an ISP may be in receipt of a Notice of non-compliant website, with the expectation that it undermines the business model of the website, but without any statutory obligation to do so.

1.12 We believe that if the Government is opposed to a regulatory requirement for ISPs to block infringing sites, then this should be reflected in the Digital Economy Bill so that ISPs are not considered ancillary services. This would avoid confusion as to what is expected of ISPs on receipt of a Notice.

1.13 We believe that we have demonstrated that the best way to protect children from inappropriate content is by deploying easy to use parental controls which are automatically switched on.

1.14 We would urge Government to focus on securing greater take-up of home filters by encouraging industry to move to automatic filtering as this will deal with both sites in receipt of a Notice of non-compliance and the long tail of pornographic websites not subject to the regulator's scrutiny. This is both more proportionate and a more effective approach.

risks and benefits

2 QUESTION 2: Which platforms and sites are most popular among children and how do young people use them? Many of the online services used by children are not specifically designed for children. What problem does this present?

2.1 Over the last 25 years, Sky has established itself as a successful and responsible consumer business and our customers expect us to act responsibly by delivering them the products and services they want in a safe environment. Sky fully recognises the trust that our customers place in

341 Digital Economy Bill, section 15(2), 22(1), 22(3) and 22(6), pages 18, 23 and 24

us, and in keeping with this, we want families to keep their children safe when enjoying the content we provide them online.

2.2 According to an Ofcom report, Google, with a reach of 56.1%, is the most popular and frequently visited site among children aged 6-14 from desktop and laptop computers. This is followed by MSN at 40.8%, BBC at 36.3% and YouTube and Facebook at 30.9%, with Sky at 5.4%.[342]

2.3 Although staying alert to the potential risks involved in children going online is important, it must also be recognised that the internet has developed into a very important medium for children and is a potent force for learning. It has become an essential tool in education and has had an extremely positive impact on the spread of knowledge and information. The internet is also a vital means by which children can communicate, engage and be entertained, and is overall a demonstrable force for good. In fact, according to Ofcom's report, 51% of parents of 3-4 year old children agree that the benefits of the internet outweigh the risks, and 65% of parents of 5-15s also agree with this. [343]

2.4 Historically, the internet was designed as a one size fits all medium so it is not universally suitable for children. However, companies such as Sky have led the way and have taken proactive steps to provide parents with the best tools to protect children from harmful content online. In doing so, Sky has developed a three pronged approach to combat the threats to online safety, as described in paragraphs 1.3-1.8 of our introduction above.

2.5 Sky will continue its commitment to provide its customers with the most accessible and effective tools to protect their families online. We will also continue exploring the opportunities presented by new technology to offer even greater parental controls in the future. Finally, we will continue helping government deliver its objectives for a safer internet.

3 QUESTION 3: What are the technical challenges for introducing greater controls on internet usage by children?

3.1 As an ISP, Sky's experience of the technical challenges encountered in delivering a safer internet for children has been limited. We have demonstrated that it is relatively straight-forward to develop a user and family-friendly approach to online safety so as to ensure that no one is excluded from the opportunity to benefit from better protection online. Sky has done so in line with government's 2013 objectives to provide more protection for children online.

3.2 In developing the tools, Sky took the initiative to move away from the industry-wide opt-in approach, and instead developed a default-on approach, which automatically deploys our internet filtering for all our

342 Ofcom, Children and Parents: Media Use and Attitudes Report, November 2015, Table 1, page 224

343 Ofcom, Children and Parents: Media Use and Attitudes Report, November 2015, section 1, page 10

customers unless they actively choose otherwise. Our default-on approach has greatly reduced the technical challenges of operating controls, making it as easy as possible for customers to protect their households. It ensures a safer internet experience for our customers, while still giving account holders the flexibility to choose the setting most appropriate for their households.

3.3 A recent Ofcom report shows that take-up of Sky's technical tools is significantly higher than those of other ISPs. The report shows that when we deployed this model to our existing customers, 62% elected to retain the parental controls element. By comparison, the report shows take-up for the alternative opt-in model used by other major broadband companies was between 5% and 15%.[344] This is clear evidence that Sky's default-on approach is more effective than the opt-in approach used by other ISPs.

3.4 Making the product easy for people to use and implement, as Sky has done, will guarantee a much higher engagement and use of filtering tools across the industry, thereby ensuring a safer internet experience for children. Policymakers should therefore look to initiatives such as Sky's approach to filtering, so that the industry as a whole can truly provide the safest experience for families across the country.

education

4 QUESTION 6: Who currently informs parents of risks? What is the role for commercial organisations to teach e-safety to parents? How could parents be better informed about risks?

4.1 Given the growing importance the internet has in children's lives, ensuring that parents are well equipped to deal with the challenges is essential. According to an Ofcom report, parents look to a number of different organisations to receive information or advice about how to protect their children from online risks. The report shows that 53% of parents get their information from their children's school, 14% from ISPs, 9% from Government or local authority, 6% from Get Safe Online, 6% from other websites with safety information, 5% from Safer Internet Centre/ Childnet, 4% from Child Exploitation and Online Protection Centre, 3% from the UK Council for Child Internet Safety (UKCCIS) and 2% from the Internet Watch Foundation (IWF).[345]

4.2 As a commercial organisation providing internet access to over 5 million UK home, Sky believes it can play a vital role in ensuring parents are aware of e-safety. We are very clear that technical tools alone will not adequately protect children. That's why alongside our tools and products, education plays a critical role in our three pronged approach to combatting the risks of children accessing inappropriate content online. Sky, along with other major ISPs, set up Internet Matters in 2013, which is an online information

344 Ofcom, Report on internet safety measures, December 2015, section 1,
345 Ofcom, Report on internet safety measures, December 2015, section 10, page 102 & 104

portal that provides up to date guidance and resources for parents in relation to online safety.

4.3 Internet Matters is a crucial resource with advice on a variety of parental concerns including appropriate content, cyber bullying and radicalisation as well as 'how-to' guides for setting up parental controls on a range of devices. The portal also provides information to help parents learn, talk about and deal with online child safety. Most importantly, however, it encourages and supports parents to talk to their children about how they can stay safe online.

4.4 Sky further supports e-safety education through our Sky Academy Skills Studio. This initiative provides schools with the opportunity visit Sky to create TV news reports on subjects they're studying at school. Our module on online safety and cyberbullying is the most popular topic. We have the capacity to reach 24,000 young people a year, with studios at our central offices in West London and at our Livingston office in Central Scotland.

4.5 As well as Internet Matters, there are a number of other organisations that provide parents with information to help children protect themselves from online risks. This includes UKCCIS, NSPCC, UK Safer Internet Centre and Parent Zone.

4.6 Sky remains strongly committed to continue educating parents about the dangers of the internet. However, in order to ensure that parents are better informed about online risks more widely, we believe that government and other policymakers should strongly support industry-led awareness raising initiatives such as Internet Matters, and should encourage broader industry engagement in education initiatives that help parents and children with online safety.

GOvernance

5 QUESTION 7: What are the challenges for media companies in providing services that take account of children? How do content providers differentiate their services for children, for example in respect of design?

5.1 Traditionally media companies have developed single platforms, principally designed for adults. This means they then need to include mechanisms to control access to unsuitable content. Sky has successfully done this with its PIN requirements on Sky Go. However, other platforms are less robust, merely asking if the user is over 18, and in some cases no controls exist at all.

5.2 Sky has always been committed to helping parents keep control of what their children watch and to give all members of the family content they want to watch. Earlier this year, we stepped up our efforts to differentiate our services for children with the launch of the Sky Kids app. This offers the

most loved children's TV shows, as well as new shows being produced by Sky specifically for children, all delivered over the internet.

5.3 We immersed children in the development of the app right from the beginning to ensure that the final product reflected young people's needs and personalities. In developing the app, we tested it on a panel of children every fortnight where they used (and broke) it, effectively becoming the developers.

5.4 As well as making sure it was a fun and engaging way for children to enjoy all their favourite shows, we worked closely with parents to make sure they were happy with the product. It allows for parents to create profiles for each child, based on their age, to ensure age-appropriate content is curated on the home page. Furthermore, we have added additional safety features including Sleep Mode so that parents can limit the time their children spend on the app, and transition them to a bedtime environment. Overall, this allows parents peace of mind that the content their children are accessing via our products is appropriate and not harmful.

5.5 Sky will continue its commitment to developing such products with children at the heart to provide the safest experience for families across the country.

6 QUESTION 8: What voluntary measures have already been put in place by providers of content to protect children? Are these sufficient? If not, what more could be done? Are company guidelines about child safety and rights accessible to parents and other users?

6.1 Many content providers act in a responsible manner and offer well-regulated content across all types of media. As well as providing internet services, Sky also broadcasts content over the internet via its on-demand services, including Sky Go, Sky Kids and Now TV.

6.2 Sky has taken significant voluntary steps to protect its customers across all its services including on-demand services where there are fewer rules than for linear services.

6.3 We have created parental control systems that have set the standard for the protection of minors across both linear and on-demand content. Our parental controls include PIN controls based on age ratings, the ability to block individual channels and single channels, the ability to lock particular recordings so they cannot be played back without a PIN, warnings and programme information both in the on-screen guide and in announcements before the programme.

6.4 We also provide options to set PINs on age rated content on our on-demand services. Customers of Sky Go and NOW TV can set age-related PINs on their account to prevent access to content unsuitable for children below a certain age.

6.5 Separately, industry has also developed a number of industry codes to ensure the protection of minors online. For example, in 2011, Sky together with three other major ISPs worked collaboratively to create a Code of Conduct, pledging to better inform and educate parents about how to protect children from online risks.[346] Subsequently, all signatories have gone much further in offering better and more effective parental controls.

6.6 The COBA Statement of Practice for Video-on-Demand ("VOD") services, of which Sky is a signatory, demonstrates that broadcasters are very capable of offering suitable child protection tools and information to help parents, absent detailed regulatory rules.[347] Broadcasters have decided to go further than the VOD regulation requires them and continue to innovate on the range and functionality of content protection tools and warnings provided for audiences. Sky was also an early signatory to the 5Rights initiative, which seeks to establish children's rights online by allowing them to make informed and conscious choices about what they access online. In developing Sky Kids app, Sky worked with 5Rights and was driven by its principles to deliver a product specifically tailored for children.[348]

6.7 In Europe, Sky played an important role in the European Commission's CEO coalition, which was chaired by Digital Agenda Commissioner Neelie Kroes.[349] It is a voluntary initiative designed to respond to emerging challenges arising from the diverse ways in which young Europeans go online. As a signatory to the Coalition, we committed to take positive action to make the internet a safer place for kids across five workstreams.

6.8 More recently, Sky has joined the Digital Economy Commissioner Günther Oettinger's "Alliance to better protect minors online". This is a new self-regulatory initiative launched by the European Commission gathering stakeholders from ICT, media and civil society to create a safer and more stimulating digital environment for children. The Alliance will build on the Communication "A European Strategy to make the Internet a better place for children" – a Better Internet for Kids initiative - adopted in 2012, which delivered some positive first results and identified areas for future action.[350] The members of the Alliance will work together to find common solutions to curtail exposure to harmful content and behaviour. The Alliance will identify risks and opportunities of being online, promote exchange of best practices and commit to codes of conduct.

6.9 All of the actions that Sky has taken to offer protection on its services are voluntary in nature and clearly demonstrates how industry-led solutions are more effective and adaptable than legislation. Sky, as a responsible business, will continue its commitment to delivering voluntary measures that help ensure the protection of children online.

---

346 https://www.gov.uk/government/news/isps-commit-to-aiding-parental-control

347 COBA, Statement of Practice for Video-on-Demand services

348 http://5rightsframework.com/in-action/sky.html

349 Coalition to make the Internet a better place for kids, Statement of purpose

350 Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions, European Strategy for a Better Internet for Children, May 2012.

Legislation and regulation

7 QUESTION 9: What are the regulatory frameworks in different media? Is current legislation adequate in the area of child protection online? Is the law routinely enforced across different media? What, if any, are the gaps? What impact does the legislation and regulation have on the way children and young people experience and use the internet? Should there be a more consistent approach?

7.1 The regulatory systems in place across both the UK and Europe have been effective in providing protection for viewers across a range of different media. The Audiovisual Media Services Directive (AVMSD) regulates broadcasting and on-demand media services in Europe.[351] In the UK, broadcasting and on-demand media services are regulated by the Communications Act 2003[352] as well as a plethora of co and self-regulatory measures.

7.2 All media services operate under a clear regulatory framework that places great importance on child protection and child safety. On-demand services are much more lightly regulated than linear services and they adhere to a much more limited set of rules. The differing level of regulation is justified by the fact that audiences have a higher expectation of protection when watching linear television. Moreover, consumers are much more involved in choosing their content on on-demand services and so parents have greater control over what content their children have access to.

7.3 The current scope of the AVMS Directive focuses primarily on services that are TV-like and for which providers have editorial responsibility. The Directive does not cover platforms or intermediaries. However, as convergence gathers pace, the lines between different media services become increasingly blurred and the regulatory framework is being adapted accordingly.

7.4 The European Commission is currently reviewing the AVMS Directive and is proposing to impose minimum regulatory requirements on video sharing platforms (VSPs)[353]. This would place obligations on VSPs to protect children from harmful content and incitements to hatred, and is likely to capture services such as YouTube.

7.5 In the UK, the Government is introducing legislation to encourage age verification of pornographic websites. We set out our concerns about these proposals in paragraphs 1.10-1.13.

---

351 Audiovisual Media Services Directive 2010/13/EU

352 Communications Act 2013

353 Proposal for a Directive of the European Parliament and of the Council amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services in view of changing market realities, May 2016

8 QUESTION 10: What challenges face the development and application of effective legislation? In particular in relation to the use of national laws in an international/cross-national context and the constantly changing nature and availability of internet sites and digital technologies? To what extent can legislation anticipate and manage future risks?

8.1 There are inherent difficulties in regulating access to, and content on, the internet, given the global nature of the content providers. National laws may only be effective to the extent content providers are located nationally. For example ATVOD, the former co-regulator for video-on-demand services was able to effectively regulate on-demand adult services such as Playboy TV UK/Benelux Ltd, Broadcasting (Gaia) Ltd and Saint Mackenzie's Ltd.[354] However, these companies represent a tiny proportion of global VOD pornography providers.

8.2 We have also seen how the Internet Watch Foundation (IWF) has been very effective in ensuring that where child abuse imagery is hosted in the UK, it gets taken down as quickly as possible. According to IWF's latest annual report, 38% of webpages hosted in the UK were removed in 60 minutes or less and 59% in 120 minutes or less. This has resulted in the UK now hosting just 0.2% of the world's known online child abuse imagery – down from 18% in 1996. [355] However, where the content is hosted internationally, take down is more challenging as the IWF has to trace the location of the hosting service before attempting to take steps to remove the content, and often without success.

8.3 Until now, UK policy makers have had to ensure that any UK legislation fits in with EU frameworks such as the E-commerce directive, and Net Neutrality rules. For legislation to be truly effective, it needs to be developed so that it can be applied and enforced globally. This is clearly a significant challenge.

8.4 Over the last five years, Sky has shown that responsible businesses can be highly effective in implementing customer-friendly solutions that work in a dynamic landscape. In the fast–evolving world of digital and internet development, we believe this is a more effective approach than developing legislation that would very quickly be out of date.

8.5 National policy-makers would be best served working with key industry players to understand trends and ensure that risks are appropriately managed. Care needs to be taken to avoid focusing on in-country operators subject to local regulation, but to ensure that the largest and most popular global platforms are part of any response. On-demand and other video services should be encouraged to take responsibility for user protection.

---

354 Ofcom, List of Video On Demand services currently regulated by Ofcom

355 Internet Watch Foundation, 2015 Annual Report

9 QUESTION 12: What more could be done by the Government? Could there be a more joined-up approach involving collaboration of the Government with research, civil society and commerce?

9.1 In our view it's crucial that policymakers strike a balance between implementing regulation and encouraging industry-led initiatives.

9.2 The role that industry has pro-actively played in conjunction with government to promote non-legislative solutions has had demonstrable success in combatting the threats to online safety, and has proven to be more effective than prescriptive legislation. For example, Sky has implemented effective parental controls with a take up of 62%, thereby mitigating the online risks to children to a great extent. This clearly demonstrates how developing such tools is far more effective than introducing legislation.

9.3 However, whilst Sky has taken action to push higher take-up of parental controls, we are concerned by the fact that take up has remained relatively low among other ISPs. Instead of legislating, we believe that policymakers should work with industry to promote safety online through the development of tools and education. In particular, policymakers should encourage other ISPs to deploy their parental controls in a more effective way, similar to Sky's approach.

August 2016

Sky and Vodafone – oral evidence (QQ 61-71)

Tuesday 25 October 2016

Watch the meeting

Members present: Lord Best (The Chairman); Baroness Benjamin; Baroness Bonham-Carter of Yarnbury; Earl of Caithness; Baroness Kidron; Baroness McIntosh of Hudnall; Baroness Quin; Lord Sheikh; and Lord Sherbourne of Didsbury

Evidence Session No. 5 Heard in Public Questions 61 - 71

Examination of witnesses

Adam Kinsley, Director of Policy, Sky, and Paul Morris, Head of Government Affairs and Sustainability, Vodafone.

Q103 **The Chairman:** Thank you very much for joining us, Paul Morris and Adam Kinsley. You are both extremely welcome. Although we have your biographical details here, I would ask you, if you would, to tell us a little bit about yourselves and how your work fits into the work of this inquiry, the consideration of children and the internet, our big theme. Alphabetically, Adam, you go first.

Adam Kinsley: Thank you very much for inviting me to speak here. I am director of policy at Sky. I am on the executive board of UKCCIS and have been involved in online child safety for Sky for a number of years. The area where I have engaged most closely with Government is in some of the technical measures Sky has put in place to do with filtering and, very importantly, to do with education, which we think is a critical component of keeping children safe online.

Paul Morris: I am Paul Morris, the head of government affairs and sustainability at Vodafone, which is, effectively, the public policy and CSR team. Obviously, in both buckets, we do programmes. Public policy is a very important part of this debate, which I am sure we will discuss today, and we do a number of programmes, which Sonia knows all about, which look at how we help parents and young people deal with some of the challenges of being online as well as, obviously, the benefits. We also take part in UKCCIS, IWF and some of the other main organisations that deal with this.

The Chairman: We have heard from various members of UKCCIS. Thank you both very much. Baroness Benjamin will kick us off.

Q104 **Baroness Benjamin:** I am sure you will agree that, as a society, we all have a corporate and moral responsibility for our children's well-being,

and the ISPs have a major role to play, especially in this new technological world that we are all exposed to. With that in mind, what do you see as the role of providers of the internet and mobile data services in helping to promote and inform about appropriate internet usage for children?

Paul Morris: It is a combination of things. First, the internet is now a more complex place, so you have network providers in this room today, but obviously there are other players as well and it is about how we all play a part. Clearly, from our perspective and for most of the industry on the network side, it is a combination of programmes to help educate parents and children about some of the challenges and, equally, what we can do on the technical side to ensure that they are safe to the best ability, which largely comes down to things such as filtering.

Adam Kinsley: From Sky's perspective, we think of this under three separate prongs or approaches. The first is the technical tools that we can give to our customers to help them protect their children and to prevent them getting access to content they may not want to see. The second is to create products that are safe for children to use. The final part is that we do think we have a role in helping to educate our customers who are parents. We are in over 11 million homes across the country, so we have very good reach, which is why we have invested heavily in, and promote very actively, Internet Matters as a portal we can direct parents to to get more advice and help because, ultimately, all the technical tools in the world will never be any silver bullet and education is absolutely critical, so we think that is vital.

Baroness Benjamin: Perhaps you can highlight how you actually engage with not just the children but the parents to understand the way the technology works and what is and what is not safe. What do you, as a company, do to ensure that those children and parents are engaging with what your products are about?

Adam Kinsley: Sky is one of the four larger fixed-line ISPs and we have our own safety centre within our home page on sky.com. Back in 2013, we collaborated with the other large fixed-line ISPs to come together and provide a central portal, which is Internet Matters, which provides advice, pooling everything that is out there, so it tries to get the best advice to parents. Then, our role, as a big communication provider which does a lot of marketing, is to try to direct parents to that single portal so that they can get simple advice which they can then act on. We do that in a number of ways. For example, when we were premiering the "Captain America" film on Sky Movies, we had a dedicated advert which featured Internet Matters, on all our bills we will put the logo of Internet Matters and on all our adverts you will see the logo. We can direct a lot of traffic, which means that parents are becoming increasingly aware of the risks and they can deal with them in a measured way.

Paul Morris: For us, we have a long-standing programme we run with Parent Zone, and I think Vicky gave evidence to the Committee. They produce a magazine or a guide for parents and the fifth one has just come out. We print a million copies and then we make an online version

available, which goes out pretty quickly. It is evolving, in all honesty, because it used to be about introducing the internet to parents and, when we did a bit of research before we launched this one, unsurprisingly, we found that parents are becoming more digitally sophisticated and more than half of parents now feel quite confident in advising their children, but the challenges are changing. There is a new term we are using, which is slightly ugly, which is "digital resilience", so we are moving from that early adopter stage to a point where we have to think about how. The computer may have been in the room—a laptop—you probably had one computer in the house and you could control, in a sense, that environment probably easier than you can today because people now have multiple devices connected to the internet and a large proportion of young people will have a smartphone, potentially, so it is as much about control as how we help young people have the skills to deal with being online.

Increasingly, with things such as social media, it is not just about accessing the internet or websites but about how they engage and in fairly large networks over social media. Today, a lot of that is about a skills approach and how we help people make good decisions online and then how they would deal with bad behaviour, which probably will happen in some shape or form—it is unavoidable—so this is where we are moving. We are moving from a poor sort of command-and-control approach to thinking about how we can help young people have the resilience and skills they need to deal with an always connected world as the two worlds, physical and digital, merge. I am 47, so I have gone through all this, but for young people, increasingly, that world has merged.

Baroness Benjamin: How do you get to children and young people at risk, because not all of them have parents who play a responsible role in their child's well-being? Do you point them to organisations that will be able to help them if they see something they do not like? How do you get to those children and how do you help them, once they do see something or are exposed to something, to get over it?

Paul Morris: You are involved in Barnardo's, I know, which is a fantastic organisation. From our perspective, you are right: parents are important carers of course, and obviously foster carers and others come into that bucket, but schools have quite a strong role. We have *ParentZone*, which is the parent magazine we produce and we work with them on that side. We do a lot of work with a charity, The Diana Award, and we run the Be Strong programme which is targeted at schools and has a number of modules which look at building digital resilience through skills, so we think that schools have a role as well. We will probably get on to some other questions about that and the PSHE approach, about which I know you have heard some evidence, but I think there is a role for schools as well. It is probably the best vehicle we can think of today, and you may have other ideas and we are open to that discussion. But the reality is that that might be the best vehicle, looking at how we can up some of the work in schools to help children be resilient and, hopefully, that will pick up most of those

children. You are right, we also need to think about those children most at risk as well, where some extra work might need to be done.

Baroness Benjamin: Does Sky do that as well?

Adam Kinsley: I would echo the things Paul was talking about and, clearly, needing to work with those organisations. It is also worth thinking about the internet value chain. In the most part, Sky is acting as an internet access provider, so it is, effectively, a pipe to lots of content and applications. Part of your question was what children can do if they are struggling with something. The chances are that that is going to be on a platform at the end of the pipe, if you like, and industry is doing some interesting thinking about how some of those platforms can be responsive to children who are running into difficulties on them.

Baroness Benjamin: Thank you.

Q105 **Baroness Quin:** As a Committee, we are looking at the balance between regulation and self-regulation. I would just like to get your thoughts about how effective self-regulation is and what the challenges are.

Adam Kinsley: It is interesting. When I think of all the things that Sky, as an organisation, has done, and it is a long list of which we are very proud, none of it has been done because of legislation, so, in that sense, it has all been done through self-regulation, often in partnership with the Government and policy-makers. I mentioned UKCCIS before and some interesting ideas emanate from a body such as that, and then the general way in which things happen is that companies sign up to the principles and then get on and deliver it, which has worked well in the past. We mentioned the Internet Watch Foundation, which is an incredible scheme built by industry without the backing of legislation, and it is really world-leading in that world. So much has been achieved and, to date, none of it has happened through regulation or legislation; it has all happened through industry endeavour and self-regulation, so there is a lot to be said for self-regulation.

The second part of your question ran into where we find difficulties. Clearly, there probably are some limits to how far we can go. It may be that self-regulation is not happening as quickly as policy-makers would like, but it may be that legislation will not get you there any quicker either. Also, a lot of companies in this space are global in nature, which presents challenges because attitudes differ in each country they operate within, so I have some sympathy there for them.

Baroness Quin: Do you want to add anything?

Paul Morris: I agree with Adam that quite a lot has been achieved. It is quite tricky because you cannot necessarily pass legislation in the UK to cover a company that might be based somewhere else, and we have seen that debate across a number of areas on the internet, so I think self-regulation has achieved quite a lot. If you look at mobile, we have a code that produces a blocking bar which is all self-regulated and is

now overseen by BBFC, so we decided to do that. With areas of censorship and other things, there could be issues.

If you start to unpick this and try to make legislation work, it sometimes becomes trickier. I think the principle is that, if it is working okay, let us leave it, but that does not mean that we do not think about new areas potentially. Equally, sometimes, if I am honest, we need to regulate because we need that certainty as well; I think there is a limit to self-regulation in the amount that we can start blocking. Obviously, with some of the horrible things that IWF help deal with—and they have been going for 20 years and have taken down 125,000 terrible images—that is all really good work. I think the blocking bar that we have works really well. If you are moving into new areas, it becomes more difficult for companies such as us to be in charge of what people should be doing on the internet, and then it is a role for the Government to make some of those decisions and, frankly, come to you folks and argue for them, and that becomes much more a position that needs to be sorted out. I think it depends, and it depends on the amount.

Baroness Quin: Given the international nature of some of the companies, is there an emerging international consensus about standards and how people should operate, or is that still fairly chaotic?

Paul Morris: There are attempts to do so. There is the We Protect programme, which we signed up to, which has some countries in it. Across Europe, there are attempts to harmonise. As Adam says, there are cultural differences in some of these areas. Apart from the things that are very illegal, there are differences in different countries, but I think there has been some progress in Europe in looking at this. We certainly have a team that works across Europe, and I think the companies themselves try to work pan-European, at least, so there has been progress; but let us be honest, it is certainly not a global approach.

Adam Kinsley: We are currently involved in an initiative from the European Commission, which Sonia will know because we were at the same meeting a few weeks ago, under Commissioner Oettinger, and there are differences across Europe, let alone the rest of the world. I think that we should be very proud in this country of what we have achieved, but it is challenging to roll it out across the whole world because different attitudes and cultural norms exist in this country; so we would like everybody to go as fast as we are, but it does not always happen.

Baroness Quin: We have seen some figures which seem to indicate that certain types of risks to children are still rising. Is there any kind of monitoring going on which then engages with the companies to try and address some of those issues?

Adam Kinsley: I was looking at the most recent data I could find from Ofcom on this point. This was a set of questions asked of teenagers, comparing one year to the next. It is quite striking that some of the things to do with access to content—such as concerns over seeing

things which are too old for them, or things of a sexual nature—had dropped materially in being a high priority for those teenagers, but behaviour, such as cyber-bullying, had gone up. You may conclude that the concern over seeing inappropriate things is because of the attitudes we have had to filtering and it may be that that is coming through, but I do not know.

Certainly, there is an awareness that cyber-bullying, as a behaviour, is a problem and there are initiatives to deal with that. I mentioned UKCCIS and we are involved with the Royal Foundation, which is looking at cyber-bullying as well. Through these mechanisms, you can still use self-regulation to pick up on some of the trends that are emerging.

Baroness Quin: Thank you.

Q106 **Lord Sherbourne of Didsbury:** Mr Morris, you said a few moments ago that you thought there was a limit to self-regulation and there is a role for the Government. Can you be more specific about that?

Paul Morris: The example we have is age verification on pornography sites in the Digital Economy Bill, which is going through now. I do not have the list of things, but there is an example the Government have chosen to regulate and the idea is that those sites will have age verification on them. I think there will be some challenges for those sites which are not based here, and that is still up for debate, but there is an example where, increasingly, you are saying, and rightly, that there should be some controls on these sites. I think the principle here is right also—and Adam alluded to this—that the internet is a big value chain and we can do a certain amount at the network level, but equally we have to ensure that those delivering the content also have responsibility. I quite like the principle here: that those delivering the content have a responsibility to have an age verification system, which looks as though it will be administered by BBFC, which does our content bar, but we are not quite sure who will be the regulator with the stick, if you like. The reality is that that is an example of moving into an area where it is inappropriate for children but not for an adult, to an extent, so that is where the legislation needs to come in probably.

Lord Sherbourne of Didsbury: Am I right to deduce—and this is a purely neutral question, both in the case of Vodafone and Sky—that there is nothing you would like the Government ever to do, really?

Adam Kinsley: No, that is not true.

Lord Sherbourne of Didsbury: Can you give us some more examples of what they should do other than the age verification question?

Adam Kinsley: Just to pick up the discussion about age verification, because it is really important and it is being discussed. We get to a situation whereby you have some overseas content sites, pornographic sites, and they are asked to comply with UK law, but there is a reasonable probability that many of them will not because they are out of jurisdiction. There then is a valid debate among legislators and policy-makers about what happens then, and a number of people have

said in the other place that access to those sites should be blocked by providers, such as us. We watch the debate with interest and, to be honest with you, we see merit in that argument and we are relatively agnostic about it. However, without any legislation, we cannot just block access to some sites, unless there is a power given to a regulator who tells us to do so, in which case we are perfectly happy to do it. The Bill is being debated at the moment and now is the time to have that debate in Parliament and, if it is decided that the right thing to do is for UK ISPs to block access to overseas sites, then that needs to be in legislation because, otherwise, it will not happen. That is a good example.

Lord Sherbourne of Didsbury: Are there any other examples of things you would like the Government to do?

Paul Morris: I have one, which is not filtering, but on the point we made about education. We think that probably more resources should be provided to schools so that they can use some of the great programmes run by the voluntary sector to sort out how we can have more digital resilience sessions in schools, so we think that that should be looked at.

Lord Sherbourne of Didsbury: By resources, do you mean money?

Paul Morris: I think yes is the answer.

Lord Sherbourne of Didsbury: Could that be done by the companies voluntarily, as good corporate citizens?

Paul Morris: We already run programmes that do that, but it a question of the scale, because there are 33,000 schools.

Lord Sherbourne of Didsbury: You could not do more?

Paul Morris: We run a programme ourselves that reaches 2,000 schools. Individual companies run a number of programmes which are all quite good. My concern about that is scale, because no one programme will be able to deliver to 33,000 schools. Of course, we have a role to play, and we have talked about technical solutions, but we are moving into a world where everyone will be online and people will be communicating with each other all the time and the ability to benefit from that is very large. But there is also, as I say, an increasing opportunity for people to make some bad mistakes as they are growing up, which is something that people need to think about as an action and not just rely on technical solutions, which comes back to education. Of course, we have a role to play, but my concern is how we get scale on that, so let us have the debate. I know that you have heard of general studies being the approach, with the organisation that runs it, and that is the sort of thing we need to think about.

Q107 **Lord Sheikh:** A number of people I know use the filtering system. What are the limitations of the filtering system that you utilise, and is there something we can do about it? Also, is there a possibility that all filtering might prevent children carrying out legitimate work they are involved in? Do these filtering systems provide the right environment to

make them child-friendly, as against providing overkill?

Adam Kinsley: There are a few questions there. The one on filtering and whether there is a risk that access to important information is over-blocked is a good question. When we launched our network-level filtering in 2013, it was a big debate and a concern. Under UKCCIS, there was a working group on over-blocking and we worked with a number of sexual health charities to make sure that they were absolutely on a white list and would never get blocked, and we have some evidence about the level of over-blocking as we have worked through those groups. I can say pretty confidently that those risks which were at first highlighted and debated, and rightly so, have not come to pass; children can access the right information where they need help, and sexual health advice and things such as that are absolutely accessible, so I am confident on that.

On the question of the limitations of filtering, we would be the first to say that it is not a silver bullet; you cannot rely on the technology to keep your family safe. If any parent thought that, we would be delivering our messages incorrectly. It absolutely needs to be supplemented with some parental responsibility, and we will help educate them on that. The tools and the technical filtering can be extremely good for younger children to prevent them inadvertently seeing content that would upset them and that they are not looking for, but have stumbled across. With older children who are seeking out this material, it becomes harder and there are challenges; you can work your way around any system, including this one. You end up where this idea of digital resilience is critically important because, at some point, you are not going to be able to protect them by preventing them seeing things, and they are going to see things they do not like, but they then need to learn how to deal with the content they are then exposed to, so I think it is important. We think it works very well for certain classes of children. The last Ofcom report suggested that 97% of parents who were using these network blocks were happy with them, and that is quite a high rate of approval, so they are doing a good job in their space, but we cannot rely on them.

Paul Morris: We are in the same boat. The BBFC helps us run our content block, which avoids over-blocking, which is one of your concerns, and I think it works pretty well. None of these technologies is going to be absolutely perfect, but it probably, if anything, errs on the side of caution, which I think is the right approach. Clearly, we are not saying that you can always block because, if a child cannot access a site, there are other avenues through their parents and other ways, so the reality is that it is probably better to err on the side of caution and, as Adam says, we are pretty confident that, on most occasions, it works well. Within the BBFC system, people can appeal if they think they have been over-blocked or they have been blocked for no reason, and there have been a handful of those. The BBFC reports back quarterly, so there is a process by which, if a website thinks it is being blocked, it can appeal.

Lord Sheikh: How do you monitor the adequacy of the filtering systems? Presumably, it is a moving target, so can the filtering system be overcome by a child or do you need participation by an adult? How do you monitor the adequacy of the systems?

Paul Morris: The approach is in place and you cannot turn it off, unless you are 18, so that is how we report it and yes, we keep an eye on it. We rely on expert advice as well and, effectively, the BBFC will give us that expertise in what we should be doing. But equally, we monitor it, we have data on the numbers and how it is used in other things, and we keep it under review.

Lord Sheikh: Do you get feedback from the parents, for example? Is there communication between you and the parents?

Paul Morris: Yes, we get it, obviously, through our customers. Our customers will ring us about a number of things and there is that feedback. We do not get strong feedback about this. It is on by default and the majority of people leave it on when they could turn it off. Generally speaking, we do not get a lot of negative feedback about it and, if we did, that would be a shame, so we are fairly confident that it is the right thing to do. We are still in the process of looking at what else can be done, so we are looking at other technologies we can bring forward, and I know this guy is going to talk about something they have done as well. We are still looking for innovation in the handset and what more can be done. Clearly, there are other players in that, so the handset manufacturers and others also do things, so there is a dual approach there.

Lord Sheikh: Are there any alternatives to a filtering system to keep a check on what children can view? Could something else be made available, or is it available?

Adam Kinsley: There are a number of ways in which parents can intervene and mediate in their child's activity online, and they range from quite intrusive to just sitting down and talking about it; it depends on where you are on the scale of parenting styles. There are software providers out there which will allow you to remotely control the access the child has on a different device. The challenge that a company such as Sky has and the reason we have brought in network-level filters is that there are so many connected devices in our customers' homes now. I am not sure what the latest data is because it must keep moving up, but the chances are that there will be eight, 10, 12 connected devices in the home and, whilst you might be able to set controls on each device, it becomes too much to ask of a parent and what they want is something which is quite simple to apply. Our solution is very simple, it is not terribly sophisticated, it does not have lots of bells and whistles, but you can buy products which have bells and whistles if that is the approach you want to take as a parent; there are the products out there. We like ours.

Lord Sheikh: Could they be varied and could a child interfere with these systems?

Adam Kinsley: Usually, they have checks and balances.

Lord Sheikh: Do they need input from a parent?

Adam Kinsley: Yes, our one does. On our one, the account holder creates the settings, the environment and the categories which are filtered in a very easy way, and it is password-controlled.

Lord Sheikh: So, if it is password-controlled, only the parents should know the password?

Adam Kinsley: Correct and, if the settings do change, so somebody manages to get in, an email is then sent back to the account holder to say that the settings have just changed, which is quite a good belt-and-braces approach.

Lord Sheikh: Are these filtering systems only in the English language or do you make them available in any other language, bearing in mind of course that Polish is the most popular language, apart from English, and the third is my mother tongue, Punjabi? Are they available in other languages?

Adam Kinsley: It is a good question.

Paul Morris: That is a really good question. I do not know if we produce it in other languages, but I will check and come back. I think probably not, but it is worth checking, and it is also a good point.

Lord Sheikh: Thank you.

Q108 **The Chairman:** With both Vodafone and Sky, your default option is "on" and people have to make a conscious decision to turn it off. We heard earlier today the alternative viewpoint, which is that people should be given a choice as to whether they turn it on or off because this gives them an opportunity to think through the specific things they want to filter out to do the job properly. It is said, in the case of the default being on—your system—that people get irritated and just turn it off, so it is a negative. You have carefully thought this through and decided that it is better to go in with the default button on and make people turn it off rather than say, "It's up to you and here are the options", which gives a sort of buy-in, as is the counterargument.

Adam Kinsley: Yes, we have done both, so we have been on a journey. When we started off and introduced our network-level broadband shield control in 2013, the term created was "active choice". Previously, we had controls, but they were hidden a bit and you had to find them, which was quite hard. We then created this system where, when you became a Sky customer, a screen would appear and you were told, "Please make a choice one way or the other, yes/no". We did a few things, a bit of nudge theory. We highlighted the "yes" button and we tried to encourage take-up. It is the same back-end system, so it is the same categories and it is rated PG/13/18, which is very simple, as I mentioned before. When we looked at the evidence, the take-up rate was surprisingly low, around the ballpark of 8% to 10%. When we introduced it, it was part of a commitment to David Cameron, the previous Prime Minister, and there was a second part to this, which said, "You also should present an active choice to all your existing

customers", not just the new ones coming on board. When we looked at how best to do that, we determined that the cleanest way to do it was to ask them to make a decision by email and communicate with them and, if they did not come back to us—and most did not—we said, "We will turn it on on a certain day but if you don't want the controls, you can then turn them off".

That is what we did and the results were remarkable. Of the number of people who kept it on after a sustained period of time, 70% had some form of control and 62% had kept the parental control piece, so we then had a decision. We said, "Hang on a minute. We've deployed this same technology in two different ways: we have asked the question and asked them to think about it; and we have turned it on and, once it was on, they quite liked it". So we then said, "Okay, we have to change our sign-up policy here" and, rather than asking them, "Do you want it on, yes/no?", we said, "We have put it on. You can turn it off if you want" and, lo and behold, the take-up rate has gone up to over 60%, so we are pretty convinced it is the right thing to do. We are the only fixed-line broadband company to do that, and we introduced a new broadband service, Now TV broadband, and we launched it completely default-on earlier this year. We have considered both options and we are pretty confident we have got the right outcome, if the objective is high parental engagement and high take-up of controls.

Paul Morris: From our perspective on the mobile side, we have had the content bar in place for a number of years. Historically, a broadband connection would be in the house—not for every child but hopefully the majority of children, there is parental supervision in the house; obviously, with a mobile it could be subtly different—and we have always taken the view that the content bar is best on by default. I think we are still of that view. Clearly, it is only on our network, so you could go to other networks or Starbucks and have a different experience, but then you have the active choice coming in at that point. So we do not control the whole environment because it is only when they are on our network, but I still think, as the industry, that it is the right choice and, as I say, it has been in place for some time.

The Chairman: Thank you.

Q109 **Baroness Bonham-Carter of Yarnbury:** Going into a slightly different area, we have heard quite a lot of concern about the time that children and young people spend online, on devices and so on. This is specifically for you, Mr Kinsley, for Sky: what prompted you to create a Sky Kids app and how does the app, now you have created it, take account of the age of the people who are using it?

Adam Kinsley: It is an evolution of the idea that there are lots of connected devices in the house and people are using them to watch content. Our research showed us that 80% of children have access to a tablet, so in that environment you have got potentially young children using tablets, so there is probably an enhanced degree of parental anxiety as to exactly what they are doing online. As I said in my introductory comments, the internet is a very positive place giving

some excellent and profound changes to the way in which children grow up, but it is not universally acceptable that everything is right for them. If you are giving a child a tablet that you can control by voice activation and you do not even have to be literate to use it, it becomes potentially a dangerous tool, and most children are not looking for bad content.

We thought that, by creating a safe environment for children to enjoy safe and positive content, it would be a welcome initiative, so that is what we did. I am really proud to say that we did that in conjunction with 5Rights and Baroness Kidron—it was great working with her—which meant that we created this for children. In the way we went through the design process, it was almost built by children, going through constant design refreshes with panels of children, which is just great to watch, seeing them trying to break the thing, and giving them something which they can really use and love. In fact, today's session is very timely because Sky has just released some wonderful new episodes of "Morph" this morning, which I had the pleasure of watching with my young children and saying, "This is the TV that we used to watch", so that is fantastic and is proving really popular. In some of the stats I have here, we are seeing an 80% year-on-year increase in downloads and streams of up to 10 million per week of children's content and we have 4,500 hours of children's content on here, which may bring us to another concern about screen time—how much you want them to see. Sky would like them to watch quite a lot, and it is all good stuff, but we have built into this a bedtime mode, which means that parents can have a setting which says, "Okay, you can watch that for 30 minutes" or whatever and then it turns itself off. There are new releases just this week, so it is constantly evolving.

This is the part of the three-pronged approach whereby the open internet has lots of stuff on it that you would not want children to see, and I think it is up to brands such as us to say, "We can do so much to prevent you seeing the bad stuff, but let's make this a positive experience and let's give you an online experience where you are just enjoying curated and safe content that children will feel safe with".

Baroness Bonham-Carter of Yarnbury: Have you done any research into who is actually going to your app, the demographics of it? Is it very middle-class?

Adam Kinsley: Our customer base tends to be right across the whole spectrum of the country, so I suspect, with that many downloads, it is transcending class and is being used by all sorts of people. I have not got those demographics, but I can certainly look into seeing if we have them. We try to model it so that it is age-appropriate, so depending on whether the child is pre-school or not, to give them a better experience.

Baroness Bonham-Carter of Yarnbury: Thank you.

Q110 **Baroness Kidron:** My question builds on those of Baroness Bonham-Carter. When we do not have a central record of identity, and there are very good reasons why we do not, and when you have a design that is for ultimate convenience—I am talking more about platforms than the beginning of the food chain, as it were—you then have an issue of not

knowing who is online, which means kids can be considered adult. Various people have put to us ideas around design that would help children. The one we felt was most powerful and simple was from a couple of head teachers who said, "Why not have maximum privacy settings by default?", which is the argument you have just made on filtering. My question is: what would good design look like and what can you see from where you sit that would actually help young people be treated well online? Here, I would urge you to take a behavioural stance, as well as a content one.

Adam Kinsley: I understand where you are coming from and I think it is the right line of questioning—that this has to be built into applications by responsible businesses by design. As I say, we did it with the filtering by turning it on, which was at the time a pretty controversial thing to do, but we thought it was the right thing to do. There is only so much that an internet access provider can do but, if you are talking about the end content applications, I think it is down to those companies—and it is often the big brands which are doing this—to do the right thing and build in the safety by design. If they stuck to the 5Rights principles, they would get there, so everybody should sign up to 5Rights; that is what we say.

Baroness Kidron: Beautifully put.

Paul Morris: There is a lot that can be done at the network level, but, equally and increasingly, we need to look at the broader value chain and continually ask those questions, because the risk to young people is subtly changing, as we have highlighted. There is probably more risk of being cyber-bullied or upset by a network that they might know or have some connection with than of potentially seeing certain content through a website. I am not saying there is not both, but that is the new reality and there might be processes that need to be put in place to deal with that.

Equally—and you can ask these companies—to be fair to them, they all do a reasonable amount, they all engage in all the bodies and other things, so I would not say they are doing nothing and ignoring this. But you are right: we should continue to look at it and understand how we can include the whole value chain because that is the only way we will get there, I think.

Baroness Kidron: The thing I would like to press you on is that a lot of sites are built on constant interaction and are promoting sharing. The bedtime function is a key thing. We hear a lot about compulsive use and kids not sleeping, which in fact was the evidence we got from teachers. One of the things that the Children's Media Foundation raised was the Google login, where you are always on and your data is, therefore, being gathered. Are there specific issues that worry you in any of those areas, or perhaps another that I have not thought of?

Paul Morris: You are right: the challenge here is it is an always-on world that our young folks, certainly teenagers, live in and, as a parent, you go through processes where you can use control and then hopefully teach your children. I remember as a child being told how much

television I should watch. The idea when I was a child that you would have so much screen time would never have happened, but that is the reality of today. The point is that there are controls there today and you can turn off the broadband connection through apps, but the challenge does come back to how we, as parents, deal with that scenario. There is only so far that technology will get you because, ultimately, you will always be able to turn these things off, which is the truth of it. If your child knows the password, for example, which they should not, they will be able to turn it off. Do you see my point? Although there is more, I think we should continue to look at how technology and the wider chain can help. Clearly, it comes back to how we ensure that we, as parents, think about these things. The increasing evidence that we see is that parents are becoming more digitally savvy, but the challenge is expanding, which is the reality of being a parent, I guess. But it is a question of dual approach here.

Adam Kinsley: The always-on culture and the amount of screen time is a fascinating area, and I have changed my mind on it—from thinking that it was a problem to recognising that screen time means all sorts of different things. Sometimes it will be educational, sometimes it will be relaxation, sometimes it will be interactive and social and it is not necessarily a bad thing, and certainly restricting it could be quite dangerous. Therefore, we come back to this idea of digital resilience over everything because trying to starve children of the oxygen of the screen, I think, is a dangerous road to go down.

I have in the back of my mind a letter I read yesterday from the parent of a child who, unfortunately, committed suicide as a result of online activity. She said that at one point, she tried to take away the phone because it was causing so much grief, which made it much worse for him. That is really quite striking and it is on top of some academic research. We have to make sure that our young people are more resilient to the risks that exist. That means not just education, but that responsibility is taken for the platforms where they are interacting and where they will come into difficulties. The ability to get an answer from the platform if they report something they do not like, and to know they have been heard—those sorts of things are critically important and would go a long way to helping a lot of young people when they do encounter difficulty.

Q111 **Baroness McIntosh of Hudnall:** Moving on to a slightly different area, there are the risks you have been describing of people getting into difficulties, but then there is the amount of data that is collected or is just circulating generally as a result of all this interactivity. First, what sort of data do you collect generally on your customers; secondly, when it is children, how do you mitigate the risk of data being collected inappropriately and it then being used or disseminated inappropriately, and all the associated risks of it being hacked and accessed?

Adam Kinsley: Clearly, data is the lifeblood of a large part of the internet value chain.

Baroness McIntosh of Hudnall: Precisely.

Adam Kinsley: The point I would make is that, generally speaking, most of our activity is as an access provider, so I go back to this idea of a connecting pipe to the internet. Therefore, other than some data to manage our network and make sure it is not going to break, fall over or go too slow, we are trying not to collect any personal data—we do not want it—and particularly children's data. We are designing systems to avoid it, so our interaction where we might collect, specifically, children's data is very limited. Clearly, with the Kids app, we were in that space, but we were very careful not to collect that personal data, other than a name so that the child can create an icon and they are not interacting with anyone else. I think it is less a question for an internet access provider than for social platforms with the vast amounts of data that they are likely to collect.

Baroness McIntosh of Hudnall: But social platforms cannot operate without you. You made the point very precisely that it is part of the value chain, and you are all part of the value chain. I suppose my pushback to you on that would be: okay, so you, as a business, are not in the business of collecting data, but you are in the business of making it possible for other people to collect data, and in what sense does that confer—or perhaps it does not—any responsibility on you?

Paul Morris: First, we are much the same as Sky and we collect enough data to, hopefully, provide you with a reasonable customer service, but not much more than that. We have been through this debate with the Investigatory Powers Bill, frankly, as it is part of the same debate. The point here is that, with encryption—and lots of quite well-known apps, such as WhatsApp, use encryption—we increasingly do not really know what is in the packet that is going across our network. Secondly—this is a debate we put forward on the Investigatory Powers Bill as well—it is important that, when you are a user of an app, a piece of technology or a platform, you know what the rules are and what is going on with that platform. It becomes increasingly difficult if, behind the scenes, a network provider such as ourselves, with data crossing the network, gets involved. In this area, of course, we do choose to be, but, as we have discussed, there is a limit to that. There is a technical limit, but equally I think there is also, in some instances, another limit, which is about people feeling as though their data has been grabbed at a point where they have not agreed to it. In this area, clearly, it is different because it is about online safety for children, but there is a principle here that, if we start moving into another area, it seeps into it.

Baroness McIntosh of Hudnall: Just on the issue of the right to be forgotten, is that technically possible, desirable and achievable?

Paul Morris: To an extent. This is European legislation, and we are going through the process of how we will introduce it, so let us not go down that route, but it will come in in May 2018. I think most people are going through the process now of thinking how that will happen and, as I understand it, the right to be forgotten is fine, but you will be allowed to continue to keep data that can help you service the customer. For example, someone would not be able to say, "I don't

want you to keep the data of my billing" and we will see how that plays out, but I think there is going to be a balance on how it will work and, of course, we will come up with systems that work. We are ISO-accredited on data, which is absolutely vital for our business. We have seen some high-profile data attacks, and we invest a lot of time to make sure that we keep people's data safe, even fairly mundane data, so it is very important for us and is becoming increasingly important for any network to have that security around it.

Baroness McIntosh of Hudnall: Given that children are all over the internet with and without their consent, and given that who you are when you are 14 is not who you are when you are 24, is it particularly more difficult, more important or more anything, technically or morally, to get to grips with that?

Adam Kinsley: Absolutely I agree with you that it is an issue, but the point I was trying to make earlier is that, as an access provider, we will have a relationship with our subscriber who will be paying the bills, who will be an adult. Everything that goes on in that house is coming through our pipe. We are not looking into who it is or anything like that, and we are not allowed to do it even if we could, but, clearly, within that pipe is traffic which is going from individual users, some of whom may be children, who are interacting on applications at the other end which may need logins and things such as that, and we have no visibility of what that content is. In any event, all we would see, if we could, which we cannot, would be a subscriber and that that computer has interacted with that platform, so we do not hold and we could not interrogate, pull out and strip out data for children if they wished to be forgotten. That needs to happen at the application end because they will have the databases of all the photos, messages or whatever it might be. Hopefully, that distinction helps.

Baroness Kidron: I absolutely understand that you are at the easy end of the data debate because you do not look at it, but you also mentioned self-regulation and that you have a seat at the table in all these places. We hear that applications that kids regularly use, when they update, automatically turn on their GPS, so you have kids posting photographs from all over the place. You have a seat at the table and I understand that you cannot look at that or prevent that, but what is your attitude towards that sort of data problem, even if you are not technically responsible for that?

Adam Kinsley: There are a lot of issues about keeping children safe online, some of which we can do something directly about and we do, and others which are more tangential but we still care about because we are part of the value chain. We actively engage in this, and we have mentioned UKCCIS, but we are also trotting over to Brussels to sit through meetings at the European Commission because we think it is the right thing to do. A lot of the issues being discussed are not our bit of the value chain, but we are looking to engage and create a healthy environment and, to be honest with you, to push best practice from the UK into other jurisdictions, which is true in a lot of areas. This is

another area where we do not have direct control, but we would want to encourage a safer place for children.

Baroness Benjamin: Young children who sex-text and send messages and images do not quite realise this, but at the NSPCC, we find that a lot of children, young boys especially, have then got a criminal record, so they cannot be forgotten. What do you do to inform those young people about sending those kinds of messages and that there is no way back?

Paul Morris: This is the educational programmes we spoke about. We try to do our best to work with organisations to try and teach young people how not to do those things. It is very difficult, and that is a good example, but you will never be able to turn off the ability to post a photograph. That is just not going to happen, so it has to be education. In a magazine this year, there was a page on it, and it is a big issue, the criminalisation, which I think they have been looking at and there has been some review of it, so clearly there is a debate to be had with law enforcement as well, and it is probably a combination of that and education. If you have a mobile, we will not be blocking people from being able to send photographs—and that is a photograph to another person, it is not on a website—so, with the best will in the world, it has to be how we help people think about their actions and not do it in the first place, and then obviously the law enforcement is separate.

Earl of Caithness: Can I follow up on Baroness McIntosh's question, which also goes back to your answers to the fourth question? Do we have any data on your customers who should be using but are not using controls, and is there a hole out there of which we are not aware?

Adam Kinsley: The short answer is no, we have not got that data. We know that we turned on the controls for everybody on day one and then people decided if they did not want them. We have not gone to the next stage, which would be the internet police and knocking on doors, saying, "Why haven't you got your controls on?" and we do not have the data. We have not looked at it by demographics or anything else and we have not mapped it across in any way and, whilst it would be quite interesting, I think that is probably a good thing.

Q112 **Earl of Caithness:** My second question is probably the most important and has been on the minds of all of us for a long time: the General Data Protection Regulation. I am sure you think about it daily. Have you made an evaluation of it and, given that it is likely to come into force before we exit from the EU, is it going to make any difference and should parts of it be incorporated into UK law when we do go?

Paul Morris: To answer your first question, we have data on the amount of people who turn on and off their content control, but not everyone is a parent, not everyone has children, so that is what you have to deal with, and we do not always know that. Frankly, I am not sure, if you were a customer, that I would say, "Are you a parent? How many children do you have?"; that becomes very difficult.

On the General Data Protection Regulation, and I want to thank the Committee for giving me the opportunity to mug up on that over the last few days, it comes in in May 2018, so we will be in the EU at that point. There are a number of proposals in it which will involve change across our businesses, because it is a change. We have already had EU legislation in place for a number of years, but this is a change. Effectively, we put together teams to ensure product by product that we comply, which we are doing at the moment. We are still thinking about our exact approach on a number of issues on Brexit, but we can clearly see that data crosses borders and data will still cross borders, so we will need to find a way to ensure that we can mirror a number of regimes around the world, including the EU way, in my view.

Adam Kinsley: I can be brief on this because we are in a similar position, in that we are currently going through our analysis. This is one of a number of directives or regulations, which have been passed or are in the process of being implemented, where we are having to think, "How do we deal with this over the next two or three years?"

Paul Morris: It will be working and in place before we leave the EU, which is the important thing.

Q113 **The Chairman:** The other EU one is net neutrality, which has been around the course a few times. The fear is that these new EU rules will make it illegal for you to put your filters and blockers on in the way that you do at the moment. Are you reacting already to this? Are you thinking that maybe it will never happen? Where have we got to?

Adam Kinsley: Net neutrality has happened. It came into force in April of this year, I believe, and it is a regulation, so it has direct effect. It does not really get into the detail of filtering. We have been in discussion with the Government and the regulator, who feel fairly confident that it will it not have a significant impact in this area.

The Chairman: Would it have done already if it were going to?

Adam Kinsley: It has been slightly strange, and here we get into the complexity of European legislation, but BEREC produced its final recommendations on how regulators should interpret the regulation and that was passed at the end of August, I believe, so there has been a bit of a holding pattern. Ofcom is the regulator and it is engaging at the moment with industry on how to enforce the regulation across a number of areas.

The Chairman: But your view is that it is not going to have a big impact?

Adam Kinsley: At the end of the day, the filters which we have, parents can have them on or off, and it would be a somewhat bizarre outcome if we were not able to protect children in this way. It feels like one where, hopefully, common sense will prevail.

The Chairman: Bizarre and unlikely.

Adam Kinsley: It is an interesting one. Earlier on, we were talking about the new legislation that is being passed on age verification and,

in that world where there might be an expectation that an ISP blocks access to some content but without being told to do it by a court or by legislation, that feels more problematic under net neutrality, which is why I gave that as an example where legislation may be helpful.

The Chairman: The legislation we are currently looking at, though, would only cover paid-for sites that were unsuitable.

Adam Kinsley: What you are talking about is our blocking access to a website. We cannot unilaterally block it with no ability to turn that off, under the net neutrality rules.

Baroness Benjamin: Is that because you think that you would be challenged if you did?

Adam Kinsley: Yes; I think 10% of relevant turnover is the fine, which tends to focus the mind somewhat.

Baroness Benjamin: Do you think we should really be pushing for legislation where age verification is concerned?

Adam Kinsley: If there is a desire for ISPs to be blocking access to those sites, then legislation is required. It is basically down to the will of Parliament. If you want ISPs to block, I think they will struggle to do so, unless they are compelled to, and not because they do not want to but because they would probably be breaking the law.

Baroness Benjamin: When you have put this argument, what has been the answer?

Adam Kinsley: On the Bill which was only introduced recently, we have made the point and it has been quite actively debated in the Scrutiny Committee so far, so we are watching with interest.

The Chairman: We are too. We have worked you very hard indeed. If there is anything we have not covered, perhaps you could think about that and send us any further evidence that you have. For all that you did share with us, we are very grateful and thank you both very much indeed. It has been a very useful session.

Dr Vera Slavtcheva-Petkova – written evidence (CHI0054)

Dr Slavtcheva-Petkova is a Senior Lecturer in Journalism, Department of Media, University of Chester

1. Summary

1.1 The evidence presented below addresses the following questions posed by the Inquiry: (1). What risks and benefits does increased internet usage present to children, with particular regard to: i. Social development and wellbeing, ii. Neurological, cognitive and emotional development, iii. Data security. (5). What roles can schools play in educating and supporting children in relation to the internet? (12). What more could be done by the Government? Could there be a more joined-up approach involving the collaboration of the Government with research, civil society and commerce?

1.2 The submission presents the results of two academic studies: 1. "Evidence on the extent of harms experienced by children as a result of online risks" (addressing question 1 with a focus on risks and conducted in collaboration with Dr Victoria Nash from the Oxford Internet Institute and Dr Monica Bulger). 2. "Children, Europe and the media" (addressing question 1 with a focus on benefits, question 5 and question 12). Sections 1.5 – 1.8 and 2 - 3.3 cover the first study, and sections 1.9 and 4 cover the second study.[356]

1.3 The first study investigated the research evidence base about the actual harms experienced by children as a result of Internet use. We looked at all peer-reviewed journal articles published on the topic in English between 1997 and 2012. We conducted a systematic literature review and we identified three main types of harms as outlined in 148 empirical studies: health-related harms as a result of using pro-eating disorder, self-harm or pro-suicide websites; sex-related harms such as Internet-initiated sexual abuse of minors, and cyber-bullying.[357]

1.4 The second project was a mixed-methods study conducted with 174 children, their parents and teachers from the UK and Bulgaria that explored what children know and how they feel about their own country and about Europe, and what factors influence their perceptions, and national and European identities. The study was particularly focussed on the role of the media (including the Internet) in that process as well as the interplay between social structures (class, gender, ethnicity), socialization agents (school, parents, peers), national context and individual agency.

---

356 Detailed findings on these and a range of other related topics can be obtained via the University of Chester's institutional repository at http://chesterrep.openrepository.com/cdr/simple-search?filter_field_0=author&filter_type_0=equals&filter_value_0=Slavtcheva-Petkova%2C+Vera&sort_by=dateissued&order=DESC

357 This project was funded by the University of Oxford's John Fell OUP Research Fund.

1.5 The first study demonstrated that the evidence base about the actual harms experienced by children as a result of online use is rather thin. The majority of harm-related studies do not present evidence about actual harms. Instead they tend to discuss potential harm and risks. Harm is rarely defined as a term and is often conflated with risk. A lot of researchers (especially on a topic such as cyberbullying) rely on surveys or other self-reported measures as opposed to documentary evidence based on actual cases or more immersive qualitative studies (e.g. online ethnography or interviews).

1.6 The evidence in some areas is more conclusive than in others. Documented cases based on police, court and medical records present evidence about young people sexually abused and psychologically or physically traumatized as a result of establishing initial online contact with perpetrators, children assisted or encouraged in their suicide attempts after visiting pro-suicide forums, and adolescents feeling encouraged to self-harm or pursue their eating disorders as a result of regularly using self-harm or pro-eating disorder websites.

1.7 The number of children who have suffered extreme harm is very small in comparison with the overall number of Internet users. Vulnerable children are more at risk.

1.8 The thin evidence base is a significant issue because policy interventions, especially increased regulation, should be made on the basis of solid and documented evidence. There is a general prevalence of survey-based projects and/or textual analyses of websites as opposed to triangulated studies based on real-live case studies and/or utilizing a range of methods and resources. The Government can encourage this type of research by prioritising these types of projects via the available research funding channels (e.g. through the Research Councils).

1.9 The second study demonstrated that primary school can play a fundamental role as a political socialization agent and by teaching media literacy in general and digital literacy in particular from a very young age. Rather than focussing almost exclusively on the potential dangers of internet use, schools should do much more to educate children how to use the Internet (and other media) in a positive and educational way (and not just for homework purposes), including as a valuable resource on news, current affairs and information about other nations, cultures and ethnicities.

2. Risks and harms: the evidence base

2.1 We conducted a systematic literature review of peer-reviewed empirical studies about harms associated with Internet use by under-18s, published in English between 1997 and 2012. Our initial database search retrieved more than 4000 articles but we narrowed them down to 148 after strictly applying the criteria for inclusion: (a) empirical work, (b) published in peer-reviewed journal, (c) main focus of study was young people (aged under 18), (d) central focus on Internet use and (e) addressed incidents of harm originating from online interactions.

2.2 Three main types of harm were outlined in the literature: 1. Health-related harms. 2. Sex-related harms. 3. Cyberbullying. There is no or little evidence base for consumer-related and data security/privacy-related harms, which are frequently mentioned in policy debate.

2.3 Scale of health-related harms: 63 academic articles presented evidence about health harms related to Internet use. This category included: eating disorders such as anorexia and bulimia (30%), self-harm/self-injury (16%), suicidal thoughts and suicides (14.3%), Internet addiction/Problematic Internet Use (11.1%) and mental health issues such as depression or psychological distress (6.4%). Other harms mentioned were aggression, sexually risky behaviours, use of stimulants and alcohol, and obesity.

2.4 Severity and frequency of health-related harms: most studies presented evidence of perceived or potential harm (the majority of studies focusing on eating disorders analysed the content of "pro-ana"/"pro-mia" websites and/or were based on surveys) as opposed to "actual" harm (e.g., documented by practitioners or evidenced by case studies). Only 11% of the studies were based on case studies. 44.4% were based on surveys and 25.4% on textual analysis of websites.

2.5 The "scariest" actual harm cases reported suicide attempts or suicides, facilitated by or incited in the online space. The most extreme cases included individuals who felt pressurized to take their own lives after declaring that they would do that online, or cases when adults "assisted" young people in their suicide attempts by advising them what drugs to use or actually supplying them with these drugs.

2.6 The online forums of some of these websites (in particular the "pro-ana"/"pro-mia" websites) also provided a support network for sufferers, which in many cases was the only support network they had access to and trusted. A number of researchers agreed that some pro-eating disorder websites could be helpful but only to people who already had anorexia. Some websites posted disclaimers which said that if you were not an anorexic, it was better not to read the information on the website because it might be harmful for you. Potentially harmful content included: "thinspiration" materials, weight loss or purging techniques and prevention of help-seeking and recovery by presenting anorexia as a lifestyle as opposed to an eating disorder.

2.7 Scale of sex-related harm: 49 academic articles presented evidence about sex-related harms linked to Internet use, focusing predominantly on online solicitation/grooming, child abuse and pornography. Three main types of studies: 1. 51% analysed the process of Internet-initiated sexual abuse, frequently on the basis of offenders' accounts. 2. 45% studied predictors of sexual offense such as risk factors and offenders' characteristics as well as whether the consumption of child abuse images ("child pornography") led to offline child sexual abuse. 3. 25% of the studies investigated the "effects" of exposure to pornography or being a victim of Internet-related sexual abuse such as a range of psychological and physical harms.

2.8 Severity and frequency of sex-related harms: the evidence base in this category was much stronger because a number of studies (18%) were based on police and/or medical records. Nonetheless, more than half of the articles reported survey data (some surveys were repeatedly used). The scale of harm in Internet-initiated child sexual abuse was extensive but the evidence about the link between viewing and downloading child abuse images and offline sexual abuse was inconclusive. Harms reported: victims suffering from feelings of shame, hate, disgust, fear, repression, guilt and speechlessness.

2.9 Cyberbullying: 36 academic articles presented evidence about potential or actual harms related to cyberbullying. 36% outlined the prevalence of cyberbullying, 17% investigated the impact of cyberbullying on anxiety, 11% looked at the association between depression and cyberbullying, and 11% were focused on predictors of cyberbullying. The majority (97.2%) of cyberbullying studies reported survey results.

2.10 Scale and impact of cyberbullying: studies reported significant cross-national, intra-national and age differences in the prevalence of cyberbullying – from 9% to 72%. There was a clear association between cyber-bullying/Internet harassment and psychological harms such as distress and depression as well as self-injury and suicide attempts. Victims of both cyber and traditional bullying were most likely to experience psychological issues.

2.11 Most cyberbullying studies investigating the link between cyberbullying and anonymity concluded that in the majority of cases the victim knew or suspected who the cyberbully was. Cyberbullying was linked to children's overall social positioning and experiences and did not occur in a vacuum.

3. Internet harms: definitions

3.1 Harm was operationalized in 44.5% of the health-related harm studies. It was defined as self-harm in the majority of these studies, including parasuicide, self-mutilation or self-injury. Other types of harm mentioned were: physical harm, desensitization to violence in real life, psychological harm, encouragement of eating disorders and distraction to academic performance.

3.2 Harm was not explicitly defined in most of the sex-related harm studies. In about a third of them an assumption could be made about what the authors meant by harm, for example, sexual abuse, bodily/physical harm, emotional/psychological harm, and social harm.

3.3 Harm was explicitly defined as a term in only 27.8% of the cyberbullying studies. Half of them discussed psychological harm and negative effects, including depression. Other types of harm mentioned were: self-harm, social harm, and potential for physical harm.

4. Benefits of Internet usage and the role of school

4.1 The evidence presented in this section is based on a mixed methods study conducted with 174 9-10-year old children, their parents and teachers. The study investigated the role the mass media (including the Internet) play in

relation to children's national and European identities as well as their knowledge of Europe and the European Union. The project also investigated the interplay between the main socialization agents (media, school, parents and peers), social structures (class, gender, and ethnicity) and individual agency in the process of identity formation and political/cultural knowledge acquisition. The study included semi-structured interviews with children, parents and teachers as well as content analysis of news items, textbooks and national curricula.

4.2 Children's political socialization as citizens is rarely studied in academic research and it is also of little (if any) interest to policy makers, but it is of extreme importance because identity formation is an active process that does not happen overnight once adolescents "officially" become adults. Political participation and civic engagement are key components of an effective democracy so it is important to trace the role of the different socialization agents (including the Internet) in that process. Furthermore, empowered and knowledgeable children are in a much better position to resist and confront extremism and bigotry, which appear to be on the rise in British society. Mediation by parents, teachers and peers is an essential aspect of children's political socialization.

4.3 38.8% of the children in my English sample indicated that the Internet was a source of information on news for them even at that relatively young age. School was a source of information on news for 35.8% of the children and parents for 52.2%.

4.4 The acquisition of political information in primary school children is most effective when even if initially accessed via the media, it is subsequently mediated either by parents or by school (and in some cases by peers). When shown photographs of national and international symbols, historical figures and current personalities, including high-profile national and international politicians, children recognised the symbols and faces they had either seen in the media (mainly on TV) or at school. When prompted to provide more information about the respective personality/symbol, children showed much greater confidence and ability to do that in cases when they had discussed who that person/symbol was at school in addition to the information they might have come across in the media.

4.5 While TV's role in this process of knowledge and collective identity formation seemed indisputable, it was much more difficult to establish what role the Internet played and how school could facilitate this role. Children reported engagement in a range of activities online, but acquisition of political and cultural information did not appear to be channelled through a small number of specific websites.

4.6 Schools can play a much more active role in that respect by encouraging the positive use of the Internet, including as a source of political information and by pointing children in the direction of reliable websites or in the very least teaching them how to identify reliable websites. Media literacy is essential and schools should play a much bigger role in educating children about the media than they currently do.

4.7 Children receive plentiful guidance at school on how to avoid online dangers but they need more structured and directed guidance on the positive usage they can make of the Internet, including as a source of political and cultural information. Quite indicative of the generally negative/safety-driven discourse about the Internet is the fact that most schools mark Safer Internet Day (an EU initiative) but do not celebrate International Internet Day, which has a much more positive focus. Internet safety can be much more effectively taught if we shift the focus of the narrative in a more positive direction.

4.8 School and socio-economic status are the two factors that influence children's knowledge of and feelings towards other nations and cultures the most. Therefore, school's role in that respect is of essential importance. Poorer children did not even realise that the UK was part of Europe (One child from a deprived area remarked: "Europe, is that in New York?"). Given the widespread availability and use of the Internet even among children in deprived areas, schools should play a much more substantial role in relation to media literacy/digital literacy and political socialization/civic engagement.

23 September 2016

South West Grid for Learning (SWGfL) – written evidence (CHI0009)

Risks and benefits

1. *What risks and benefits does increased internet usage present to children, with particular regard to: i. Social development and wellbeing ii. Neurological, cognitive and emotional development, iii. Data security.*

2. *Which platforms and sites are most popular among children and how do young people use them? Many of the online services used by children are not specifically designed for children. What problems does this present?*

The UK Safer Internet Centre hosts a dedicated helpline for the entire children's workforce, The Professionals Online Safety Helpline, (also referred to as POSH) www.saferinternet.org.uk/helpline which is operated by South West Grid for Learning (SWGfL). The helpline is well established and works in partnership with organisations such as CEOP, National Crime Agency, NSPCC, Social Services, Schools and Internet Platforms to ensure the safety of children online. The helpline is seen to be at the forefront of incident management for non-criminal matters and as such is often the "go to" for media outlets reporting on relevant stories. The broader team of SWGfL carries out significant work in schools directly with young people and their carers, delivering online safety awareness and training sessions. These two areas of work provide us a unique insight into the trends and behaviours of young people online.

For the last two years, the preferred sites for young people have been Snapchat, Instagram, Kik, Whatsapp, YouTube and then the more traditional social media platforms such as Facebook and Twitter.

Gaming is a an area where children are often exposed to inappropriate content by playing and using games that despite being PEGI rated are either ignored by them as players or not understood by parents. This is evidenced by the UKSIC Online Safety Team that visit schools on a regular basis delivering Online Safety Sessions to children, teachers and parents.

We often use the example of the Rockstar's Game 'Grand Theft Auto'. This is clearly rated as 18 with warnings on graphic content, sexual material, alcohol & drugs. However when we talk to children it is clear that nearly all year 4 plus children know the game and can tell you about the characters. With half of classes actively playing it and that number growing with the increase of age of the children. Couple the inappropriate content with online activities and these sorts of 'games' can have a serious negative effect.

The activities being undertaken are socialising (both publically and via private messaging apps), learning, research, and the problematic issues are around bullying, sexting and privacy.

There are regular issues with under 13's using apps and websites which are required to be COPPA compliant (https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule) being reported to POSH, most are fairly low risk or harm matters such as embarrassing YouTube video's or inappropriate behaviour on social media. Most sites have relatively easy to find and use routes for reporting these accounts, Google being the exception. They have moved the email/form for reporting underage accounts several times over the last 3 years and it is currently hosted as part of the "legal issues" section.

Concerns about younger users accessing these sites are unsolicited contacts from strangers, grooming risks (assisted by the naivety of this age group), access to inappropriate or scary content and bullying.

3. *What are the technical challenges for introducing greater controls on internet usage by children?*

There a large number of sites which have been designed with children in mind, a rare few have been successful, in part due to the merchandising which accompanies them, these include Club Penguin, Moshi Monsters and Bin Weevils. All these are now defunct. The problem with child friendly sites is that young people can feel patronised, and there is an allure of "adult" sites, which this segregation only adds to.

Moderation of younger sites – moderation, also age verification

4. *What are the potential future harms and benefits to children from emerging technology, such as Artificial Intelligence, Machine Learning and the Internet of Things?*

As with all technology, there are significant benefits from future tech to education, the future workplace and home, which young people can recognise and embrace. We are moving into a new area of accessibility which has limitless possibilities. The concerns about this are of course the speed at which they grow – are the providers themselves ready and can they ensure user safety? How do the people in post to keep children safe keep up with emerging threats? And how do the Police stay informed and equipped to manage incidents?

5. *What roles can schools play in educating and supporting children in relation to the internet? What guidance is provided about the internet to schools and teachers? Is guidance consistently adopted and are there any gaps?*

Schools have a responsibility, through the legal duty of care, for ensuring that all pupils and staff are safe. This includes protecting staff and pupils from the dangers associated with electronic communications. It is the duty of the Headteacher to ensure that all staff are aware of the possible dangers associated with electronic communications, and the means for ensuring safe usage. The head teacher may, however, delegate day to day management of e-safety issues to a member of staff who is sufficiently knowledgeable, trained and competent.

It is also the responsibility of the governing body to ensure that policies are followed to ensure the safety of the school community.
Following the consultation launched in December 2015, the Department for Education has published its response and revised statutory guidance; 'Keeping Children Safe in Education'. This revised guidance is for schools (including academies, free schools special schools, PRU's and independent schools) and colleges across England and will become active on 5th September 2016 (until then, the existing version published in July 2015 remains in place). This guidance sits alongside other work such as Ofsted Guidance for Safeguarding which references Online Safety throughout.

SWGfL have played an instrumental role in advising the Government, Ofsted and others in online safety. Each year in conjunction with Plymouth University a 'state of the nation' report is released comprised of data from 7000 schools relating to online safety by SWGfL. In the last report[358], adopted by UKCCIS, numerous headlines figures were published including the fact that 40% of primary schools only had a basic filtering system in place and 6% had none at all. It also highlighted that 55% of school governors and 50% of staff had received no online safety training. Policies around technology were also poor with 35% of primary schools having no policies around mobile phones.

Professor Andy Phippen who compiled the report said "In general the report shows that while schools are increasingly aware of online safety issues, reflected in their policy scope and development, they are less able to ensure effective training for both staff and governors, which does raise the question around the effectiveness of schools to engage with the ever changing issues that arise in the field".

The question is not so much what role they have, but how capable and equipped are schools to manage and support children with online safety issues.

6. *Who currently informs parents of risks? What is the role for commercial organisations to teach e-safety to parents? How could parents be better informed about risks?*

There are several main organisations who support parents. The UK Safer Internet Centre hosts a parents advice area and carries out regular parents sessions in schools, as well as leading on Safer Internet Day (February each year) where parents are one of the target audiences. Last year Safer Internet Day reached 40% of UK Children and 20% of UK Parents. The educational resources were downloaded 316,000 times and the video productions used to promote online safety for the day where viewed 240,000 times. In addition the day was supported by the media including the BBC, ITV, major newspapers and many more. The day generated 800 news items and 194 TV Broadcasts.

The main UK organisations are:-

- UK Safer Internet Centre
- Internet Matters

358 www.swgfl.org.uk/report2015

- O2 NSPCC
- CEOP

Governance

7. *What are the challenges for media companies in providing services that take account of children? How do content providers differentiate their services for children, for example in respect of design?*

8. *What voluntary measures have already been put in place by providers of content to protect children? Are these sufficient? If not, what more could be done? Are company guidelines about child safety and rights accessible to parents and other users?*

We were involved in the UKCCIS working groups which created these two resources
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/487973/ukccis_guide-final__3_.pdf

https://www.internetmatters.org/wp-content/uploads/2015/12/Official-UK-social-media-guidance-UKCCIS.pdf

Most sites have robust terms of service or community standards which include safeguards for children such as not being searchable to non friends, or having privacy settings in place by default. Some sites are difficult to navigate when searching for guidance for parents.

Legislation and Regulation

9. *What are the regulatory frameworks in different media? Is current legislation adequate in the area of child protection online? Is the law routinely enforced across different media? What, if any, are the gaps? What impact does the legislation and regulation have on the way children and young people experience and use the internet? Should there be a more consistent approach?*

There are a number of criminal offences that can be applied to online safety but most of these have not been developed specifically to address situations online. These include:-

- Offences Against the Person Act 1861, s16 (Threat to Kill)

- Protection from Harassment Act 1997 s1,2,4,4a (Fear of violence, harassment, stalking etc.)

- Malicious Communications Act 1988, s1 (electronic communications which are offensive, threats, cause distress or anxiety)

In addition other offences can be applied like the Contempt of Court Act 1981, Sexual Offences Amendment Act 1992, s5 (identification of a victim of a sexual offence)

However all these offences pre-date social media and only cover England and Wales. With the internet knowing no geographical borders or boundaries when a perpetrator is outside of the area it becomes increasingly difficult to apply any sanction or protection.
The Regulation of Investigatory Powers Act 2000 (RIPA) is also an area of concern with overseas providers refusing to acknowledge the process and therefore denying law enforcement agencies the ability to investigate not necessarily to prosecute but in many cases just to safeguard.

We have also already mentioned the PEGI rating scheme for games and the issues with it being adhered too.

We do find that platforms are far more willing to assist and help when they are given a choice and work towards voluntary arrangements. Good examples of these are the CEO Coalition to make the Internet a better place for kids. Launched in 2011 it is designed to respond to emerging challenges arising from the diverse ways in which young Europeans go online.

There is also the Safer Social Networking Principles for the EU. Again a self-regulatory agreement signed by the major social media companies as well as researchers and child welfare organisations.

https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/sn_principles.pdf

Our concern is that if legislation is forced onto companies especially those who are principally outside of England and Wales and based overseas that they may withdraw both from UK geographical locations and from agreements shown above, returning to foreign territory and therefore not engaging as they currently do.

10. *What challenges face the development and application of effective legislation? In particular in relation to the use of national laws in an international/cross-national context and the constantly changing nature and availability of internet sites and digital technologies? To what extent can legislation anticipate and manage future risks?*

This is always a difficult area, the UK has little recourse over offences committed overseas and there is concern that the UK leaving the EU may exacerbate this issue further. Industry have always been clear that while they wish to work with the UK to keep users safe, they do not support legislation or regulation per se. There needs to be work carried out on international data sharing for the investigation of crimes, MLAT agreements are very slow.

11. *Does the upcoming General Data Protection Regulation take sufficient account of the needs of children? As the UK leaves the EU, what provisions of the Regulation or other Directives should it seek to retain, or continue to implement, with specific regard to children? Should any other legislation should be introduced?*

No? I don't think children were in mind when this was being drafted however!

12. *What more could be done by the Government? Could there be a more joined-up approach involving the collaboration of the Government with research, civil society and commerce?*

There has been an increase in awareness and engagement with Government on this topic over the last few years. Initiatives supported by various departments such as home filtering, friendly WiFi, Dare to Care, Reclaim the internet and "This is Abuse" all demonstrate the power of collaborative working. This momentum needs to continue and must remain cross party and transparent to ensure fairness and access for all relevant organisations.

August 2016

Stonewall – written evidence (CHI0039)

Children and the internet inquiry

Introduction

1. Stonewall is a national charity which campaigns for lesbian, gay, bisexual and trans (LGBT) equality in Britain and abroad. We warmly welcome this opportunity to respond to the Committee's inquiry into children's access to, and use of, the internet.

2. Stonewall works with over 1000 schools to embed LGBT equality across the education sector. We want every school to be free from homophobic, biphobic and transphobic bullying and ensure that every young person is free to be themselves, regardless of sexual orientation or gender identity.

3. Stonewall believes the internet is an excellent tool for young people to access important resources, learn about the real world and connect with other young people. We are however concerned that if misused, online services can be a place where young people may access misleading information, inappropriate content and be subjected to cyberbullying or harassment.

4. This response focuses on the experiences of LGBT young people and their use of the internet.

LGBT young people and the internet

5. Many LGBT young people feel isolated growing up due to a lack of visible role models and an education that is rarely inclusive of LGBT issues. University of Cambridge research for Stonewall in *The School Report* (2012) – which surveyed more than 1,600 lesbian, gay and bisexual young people – found that **53 per cent** of LGB young people had never been taught anything about LGB issues at school. Furthermore, **35 per cent** of LGB young people said their school library didn't contain books or information about LGB issues and a further **50 per cent** didn't know whether their local library did.

6. As a result, LGBT young people frequently turn to online services to learn about LGBT issues and meet other LGBT young people. For example, research from *The School Report* (2012) found that **63 per cent** of LGB young people had used the internet to meet other LGB people.

7. Whilst an excellent tool, using online services can pose risks to young people's health and wellbeing. LGBT young people who use online services can become victims of cyberbullying – research from *The School Report* (2012) found that **23 per cent** of LGB young people had experienced it. Additionally, LGBT young people can face other risks such

as blackmail and grooming from adult chatrooms and websites – and can face barriers to reporting through fear of being 'outed', that they will not be taken seriously or will face discrimination because they are LGBT.

Schools

8. Research shows that LGBT young people face high levels of bullying both online and offline. *The School Report* (2012) found that **55 per cent** of LGB young people have been subjected to homophobic and biphobic bullying. Additionally, the *Metro Centre's Youth Chances Survey* (2014) found that **28 per cent** of trans young people have experienced physical abuse at school. We know from our work with teachers across the country that many staff feel ill-equipped to support trans young people when they are being bullied.

9. Stonewall welcomes the Department for Education's recent update to the *Keeping Children Safe in Schools* statutory guidance as it highlights the severity of online safety by increasing its prominence. Due to come into force on the 5 September, this guidance recommends schools ensure they have the appropriate filters in place and that they include online safety within the curriculum. Stonewall recommends this guidance is regularly revisited during teacher training and we await to see how this is implemented to ensure it successfully considers groups of young people who may face specific vulnerabilities.

10. Stonewall greatly welcomed Ofsted's commitment to tackle homophobic, biphobic and transphobic bullying in schools by ensuring a school's measures to tackle it are an integral part of their inspection process. We believe that Ofsted should build on this commitment by ensuring that inspectors are guided and trained to consider different groups of pupils and specific experiences and vulnerabilities, including LGBT young people when inspecting e-safety.

11. Schools can take practical steps to tackle bullying both online and offline. Stonewall strongly recommends that anti-bullying policies include specific on tackling homophobic, biphobic and transphobic bullying, that this includes cyberbullying and is linked to e-safety policies. Additionally, staff should receive regular training so that they have the confidence to tackle homophobic, biphobic and transphobic bullying, cyberbullying and online safety.

12. Stonewall recognises the importance of online filters and monitoring systems to protect young people from harmful online content at school. However, while they play an important role in protecting young people from such content, we are concerned that they can also inadvertently block access to vital, age-appropriate information. We know that some online filters block searches which include specific words and search terms – for LGBT young people, this can prevent them from accessing important information. Stonewall recommends that online filters should be regularly reviewed to ensure what type of content is blocked and so that appropriate sites can be unblocked by staff.

13. Stonewall has supported thousands of teachers to tackle homophobic, biphobic and transphobic bullying and to create more inclusive environments through a range of best practice education resources and training. Additionally, many schools and young people have used Stonewall's #NoBystanders campaign in a range of innovative ways to stand up to hate and abuse – including online.

Personal, Social, Health and Economic (PSHE) education and Sex and Relationships Education (SRE)

14. Stonewall believes that one of the most effective ways to protect young people from harmful material and abuse online is to embed the principles of online safety within the school curriculum. The provision of high-quality Personal, Social, Health and Economic (PSHE) education and Sex and Relationships Education (SRE), which includes LGBT people and experiences, is key to increase online safety and reducing the risks associated with online services. We remain concerned that the provision of PSHE and SRE in schools is not compulsory and join others across and beyond the education sector in calling for inclusive, statutory PSHE and SRE.

Social media platforms and online forums

15. *The School Report* (2012) found that **39 per cent** of LGB young people use social media platforms such as Facebook and more than **35 per cent** use online youth forums. The growth of social media in recent years means figures on usage are likely to be higher.

16. Stonewall is becoming increasingly concerned that levels of cyberbullying, harassment and grooming are increasing alongside the usage of social media platforms and other online forums. Furthermore, there remains a lack of transparency in the frequency of abuse cases and this means the severity of the issue remains unknown.

17. Social media platforms and online forums have a key role to play in ensuring young people can use their services safely and responsibly. It is crucial that these platforms put in place clear and simple-to-use reporting tools that allow young people to alert when a case of online abuse has occurred – and, that it is then followed up so that the young person reporting is made aware of the outcome. Stonewall also believes that social media platforms and online forums should begin to track and record incidences of abuse on their services by type so that they can more effectively gauge the scale, identify and target problem areas such as homophobic, biphobic and transpobic abuse.

Legislation

18. There are a number of existing pieces of legislation that relate to cyberbullying and online harassment. Stonewall is concerned that what constitutes online abuse and criminal behaviour is poorly understood by

the general public, and often by the police. Without this clear understanding, it is difficult to both establish the scale of, and to effectively tackle, online abuse towards young people. Stonewall would like to see greater clarity and a streamlining of existing legislation. Alongside this, we need guidance which is easy to understand and easily accessible to both young people and parents, so that they are fully aware of their protection under the law, how to respond and where to report different forms of online abuse. Finally, police forces should receive guidance and training to deal appropriately with cases of online abuse involving young people.

August 2016

Karl Taylor, Jennifer Roberts, Emily McDool, Philip Powell, Department of Economics, University of Sheffield – written evidence (CHI0008)

Written evidence to be found under Philip Powell

techUK – written evidence (CHI0047)

About techUK

techUK welcomes the opportunity to provide written evidence to the House of Lords Select Committee on Communications on the topic of Children and the Internet. techUK is the trade association for the UK technology sector, representing over 900 businesses. techUK's members range from leading FTSE 100 companies to new innovative start-ups. Collectively they employ more than 800,000 people, about half of all tech sector jobs in the UK. The majority of our members are small and medium sized businesses.

Children and the internet: Call for Evidence

1.1 The internet is interwoven into the fabric of life for adults and children. It has changed the way we learn and interact with the world, enhancing creativity and self-expression. Parents, policy makers and the technology industry have worked hard to enable the online world to be a positive environment for children and young people.

1.2 This response highlights four key aspects of the technology industry's work to protect children and young people online:

- **The UK has developed one of the best partnership models in the world for government, industry and wider stakeholders to ensure that parents and children have the tools and knowledge to make smart and responsible choices online.** Working through the UK Council for Child Internet Safety and the Internet Watch Foundation, as well as internationally through WeProtect, these partnerships work to foster a positive environment for children and young people.

- **The online world offers opportunities for children and young people to learn, create and communicate**. Children's use of technology can be beneficial for digital skills, and can have a positive impact upon their future, career, and life skills.

- **Technical solutions are available to help parents keep their children safe online.** Parental controls and family friendly network level filtering are easily available and some online services have developed specialised products for children and young people.

- **Education and outreach play a critical role in creating a safe internet environment for children**. Technology companies work in collaboration with NGOs and other organisations enhance the confidence and resilience of parents and children and build a culture of tech literacy.

1. How the increase in use of and access to the internet is affecting the development and wellbeing of children in both positive and negative ways.

This response refers to Questions 1(i) and 4:

> **1. What risks and benefits does increased internet usage present to children, with particular regard to:**
> **i. Social development and wellbeing**
>
> **4. What are the potential future harms and benefits to children from emerging technology, such as Artificial Intelligence, Machine Learning and the Internet of Things?**

2.1 The benefits of internet usage are constantly evolving – the online world offers opportunities for people of all ages to learn, create and communicate. The rapid increase in new products and services over the last few years, from MOOCs to messaging, and from gaming to helping with homework, provides fantastic opportunities for innovation and self-expression for young people to seize upon.

2.2 UK internet users agree, with Ofcom's 2016 Communications Market Report showing that internet users believe that increased connectivity broadens people's horizons, encourages people to stay informed, enables greater work flexibility, and allows them keep up to date with family and friends.[359]

2.3 Many parents agree on the positive impact of children and young people's use of technology. Recent Family Online Safety Institute research shows that parents see a beneficial effect on their child's technology skills (92%) and their ability to research and find information (89%). Additionally, 78% of parents believe that their child's technology use has a positive impact on their future, career, and life skills, and 64% think it positively affects his or her creativity. They are also optimistic about the impact technology use has on their child's performance in school (58%) and communication skills (55%).[360]

2.4 The UK tech industry works hard individually and in partnership with Government and wider stakeholders to tackle important issues such as inappropriate content and online abuse. These collaborative partnerships work to foster a positive environment for children and young people to create and communicate as new and innovative technology is developed. Some of these current activities are explored further in the following sections.

2. The responsibility of industry to develop and maintain controls, and the responsibility of users to practise self-governance.

This response refers to Questions 6 and 8:

---

359 http://stakeholders.ofcom.org.uk/binaries/research/cmr/cmr16/uk/CMR_UK_2016.pdf
360 https://www.fosi.org/policy-research/parents-privacy-technology-use/

6. Who currently informs parents of risks? What is the role for commercial organisations to teach e-safety to parents? How could parents be better informed about risks?

8. What voluntary measures have already been put in place by providers of content to protect children? Are these sufficient? If not, what more could be done? Are company guidelines about child safety and rights accessible to parents and other users?

3.1 There are aspects of our online world which are inappropriate for our children, just as there are in the offline world. The UK has made great progress in championing technical solutions and a number of broader education and awareness activities to ensure that children do not access inappropriate materials and to enhance the confidence and resilience of parents and children.

3.2 Many technical solutions are available to help parents manage and keep their children safer online, such as free parental controls like Symantec's Norton Family[361] and Microsoft's Family Safety[362] features. Family friendly network level filtering, which applies to all the computers and devices using the home broadband service, have been provided by the four main internet service providers since 2013.[363] Parental controls are also built into devices (e.g. Xbox, PlayStation, iPhones and iPads)[364] where restrictions can be enabled to protect children from inappropriate content.

3.3 Some online services have created specialised products for children and young people. For example, Google has developed a Safe Search function which can help block inappropriate or explicit images from search engine results. [365] YouTube Kids provides a restricted version of YouTube for families, with no public comments, easy flagging and optional search.[366]

3.4 The responsibility of users to practise self-governance is also a key tenet of protecting the online environment as a positive space for both adults and children. Social networking sites such as YouTube identify community guidelines with clear ground rules of what is and is not acceptable, including hateful content, nudity or sexual content, and online harassment and bullying.[367] If users find inappropriate content they can submit it for review to YouTube staff, and serious or repeated violations can lead to account termination.

3.5 In addition to technical solutions, it is critical that education and outreach continue to be essential parts of the overall response in building a culture of tech literacy and fostering a positive environment for children and young people. The technology industry works actively with a range of NGOs and organisations to provide parents with the knowledge and support they need to get the most out

361 https://onlinefamily.norton.com/familysafety/basicpremium.fs
362 http://windows.microsoft.com/en-gb/windows-10/set-up-family-after-upgrade
363 http://stakeholders.ofcom.org.uk/binaries/internet/internet_safety_measures_2.pdf
364 https://support.apple.com/en-gb/HT201304
365 https://support.google.com/websearch/answer/510?source=gsearch&hl=en
366 https://kids.youtube.com/
367 https://www.youtube.com/yt/policyandsafety/communityguidelines.html

of technology and deal with any challenges it might bring. These include, but are not limited to:

- **Safer Internet Day:** an annual campaign celebrated globally in February, the UK campaign was coordinated by the UK Safer Internet Centre with the 2016 theme 'Play your part for a better internet'. Over 1,140 organisations supported the day, making it the biggest campaign to date. Safer Internet Day 2016 reached 40% of UK children and 20% of UK parents - 2.8 million children and 2.5 million parents.[368]

- **Internet Matters**: backed by the four main Internet Service Providers (BT, Sky, TalkTalk and Virgin Media) as well as the BBC and Google, and supported by leading child online safety experts, Internet Matters is an online portal to provide advice and allow parents and teachers (primary and secondary) to make informed choices when tackling e-safety issues.[369]

- **The Right Click workshops**: BT and UNICEF UK are working together to deliver a programme of online safety workshops across the UK. With the aim to deliver 600 workshops by the end of March 2017, the initiative is aimed at empowering children to use the internet positively while staying safe and equipping parents with the tools to help keep their children protected online. This is being rolled out to schools that have attained UNICEF UK's Rights Respecting Schools Award (RRSA) which actively supports UK schools to put children's rights at their heart to improve well-being and help all children reach their full potential.[370]

- **Internet Legends**: Google recently partnered with Parent Zone to bring a new internet safety initiative to primary schools around the country. Reaching 10,000 students in this academic year, the tour aims to inspire young people to stay safe and create a positive culture online. Google are now working with Internet Matters to extend the programme reach to parents.[371]

- **Digital Parenting Magazine**: Vodafone and Parent Zone partnered to develop the Digital Parenting Magazine to help young people and families get the most out of their digital technologies and deal with the challenges that these bring. Over 1 million magazines have been sent out to schools.[372]

- **Barefoot Programme:** supporting primary educators in developing the confidence, knowledge, skills and resources to teach computer science. The programme includes free high-quality resources, lesson plans and

368 http://www.saferinternet.org.uk/safer-internet-day/2016
369 https://www.internetmatters.org/
370 http://www.unicef.org.uk/rights-respecting-schools/training-and-support/internet-safety/
371 https://www.google.co.uk/intl/en-GB/safetycenter/families/legends/
372 http://www.vodafone.com/content/digital-parenting/learning-and-fun/digital-parenting-magazine.html

local CPD workshops. Supporters include BT, Raspberry Pi, and the Department for Education.[373]

- **Summer safety workshop series**: Google experts visited five cities across the UK in summer 2015 to help thousands of people across Britain improve their awareness on how to be safer and more secure online. The workshops provided detailed introductions for how to be safer online using simple tools and attendees were also offered further one-to-one online safety consultations.[374]

- **CLICK: Path to Protection:** a joint initiative between BT and the Marie Collins Foundation, the aim is to create a framework that will eventually train all front line workers to improve the aftercare given to children who have been affected by online abuse and their families. The training content has being developed by a group of experienced professionals including representatives from education and children's services, psychology services, the College of Policing, the Association of Chief Police Officers' lead for Child Abuse (ACPO), the Crown Prosecution Service (CPS) and academia.[375]

- **Duke of Cambridge's Royal Foundation Taskforce on the Prevention of Cyberbullying**: leading technology companies including Google, Snapchat, Facebook, Twitter, BT, EE, Sky, BBC, TalkTalk, Telefonica, Virgin Media, and Vodafone, alongside experts, NGO, and a panel of young people are supporting the Duke's new industry-led taskforce to support young people and their families affected by cyberbullying.[376]

- **UK Council for Child Internet Safety** (UKCCIS): a group of more than 200 organisations drawn from across government, industry, law, academia and charity sectors who work in partnership to help keep children safe online. UKCCIS also recently published advice for parents, schools and colleges, and social media providers to help keep children and young people safe online.[377] UKCCIS has recently undergone reform, with a refreshed membership and new working groups. This should allow it to focus on issues and identify the right actions and who should lead them.

3. Legislation and regulation in this field.

This response refers to Questions 11 and 12:

---

373 http://barefootcas.org.uk/
374 https://events.withgoogle.com/google-safety-workshop-leeds/
375 http://www.mariecollinsfoundation.org.uk/news/post/10-bt-and-marie-collins-foundation-programme-to-help-online-sexual-abuse-victims
376 https://www.royal.uk/leading-technology-companies-join-royal-foundation-taskforce-prevention-cyberbullying
377 https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis

11. Does the upcoming General Data Protection Regulation take sufficient account of the needs of children? As the UK leaves the EU, what provisions of the Regulation or other Directives should it seek to retain, or continue to implement, with specific regard to children? Should any other legislation should be introduced?
12. What more could be done by the Government? Could there be a more joined-up approach involving the collaboration of the Government with research, civil society and commerce?

4.1 The UK has developed one of the best models in the world for government, industry and wider stakeholders working in partnership to tackle the risks that are posed to the safety of children online. Industry self-regulation has proven to be a key enabler of innovative and effective ways to enhance child protection online.

4.2 One example of collaborative partnership is the UK Council for Child Internet Safety (UKCCIS), a group of more than 200 organisations drawn from across government, industry, law, academia and charity sectors that work in partnership to help keep children safe online. Five working groups focus on the topics of Filtering, Social Media, Education, Evidence, and Age Verification, and UKCCIS recently published advice for parents, schools and colleges, and social media providers to think about 'safety by design' and help keep children and young people safe online.[378]

4.3 The work of the Internet Watch Foundation (IWF)[379] is another example whose self-regulatory partnership approach is widely recognised as a model of good practice in combating the abuse of technology for the dissemination of criminal content. An independent self-regulatory body funded by the EU and the online industry, the IWF removes the illegal content at the source through its Notice and Takedown service. Industry takes its responsibilities in this area incredibly seriously and in 2015 the identified URLs hosted in the UK were removed within 5 days.[380]

4.4 Much online criminal activity is global in nature, and requires cross-industry, cross-government and cross-border collaboration. Launched in the UK in 2014 with the then UK Prime Minister David Cameron and representatives from over fifty countries, leading technology companies, law enforcement agencies, and charities, the WePROTECT Global Alliance is an international movement dedicated to national and global action to end the sexual exploitation of children online. The UK Government has lead the way in committing £50 million over five years to tackle violence against children globally, and the technology industry has pledged to continue fighting this abuse of the internet by developing new technology, tools and expertise.[381] As the UK prepares to leave the EU, techUK urges continued and strengthened engagement of the UK

---

378 https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis
379 https://www.iwf.org.uk/
380 https://www.iwf.org.uk/assets/media/annual-reports/IWF%202015%20Annual%20Report%20Final%20for%20web.pdf
381 https://www.gov.uk/government/news/tech-industry-fights-online-child-sexual-exploitation

with international networks to share best practice and enable greater coordination of child online protection.

4.5 Under the current timeline the UK may not exit the EU before the General Data Protection Regulation (GDPR) is due to come into force in May 2018, a point already highlighted by the Information Commissioner's Office.[382] techUK would note that the nature of the GDPR means it will impact the entire digital supply chain. Many business will have either customers or suppliers across the EU who will need to be GDPR compliant regardless of UK efforts. A recent survey showed that 63% of techUK members have operations across Europe and would have to comply with EU rules, regardless of any revisions to the UK's to data protection landscape.

4.6 Divergence of UK data protection laws from the EU may create increased regulatory space for innovation but would undermine the compliance needs of the digital supply chain increasing the risk of regulatory clash. Government has already begun preparations to implement the regulation and continued harmonisation of the UK-EU data protection landscape would harmonise citizens' rights while easing the regulatory burden on UK businesses.

4.7 In the first draft of Article 8 of the GDPR, it was proposed that 13 years old should be the lowest age of consent for personal data without an online provider having to get the consent of the child's parent or guardian. 13 years old has been the de facto age of most EU member states and internationally, the US Children's Online Privacy Protection Act[383] also specifies the age 13. A last minute amendment to the text resulted in member states having the option of specifying an age of consent between 13 and 16 with the implementation of a default age of 16 in May 2018 if national legislation is not introduced. techUK recommends that 13 years of age is adopted as the UK age of consent for these purposes, specified in legislation if necessary.

4.8 Prior to the adoption of new EU rules on the Open Internet (Regulation 2015/2120[384]), significant work was undertaken by UK Internet Service Providers to develop a set of tools to protect children from harmful content. The Broadband Stakeholder Group (BSG) developed in 2011 and 2012 a Code of Practice on traffic management practices and on the Open Internet together with Internet Service Providers, and the support of the wider industry, Government and Ofcom. The Codes include a set of commitments on how lawful content should be delivered to consumers and permissible traffic management practices- these include the blocking of websites as advised by the IWF, and the deployment of child protection tools.

4.9 The UK self-regulatory approach to the Open Internet had proven to be effective without the need for a formal legislative backstop. However following the adoption of EU Regulation 2015/2120, the BSG revised its Code of Practice as a form of good practice and to comply with the new EU rules. The new Code

382 https://iconewsblog.wordpress.com/2016/07/07/gdpr-still-relevant-for-the-uk/

383 https://www.ftc.gov/tips-advice/business-center/privacy-and-security/children%27s-privacy

384 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2015.310.01.0001.01.ENG&toc=OJ:L:2015:310:TOC

was published in June 2016 with the continued support of Government, Ofcom and wider industry.[385] The revised Code continues to include, as part of the list of permissible traffic management practices, the deployment of parental control filters and child protection tools, as well as a commitment to block websites as advised by the IWF. Although the Regulation does not specifically refer to these practices as permissible, the Code demonstrates that ISPs remain committed to ensure children are protected from harmful content.

4.10 Through the Digital Economy Bill, UK Government aims to establish a new law requiring age verification for commercial pornographic websites and applications containing still and moving images, and a new regulatory framework to underpin it.[386] Having begun the legislative process with first reading in House of Commons on the 5 July 2016, this will be taken forward in the next parliamentary session.

4.11 Industry looks forward to continuing collaborative partnerships to provide education and outreach and ensure that parents and children have the tools and knowledge to make smart and responsible choices online. This work can be further enabled by greater cross-government coordination to help tackle these multi-faceted social challenges. techUK stands ready to participate in and inform the House of Lords Select Committee discussion as it develops recommendations regarding how policies and practices might increase the value of the internet for children.

September 2016

385 http://www.broadbanduk.org/2016/06/08/bsg-publishes-new-open-internet-code-of-practice/

386 http://www.publications.parliament.uk/pa/bills/cbill/2016-2017/0045/cbill_2016-20170045_en_1.htm

Terrence Higgins Trust – written evidence (CHI0058)

Children and the internet is a big safeguarding issue for the Government. The Government states that 'Sex and relationships education (SRE) can provide the knowledge needed to tackle negative attitudes that lead to sexual harassment and violence'. The Government says they are committed to safeguarding, yet they are not educating children about safeguarding, both online and offline, adequately in every school, both primary and secondary. In 2015, a Cochrane review[387] concluded that 'Children who are taught about preventing sexual abuse are more likely than others to tell an adult if they had, or were actually experiencing sexual abuse.'

It needs to be made clear that safeguarding should be interwoven in the curriculum. Statutory Sex and Relationships Education (SRE) and Personal, Social, Health and Economic education (PSHE) play a vital role in ensuring that safeguarding requirements are met, however SRE and PSHE are only statutory in maintained secondary schools. Despite the previous Conservative Government's decision earlier this year that SRE and PSHE are not to be statutory, for safeguarding to be delivered effectively, SRE and PSHE need to be statutory in all schools, both primary and secondary.

The Parliamentary Education Select Committee Inquiry into SRE and PSHE concluded: "We accept the argument that statutory status is needed for PSHE, with relationships and sex education as a core part of it. In particular this will contribute to ensuring that appropriate curriculum time is devoted to the subject, to stimulating the demand for trained teachers, and to meeting safeguarding requirements" (Life Lessons, 2015).

However, the Government does not address the fact that the last Ofsted report which looked at SRE, in 2013 (PSHE: Not yet good enough)[388] showed that SRE was inadequate in 43% of secondary schools that teach it and that it is not taught at all in many schools. Although the Government states that PSHE is something that all schools are expected to teach, and SRE is something that must be taught in all maintained secondary schools (which make up a mere 40% of secondary schools), SRE does not have the same status as other subjects and this is problematic.

There is very clear evidence from Ofsted, local authorities and in a report published earlier this year by Terrence Higgins Trust (SRE: SShh…stop talking),[389] highlighting from young people themselves that SRE is inadequate or absent in many schools.

Current legislation does not mandate all schools, both primary and secondary, to teach SRE. Furthermore, the Government's policy is that more schools (both

---

387 http://www.cochrane.org/news/teaching-children-schools-about-sexual-abuse-may-help-them-report-abuse

388 https://www.gov.uk/government/publications/not-yet-good-enough-personal-social-health-and-economic-education

389 http://www.tht.org.uk/get-involved/Campaign/Our-campaigns/SRE

primary and secondary) should become academies. Yet academies have no statutory requirement to teach SRE. The Government has not provided any evidence to support their feeling that 'we believe that most secondary academies and many primary schools also teach [SRE]'. Terrence Higgins Trust's report (SRE: SShh…stop talking)[390] has revealed that young people surveyed thought SRE should be mandatory in all schools. Only then can we ensure all children and young people receive and ensure that standards are driven up as more resources, time and finances are given to the subject, ensuring that all children are adequately safeguarded, both on and offline.

The guidance commissioned by the Government to support the teaching of PSHE and SRE does not cover the breadth of the subjects. For example, the PSHE Association guidance published in 2015 on consent only applies to secondary schools, but primary school-aged children can be victims of sexual abuse. Furthermore, the Government has not provided any data to show that this guidance is being used in those schools that it is relevant to. The Government's own SRE guidance is in desperate need of updating as it is now 16 years old and much has happened during this time, both in terms of advances and access to technology but also in terms of the law around, for example, same-sex marriage. How can this out-of-date guidance actually do what the Government states it does: 'It also sets out that they should understand how the law applies to sexual relationships' when it was written long before the advent of smart phones and before same-sex marriage was introduced?

The Government has highlighted their talks with head teachers to produce an action plan for improving PSHE and SRE, there is still no plan, or timeline. To add insult to injury, the recommendation made by the Education Select Committee[391] in February 2015 to make PSHE and SRE statutory in all primary and secondary schools has been rejected by the Government. We are still awaiting the Government response to the recent report on Sexual Violence and Sexual Harassment in Schools[392] by the Women's and Equalities Select Committee in September 2016, which included several recommendations on the need for statutory PSHE and SRE in all schools. In July 2016, the **United Nations recommended that SRE becomes mandatory in UK schools**. This is part of the UNCRC verdict on the UK's child rights.[393]

The idea that computing is a place to learn responsible, respectful and secure use of technology is certainly not an acceptable substitute for good quality SRE. SRE, not computing, is where children and young people should learn about consent, abuse, safeguarding, gender, sexuality and relationships by teachers who have had the correct training and guidance. To make certain this happens SRE needs to be on the schools' timetable for all children and young people, like computing and other subjects are.

The Government is right in saying that SRE and PSHE need to be of high quality and not a 'tick box' approach. The best way to achieve high quality in any

390 *Ibid.*
391 http://www.publications.parliament.uk/pa/cm201415/cmselect/cmeduc/145/145.pdf
392 http://www.publications.parliament.uk/pa/cm201617/cmselect/cmwomeq/91/9102.htm
393 https://humanism.org.uk/wp-content/uploads/CRC_C_GBR_CO_5_24195_E.docx

subject is to make it a requirement in all schools. Following statutory status teacher training, resources, guidance and the option to become a specialist SRE teacher all ensue. There is no other way to drive up standards across all schools.

The Government must stop using delaying tactics and respond to the persistent calls from teachers, parents and health and child protection experts to make SRE a requirement in all schools. This is in addition to MPs including the Education Select Committee, the Women's and Equalities Select Committee, the Health Select Committee, the Home Affairs Select Committee and the Business Select Committee, and crucially from young people themselves. Good quality, age-appropriate, inclusive, SRE needs to be given to all children and young people, regardless of the type of school they attend or their sexuality so that they are all protected on and offline, and so that they are all prepared for life beyond the school gates.

23 November 2016

David Thewlis – written evidence (CHI0066)

1. I am making this submission as a concerned Christian, father and grandfather.

2. Prior to the General Election I 2015 the Conservatives committed to introducing measures to protect children from being able to access corrupt and damaging material, on-line.

3. The Government is to be commended for its efforts to put these measures in place and provide a world-wide lead in this matter.

4. I welcome the proposed introduction of robust Age Verification controls which are contained in the Digital Economy Bill, currently before Parliament.

5. The appointment of an Independent Regulator to oversee these restrictions, along with being given powers to require ISPs to block specific websites and issue targeted sanctions is right, essential and welcomed.

6. With computers and technology developing so rapidly and absorbing so much of our time and interest, it is vital that Government and indeed all in positions of responsibility, take action to protect children from accessing material which damages for life. I will continue to support every effort of the Government to this end.

7 December 2016

Three – written evidence (CHI0016)

1. This is Three's (Hutchison 3G UK Ltd) response to the House of Lords Select Committee on Communications' Call for Evidence on children and the internet. The Call for Evidence will help inform the Committee's approach as it scrutinises the work of Government in enabling children and young people to safely take advantages of the opportunities of being online. Three is committed to making mobile better for all our customers; as such we welcome the opportunity to respond.

2. Three is the UK's challenger mobile operator. Since we launched in 2003 we have focused on ensuring that our customers are able to make the most of their devices through market-leading propositions such 4G at-no-extra-cost and Feel at Home, enabling our customers to call, text and use their data abroad now in 42 destinations from September, using the same allowances they do at home.

3. Three is already actively involved in supporting parents, teachers and young people to stay safe online. Through our 'Discovery. With Three.' locations in Maidenhead, Swansea and Islington - in addition to hundreds of free sessions run in our stores across the UK - we have supported more than 7,000 adults and young people in developing their digital skills, in a friendly and helpful learning environment.[394] This includes advice on how to enable children to make the most of the internet while also being able to browse confidently and safely. In Swansea we are trialling working with Communities First to deliver Online Safety for Parents sessions. Crucially this resource is available to all mobile users, not just Three customers.

4. As the Committee will be aware, access to the internet is increasingly an essential part of our daily lives. Recent Ofcom research has found over a third of adults (34%) check their mobile device within five minutes of waking up every morning.[395] As the Call for Evidence notes, this is increasingly the case for children as well. 42% of children aged 5-15 have a mobile device, with 35% owning an internet connected smartphone.[396]

5. This rapid uptake of devices for children reflects the benefits of connectivity to them and their families. It helps children to stay safe and better connected to their parents, as well as opening up opportunities for enhanced digital participation and learning. However the risks of children accessing inappropriate content online are well documented. The challenge for policymakers and industry is to ensure that children and families are able to enjoy these opportunities safely and responsibly.

---

394 Please visit http://www.three.co.uk/discovery for more information

395 Ofcom, Communications Markets Report, 2015, http://stakeholders.ofcom.org.uk/binaries/research/cmr/cmr15/CMR_UK_2015.pdf

396 Ofcom research – most recent 'Children and Parents: Media Use and Attitudes Report' Nov 2015 http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/children-parents-nov-15/childrens_parents_nov2015.pdf pg. 37

Working together to provide parents with the tools to keep their children safe online.

6. We recognise that Communications Providers (CPs) have a critical role to play to keep children safe online. The mobile industry has helped lead the way on this. Our network has filters that can be applied to exclude adult content targeted at customers over the age of 18 which have been developed in line with the content self-regulation code of practice alongside other mobile operators, and is based on an independent framework produced by the British Board of Film Classification (BBFC).

7. In addition to our existing default-on filtering for our Pay As You Go mobile phone customers, in 2015 we supported the UK Government's commitment to child safety by introducing default-on filtering to all new Pay Monthly customers as well. To switch off these filters on Three's mobile services requires an age-verified bill payer to make an active choice to do so.

8. Content filtering represents a vital tool in supporting parents, teachers and guardians to keep children safe online, but any effective strategy will require active and meaningful engagement with this group, rather than technology centred solutions alone, such as age verification and content filtering. Filtering tools have their technical limitations, for example they will not cover the use of handsets accessing the internet over a Wi-Fi connection – doing so means that the traffic is no longer being carried across our network, and that the content received by the end user is no longer subject to the mobile networks filtering practices.

9. This is why despite the availability of filters on a default-on basis, nearly one in five parents of 5 to 10-year-olds say their children have accessed inappropriate content online in the last year. Indeed only 43% of parents use parental controls to restrict what their children can access.[397] Children increasingly face risks to being online that simply cannot be picked up by these methods, for example cyberbullying by their peers on social networks.

10. Much of the research in this area suggests that adults feel disempowered in trying to help children stay safe online. Almost a fifth (19%) of parents are worried their lack of tech skills could be putting their children at risk – 44% say their children's expertise outstrips their own.[398] Government must adopt a strategy that empowers the parents, teachers, guardians and children alike - viewing filtering, age verification, and other technological methods as supporting tools for staying safe online, in addition to a critical skillset that prepares children and adults to deal with a wider variety of situations.

---

397 http://home.bt.com/tech-gadgets/internet/safer-internet-day-2015-bt-poll-shows-child-internet-safety-concern-11363959864051

398 https://www.uswitch.com/media-centre/2016/01/parents-grip-slipping-on-youngest-children-as-four-year-olds-surf-internet-unsupervised/

Government's role in supporting adults and children with the skills to stay safe online.

11. While Three continues to support parents, teachers, guardians and children with developing the right skills and tools to keep safe online, the Committee must also assess what role Government can take achieving this, and whether in some key respects Government might be better placed to support than the communications providers.

12. Education will be a critical space for this, and schools represent an opportunity for Government to support all children of all backgrounds to develop the skills they need to get online safely – not least as children increasingly are encouraged to access the internet as part of their learning inside and outside of school. With coding now forming a key part of the curriculum there is an opportunity for schools to address issues relating to safety and security from a primary school age. Enabling children to have the technical tools and social skills that they need to empower them in a number of situations that would not be picked up by filtering, such as cyberbullying, will be essential.

13. Similarly the Government can also have a role in encouraging parents, teachers and guardians to be aware and actively engage with the resources available to them. This includes support from their communications providers, but also resources from the BBFC, Internet Watch Foundation and many other internet safety dedicated charities.

14. The critical change needed in the Government's approach though must be to recognise the importance of technical solutions as a supporting tool for *empowered* parents, teachers and guardians, rather than a stand-alone solution.

Conclusion

15. Ensuring that children can enjoy the benefits of being online both safely and responsibly remains a critical issue for parents, teachers, guardians, industry and the Government. Three continues to support the wider objective of policymakers in this regard.

16. While industry has been active in providing parents, teachers and guardians with the tools to support safe browsing, the emphasis must also be on their skills and confidence. Tools such as content filtering should complement their digital and social skills, rather than being an alternative or replacements for them. This will require ambition from the Government, and crucially a change in terms of how it thinks about the challenge of keeping all children safe online.

24 August 2016

Virgin Media – written evidence (CHI0052)

Response to the Lords Communications Committee Inquiry into Children and the Internet

Introduction

1. Virgin Media welcomes the Committee's inquiry into Children and the Internet, and the opportunity to contribute towards its findings. This inquiry follows continued parliamentary interest in the role of the internet in children's lives. Indeed in the last decade successive independent government-commissioned reviews have explored the impact of the internet on children, covering issues such as commercialisation and sexualisation (Bailey 2011), to safety (Byron 2008) and child development (Buckingham 2009). Each of these inquiries has made recommendations which the industry, in its widest sense, has worked to meet.

2. Each iteration of Ofcom's annual *Adults' Media Use and Attitudes Report*[399] has demonstrated strong and sustained uptake of digital devices and services amongst the UK population – driven not least by high quality entertainment; plurality of news media; the ability to communicate across a range of platforms; and a key consumer interest – to make savings on purchases. These are all direct consumer benefits. The internet provides huge opportunities for children and young people, not least in education, self-expression and discovery.

3. Alongside myriad opportunities afforded by the internet, there are of course risks to be balanced. Whist it may be understandable that discourse related to children and the internet has tended to focus on risk, it is important to recognise that in the debate, the term 'online safety' has commonly been used as a catch-all for a very broad and disparate range of risks. It is unhelpful to conflate these risks, and to discuss their causes and their treatment as one and the same. They are not. Therefore, for the purpose of this submission, when we talk about 'online harm' or 'risks' we are predominantly referring to content risks, rather than contact risks or conduct risks. Focussing on one risk profile over another may not be effective – one solution to a risk profile may solve a problem, but may not be appropriate for another, and in extreme instances could be counterproductive.

4. Virgin Media's, as a responsible ISP, actively encourages vigilance by educating our customers about where risks lie. Further, we seek to support and enable our customers to make decisions and implement solutions that are right for their households to tackle those risks. Our approach to is twofold, we:

---

399 Most recent version can be accessed at: http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/adults-literacy-2016/2016-Adults-media-use-and-attitudes.pdf

- Encourage parents to implement parental controls by providing free, easily installed software and presenting every customer with an active choice;
- Educate and build awareness of online risk amongst our customers to allow them to adopt holistic approaches to digital parenting.

5. It is the latter approach which we believe needs to be given further and careful consideration by policy makers. Advice to parents in response to content risks has tended to centre on the amount of time that children spend with screens, with recommendations to limit time, or to remove devices. These proposed solutions don't necessarily deal with the problems that children might encounter online, nor do they acknowledge that the internet is blended in our day-to-day lives. Encouragingly, there has been a recent step change in the discussion. In "Families and screen time"[400] – the most recent Policy Brief from the *Media Policy Project* – Blum-Ross and Livingstone provide an overview of the current advice to children and parents. They conclude that (1) it is time to recognise that the internet is 'no longer an optional extra' that can be treated in isolation of other activities; (2) the dominant messages to parents about limiting and controlling screen time is unhelpful; and (3) that a focus on restrictions 'leaves parents unsupported in finding opportunities for children and parents to learn, connect and create together".

6. New ways to support parents must be found and Virgin Media believes an approach which needs further exploration is how to build resilience of children online. Whilst the concept of building children's online resilience was promoted within Tanya Byron's review *Safer Children in a Digital World* (2008)[401] further academic discourse related to *how* to equip children to deal with exposure to harmful or inappropriate content had been lacking. For this reason, in 2014 Virgin Media, in partnership with the Parentzone, commissioned the Oxford Internet Institute to further examine the concept of child resilience online. The report *A shared responsibility building children's online resilience* [402] recognised that parents cannot monitor their children at all times, and therefore different strategies need to be put in place to help children navigate the online world and recognise risks and how to deal with them.

7. The Oxford Internet Institute study had three very positive findings:

   a) Resilient children get more out of the online world. Young people that make their own judgments about their internet use, and are able to analyse risk, are more likely to seek out positive opportunities online. As

---

400 Blum-Ross, A; Livingstone, S (2016) "Families and screen time: Current advice and emerging research" Media Policy Project, LSE. Available at: http://eprints.lse.ac.uk/66927/1/Policy%20Brief%2017-%20Families%20%20Screen%20Time.pdf

401 Byron, T (2008) "Safer Children in a Digital World" (2008). Available at: http://webarchive.nationalarchives.gov.uk/20100407120701/http://dcsf.gov.uk/byronreview/actionplan/index.shtml

402 Przybylski, A.K.; Mishkin, A.; Shotbolt, V.; CEO, Linington, S.; (2014) "A shared responsibility building children's online resilience" Oxford Internet Institute. Available at: https://parentzone.org.uk/system/files/attachments/VM%20Resilience%20Report_1.pdf

such, it is valid that government policy should be geared towards building resilience.

b) Supportive and enabling parenting does more to foster resilience than parents who restrict or monitor internet use. In fact, the research indicated that restricting internet access can have a deleterious effect on building resilience.

c) Building digital skills contributes to resilience. The more a young person understands about the digital world, the better equipped they are to deal with the risks it throws up.

8. The research indicated that creating the most positive and safest environment for child online requires a more lateral policy framework – one that views the need to build digital skills through the lens of child internet safety, and one gives parents the confidence to enable their children to explore the internet.

Response to specific inquiry questions
Q. What are the technical challenges for introducing greater controls on internet usage by children?

9. It should be noted that parental controls are available. Each of the four leading UK ISPs have introduced parental controls covering home, mobile and public WiFi. These controls provide parents with the choice to mitigate the risk of their children encountering potentially inappropriate content online. Each of the four leading ISPs – including Virgin Media – dedicates significant resource to product development of these tools, and to marketing and customer activity in order to ensure that our customers are aware of, and make a choice on, whether to activate free network level parental controls.

10. Virgin Media introduced an 'active choice' at the point of installation for all new customers in 2014. By 2015, we extended an 'active choice' to c.95% of our existing broadband customers. This included multiple targeted communications – 'pop-up' messages and emails – to customers that had yet to make an active choice. As a result of this activity, Virgin Media's activation rates amongst new and existing customers have become increasingly predictable, indicating that product awareness and demand has reached a level of maturity. One profound implication of greater levels of control is the risk that it can undermine the active choice made by households.

11. We empower our customers by providing them with the ability to dial up or dial down the level of control should they choose. We provide a number of these tools:

- Customers can choose to 'whitelist' sites, or 'blacklist' sites beyond the scope of our own filters.
- We provide time of day restrictions, to enable customers to implement filters at their own preference, different times of the day.

- Over-blocking and under-blocking mechanisms allow parents to escalate specific examples of inaccurate site classifications – in the last eighteen months we have seen few under blocking cases.

12. ISPs have long made clear that filtering is not a magic bullet to children encountering inappropriate content online. In what is a potentially very wide ranging spectrum of what can be considered 'harmful' there can be significant challenges in identifying what should or not be in scope – i.e. particularly with sites with User Generated Content – which filters may not pick up on. Further for children of different ages, or developmental stages, there should be an expectation that what is considered harmful differs and therefore a blanket approach can't be applied. Indeed in our own research, parents told us that they do not want a blanket approach.

13. Whilst technological solutions may be available, it must be understood that technology can be a blunt instrument, and that it cannot necessarily appreciate context. It is for this reason that we invest in teams to monitor and evaluate the efficacy of these tools and make decisions accordingly. It is for these reasons that industry has continuously asked policy makers to appreciate that technological solutions are not always the answer and to instead consider a wider, rounded approach which includes consumer awareness and education.

14. *Virgin Media* believes *greater consideration should be given to meeting Byron's recommendation to build children's resilience to help them to identify risk, navigate risk, and make informed and safe decisions as a result.*

Q. Who currently informs parents of risks?
What is the role for commercial organisations to teach e-safety to parents?
How could parents be better informed about risks?

15. There are various ways that parents today are informed about risk and opportunities for their children's use of the internet. These are undertaken by a wide range of civic organisations, commercial companies, regulators and educational establishments.

16. Virgin Media supports a range of educational and charitable initiatives with the purpose of helping parents to navigate the online world, and to help their children in a positive and informed way. One of the main external initiatives which we help to resource is Internet Matters. Internet Matters[403] was set up by ISPs in response to a concern that there needed to be a hub for information for parents about online controls. Internet Matters is funded by significant industry investment and tens of millions of annual marketing resource. More recently Virgin Media's Chief Executive, Tom Mockridge, joined The Duke of Cambridge's Royal Foundation Taskforce on the Prevention of Cyberbullying. In addition we routinely work with dedicated children's and parenting organisations like Childnet, Parentzone to ensure

403 Access at: https://www.internetmatters.org/

that information is spread as widely as possible and to extend the reach of support and guidance, in a range of contexts where parents might expect to find information available to them.

17. As well as supporting external initiatives, Virgin Media also invests in providing resources for parents and guardians on our own site. Our dedicated resource "Switched On Families" [404] is available to all, and focuses on supporting our customers to make decisions to help keep children in their household safe online. Switched On Families provides tailored advice which is suitable for different age groups, and across a range of online issues.

18. *Virgin Media* believes *it is important to retain a system where parents and guardians can access support and information from a range of different sources, in the context where they would want or expect to receive it.*

Q. What voluntary measures have already been put in place by providers of content to protect children? Are these sufficient? If not, what more could be done? Are company guidelines about child safety and rights accessible to parents and other users?

19. Virgin Media, as an ISP governed by the EU Telecommunications Framework and E-Commerce Directive, has no regulated responsibility to block consumer access to any content. However we exercise responsibilities to help create a safe environment for internet users. As outlined earlier in this response, Virgin Media provides active choice controls for all of our users. Any adult who signs up to use Virgin Media services must make a decision about whether or not to take up our offer of filters on behalf of the rest of their household.

20. Of course widespread adoption of a range of devices means that the idea of the internet being confined to a computer in the family living room alone is redundant. Virgin Media is signatory to the 2003 IMCB Code of Conduct governing mobile internet access, which requires that all mobile operators put in place default filters on adult content across mobile devices. Adult users must request to have the filters removed before being able to access adult content.

21. Additionally, in 2013, Virgin Media worked with UKCCIS to develop a statement on filtering across public WiFi, which commits all providers to apply default filtering of pornography material on public WiFi connections, unless the customer specifically requests otherwise.

22. Members of the committee should be aware that the status quo regarding filters is potentially at risk, as a result of recently published BEREC Guidelines. Our key concern relates to Article 3(3) of Regulation (EU) 2015/2120 (laying down measures concerning open internet access) may prevent us from continuing to provide default filtering of legal pornographic material in the manner described. Virgin Media would welcome clarification

404 Access at: http://keepup.virginmedia.com/switchedonfamilies

from the government on in-home filters as well as mobile and Public WiFi connections. Under Article 10(3) of the Regulation, Member States may maintain until 31 December 2016 national measures, including self-regulatory schemes, in place before 29 November 2015 that do not comply with Article 3(2) or (3). Member States concerned had to notify those measures to the Commission by 30 April 2016. We understand that government did notify parental controls measures to the Commission but we are unclear what exactly was notified or to what extent we will be permitted to continue filtering adult content after 31 December 2016.

23. Finally, Virgin Media alongside other leading ISOs and Mobile Network Operators (MNOs), is a founding member and funder of the Internet Watch Foundation (IWF), whose mission includes the identification and removal of child abuse imagery from the internet. The collaborative approach between the IWF and industry is truly world leading and has resulted in the near eradication of UK produced child abuse imagery. It has established international collaboration arrangements with many territories but a key challenge remains tackling the production and dissemination of child abuse imagery from non-cooperative countries.

Q. What are the regulatory frameworks in different media? Is current legislation adequate in the area of child protection online? Is the law routinely enforced across different media? What, if any, are the gaps? What impact does the legislation and regulation have on the way children and young people experience and use the internet? Should there be a more consistent approach?

24. An often repeated falsehood is that the internet is an unregulated environment, and that as a result it is unsafe for children. Just as our environment is regulated offline, there are numerous pieces of regulation which relate specifically to online. In addition to the legal framework, there is self-regulation, and wider industry and third sector-led initiatives, which taken together provide part of an ecology of solutions for children's experience of the internet.

September 2016

Virgin Media – supplementary written evidence (CHI0059)

During our workshop on the activity Virgin Media undertakes on online child safety, there was a discussion about whether 'default on' for filtering is better than the active choice solution offered by the majority of large ISPs for home broadband. I thought it might be helpful to set out why Virgin Media's policy is to implement active choice, and why we do not think that default on is in the interests of child safety.

At the outset it's important to note that not all of our customers will have children present within their household – it should be expected that in the vast majority of cases a filtering solution will not be desirable to these users. Where there are children present in a household, it doesn't necessarily follow that filters will always be appropriate, for example for toddlers who have limited access to technology, though this will of course change with time.

Irrespective we ask *all* of our customers to make a decision – an active choice – about whether or not they wish to use filters at the point at which they set up our service. We provide new users with written materials about filters and our *Switched on Families*[405] resources, and our technician who sets up the service will talk the user (who must be an account holder over the age of 18) through the settings and what they mean.

Active choice is important because it takes customers on a journey, and:

a. **requires users to make a considered decision about whether filtering is the right approach for their household.**

   Active choice forces a user to make a decision either way, and removes their ability to be passive. Instead they must take responsibility for their actions and become a decision maker. If the need for filters changes at that point, they are informed that they are able to switch these on or off at any time.

b. **provides a point of education, and prompts further considerations in the user.**

   Once a decision has been taken to switch filters on or off, the user is directed to make further decisions about a range of further controls. We provide further granular controls because different households may have a range of needs, and these needs may be complex, i.e. children at different ages and levels of maturity requiring different levels of control. Our controls, beyond basic filters relate to further types of content; time specific filters; and give households the option to whitelist or blacklist further sites. Choice is important because a one-size fits all approach may frustrate users, and drive people to turn them off.

405 http://keepup.virginmedia.com/switchedonfamilies

This user journey, with consumer education at its heart, is especially important because filters are not a perfect solution. Filters cannot contend with the diverse range of risks which a child may encounter online. While filters are an aid to helping households, they are a means to an end, but not an end in themselves. They should not be considered as such, and are certainly not marketed as such by Virgin Media.

In this context, default on becomes a worrying proposal. In the debate between default on, and active choice, there are parallels to public policy debates about consent and the online environment. The Article 29 Working Party (made up on national European Data Protection Authorities), has described active choice as:

- Informed
- Prior
- Freely given
- Without limitation

Indeed the Article 29 Working Party went on to say in an opinion on consent and active choice in relation to another policy debate, that 'absence of behaviour cannot be regarded as valid consent.' By extension, when it comes to filters, a default on solution removes the point of decision making, it means that consumers are not necessarily informed of potential risks because they less likely to be cognisant of what filters do, or of their limitations. This means that rather than a household being protected by filters, instead they are potentially in a more vulnerable position. A default on solution cannot be considered as a kind of safety net for families.

As we said in our written evidence: filters cannot contend with the myriad risks that children will undoubtedly encounter online, and therefore there is a need to help them to learn to identify, and navigate risks. Part of that starts with parents and guardians understanding what tools they have in the home. Alongside the promotion of parental education resources through our initiative *Switched on Families,* and through other connected industry wide initiatives like Internet Matters, we also promote the concept of building resilience amongst children and young people, to equip them to become informed digital citizens. We noted from various oral evidence sessions that there is a growing call for building childhood resilience.

Members will be aware that there is currently a debate taking place in the Commons about how to limit children's exposure to pornographic content online, and the provisions in the Digital Economy Bill to introduce age verification for commercial pornographic sites. This debate has largely focussed on carving out a role for ISPs as a tool for the regulator, despite evidence from the Government's consultative exercise clearly indicating that site blocking is not a proportionate response to the issue.[406] We have supported the Government's proposal to introduce a range of sanctions for sites which do not comply with the requirements in the Bill, including the 'Follow the money' approach through ancillary service providers like advertisers and payment card processors. The UK

406 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/500701/Report_of_DCMS_Expert_Panel__Autumn_2015__FINAL_.pdf

has led the way in rolling out this approach in response to Intellectual Property Crime online, and it has proven to be so effective that the European Commission recently announced its intention to adopt a similar approach across Europe.[407]

The Government has brought forward an amendment to compel ISPs to site block on notification by the Regulator. The decision to include ISPs within the scope of the Bill and to compel ISPs to site block on notification from the BBFC is without precedent, and carries risks. The Bill does not fully acknowledge the technical limitations of site blocking, and our concern is that we would be held liable for any technical failure which we could not reasonably control. The Bill as currently stands does not allow for these known limitations.
The UK sets an example internationally in how our media and wider content is regulated. It is therefore imperative that in bringing forward this legislation the Government is alert to the need for robust checks and balances. We must ensure that the scope of this amendment does not extend beyond what is intended in the Bill and therefore it is imperative that the Bill has in place:

a) a stronger oversight role for the Secretary of State than the Government currently proposes – the Bill currently stipulates that the Secretary of State is 'informed' of sites to be blocked
b) on-going scrutiny of the process, and for annual review to look at whether the policy objective is being met
c) a clear process, which ensures any role for ISPs is a backstop mechanism after all other sanctions are exhausted, as site blocking is the least proportionate response to the issue. The regulator should make best endeavours to encourage sites to comply with age verification before considering site blocking. There is a risk that unless this is stipulated on the face of the Bill, this could become the Regulator's first choice of sanction.

I do hope this clarifies our position for you.

28 November 2016

407 https://ec.europa.eu/commission/2014-2019/ansip/announcements/speech-vice-president-ansip-ceipieuropean-audiovisual-observatory-event-copyright-enforcement-online_en

Vodafone UK – written evidence (CHI0023)

Children and the Internet

Introduction

Just over thirty years ago, Vodafone started the mobile phone digital revolution by making the very first mobile phone call in the UK. We remain convinced that our technology can truly transform people's lives. We believe that all British citizens and businesses should enjoy the benefits of internet connectivity at home, at work and while on the move.
But we also recognise that with the opportunities that access to the internet provides there are threats and challenges that need to be navigated by us all. Vodafone is committed to helping UK families, including children and young people, to develop the skills and resilience they need to take advantage of the digital world and lead healthy digital lifestyles.
There are well-known threats such as inappropriate or illegal material but it is also becoming clear that navigating through the digital world brings broader challenges too.

In particular there are challenges for parents in how to have appropriate conversations in their families in a context in which their children may have more digital expertise than they do themselves.

Increasingly our focus is on supporting families and young people to develop the skills they need to be safe and digitally resilient online. Historically there has been a lot of focus on helping parents understand how to keep their children safe including how to use technology like parental controls to accomplish this. This is still very important but we need to recognise the reality that young people will continue to live an increasingly digital life whereas in the past there was a more noticeable divide between the physical and virtual world.

This being the case, we need to help young people cope with the always on digital world they live in by helping them develop the skills they need to be digitally resilient. To do this we believe that there is an opportunity for Government to work with schools to enhance the way children learn about digital resilience through peer-to-peer lessons. Even one peer-to-peer session would be a step forward for the way children engage with this vital issue.

Protecting children from inappropriate material

Before discussing those broader challenges, it is important to state clearly that Vodafone has always taken the issue of protecting children and young people from inappropriate online material very seriously and we have been closely involved in work in this area for many years. Like other fixed and mobile operators, we have robust controls available to block sites (including pornographic sites) in accordance with BBFC guidelines. This includes our mobile content bar which requires customers to prove they are over 18 in order

to remove it. We also use the Internet Watch Foundation (IWF) list to block access to child abuse material.

In addition to the technological provisions in place, we are actively engaged in the policy debate on these issues. We are Executive Board members of the UK Council for Child Internet Safety and are on the Funding Council of the Internet Watch Foundation. We also signed the #WePROTECT Statement of Action in December 2014.

Impact of digital on social interaction

It is clear that one unfortunate downside of access to the internet is the potential for anti-social behaviour and illegal activity ranging for cyber-bullying to an increase in child sexual exploitation.

New figures from YouGov commissioned by the Diana Award as part of the Stand up to Bullying campaign supported by the Vodafone Foundation suggest 64% of the population believe that bullying is widespread with 81% reporting bullying as commonplace in schools. A large proportion of this will include virtual as well as physical bullying and sometimes will be entirely online. Vodafone's own research suggested that 68% of the young people we polled knew of someone who had been cyberbullied.

Current policy environment

Historically the focus by Government has been to work with the industry to help parents understand how to keep their children safe online using education programmes run by third parties (often industry-backed) coupled with support for parental controls delivered to devices.

The general approach has been to encourage effective self-regulation but Government has also looked to legislation as well and is currently considering how to legislate to fulfil a manifesto commitment to introduce age verification for online pornographic material.

Current Vodafone engagement

With support from the Vodafone Foundation, we are supporting families and young people to enable them to develop the skills they need to be safe and digitally resilient online.

Digital Parenting Magazine

A key part of our work has been helping parents understand how to keep their children safe using the Digital Parenting Magazine as a way of providing parents with a resource they can use to help them decide how to deal with what is now an important area of parenting. The fifth edition will be published in the autumn and we will print one million copies which will be available on request from Parent Zone who are the voluntary sector partner on this project as well as providing it online as well. It is largely requested by schools and other local public sector organisations.

Stand UP to Bullying campaign

Vodafone is supporting the Diana Award Stand Up to Bullying campaign. The aim of the campaign is for individuals, local communities, schools and business to stand up to bullying by registering support while also providing briefing materials to design to help tackle bullying. We are also members of the Duke of Cambridge's Cyberbullying Taskforce.

Be Strong programme

We have also been working with the Diana Award to help build teens' emotional resilience across various areas of online safety, starting with cyberbullying to help them develop the ability to cope with anything that comes up in their digital lives. We worked in partnership with the Diana Award to create these resources, which use a peer-to-peer format: each module provides all the resources needed for teachers to train a small group of students (who we call the 'Tech Trainers') to deliver short lessons to other students in the school, including lesson plans and videos. We have designed the programme to be flexible, but recommend that training be delivered to students who are 11-13 by Tech Trainers who are 13 and above. The modules include *Coding & Creativity*, *Peer Pressure Online* and *Selfies & Self Esteem*.

This peer-to-peer format is based on the highly successful methods used by the Diana Award Anti-Bullying Ambassador Programme, which provides anti-bullying training to schools and youth organisations.

We have also created a suite of #BeStrong 'support emojis' to help young people convey compassion and support to friends who are being bullied online. The emojis focus on awareness and engagement. The intention was to encourage young people to support each other - as peer to peer support has been proven to be the most successful intervention in a bullying situation. The emojis were chosen by the teens via the survey, with a set of emojis selected as the favourites. There has been a reach of over 150m across social and online media and approaching 1m views of YouTubers' videos about the emojis).

Scout Partnership and Digital Manifesto.

Through our partnership with the Scouts, we will be using our resources to help them build digital resilience and confidence within the Scouts themselves and the wider community. A key part of this programme will involve supporting the Digital Citizen and Digital Maker badges to help young people involved in the Scouting Movement to improve their digital skills and help their communities to do likewise

Our plan is to make digital resilience a key part of this programme with the aim to encourage Scout groups to build digital resilience.

Going forward

Vodafone will continue to have measures in place to protect children as well as engaging in wider policy and regulatory discussions with Government and

others. We also believe there are some areas in which there is an opportunity for Government to respond to the evolving challenges posed by the digital age.

Embedding digital resilience

Since 2015, schools have been encouraged to put in place strengthened measures to protect children from harm online, including cyber bullying, pornography and the risk of radicalisation and most schools teach some form of online safety
However, there is not a specific requirement for a peer to peer digital resilience session with the current focus on teachers/adults in schools understanding the risks and teaching pupils.

We believe there is an opportunity to go further and use the shared experiences of children themselves to better embed digital resilience. We believe that we need to give digital resilience more focus and the most obvious way to do this is for schools to be given the resources to set up peer to peer digital resilience lessons. For example, if schools had at least one peer-to-peer digital resilience session it would be a step forward.

Clearly schools are under a lot of pressure and we recognise that asking for them to do more is difficult which is why we think that encouraging and resourcing them to bring in experts to deliver these sessions if they don't have the necessary expertise in-school may be the way forward. There are a number of high quality providers in the voluntary sector that could help deliver such a programme.

August 2016

Vodafone and Sky – oral evidence (QQ 61-71)

Transcript to be found under Sky

The Wild Network – written evidence (CHI0019)

Summary

The evidence is abundant, clear and growing exponentially: 'Wild Time' – what we call the time that children spend roaming free and playing wild – supports countless aspects of their physical, mental, cognitive, and social wellbeing as well as the development of personal and community resilience. Our contribution to the Select Committee concerns the indirect impact that screen-based entertainment (including the Internet) has in terms of *displacing* children's opportunities for Wild Time.

About The Wild Network

The Wild Network was founded off the back of the 2012 Natural Childhood Report (Moss, 2012). This concluded that there are several complicated and inter-linked barriers preventing children from spending enough time outside in nature and that this is having profound impacts on their wellbeing. One of those barriers is screen-based entertainment. Over the past four years, The Wild Network has developed into a unique organisation made up of partners from multiple sectors, supported by a growing community of mums, dads, teachers and people in communities across the world. Partners include the National Trust, the RSPB, the Woodland Trust and the Wildlife Trusts and some commercial interests, such as Unilever. Our mission is to grow what we call 'Wild Time'.

Statement

There has been a significant decline in the amount of Wild Time that children get. (A recent report by Unilever concluded that UK children have less time outdoors than a high-security prisoner.) This is linked – sometimes directly –to a number of profound impacts on children's health and wellbeing, as well as on their relationship with nature and their eco-literacy.

It's not clear whether children go outside less because screen-based entertainment is simply more attractive, or whether children spend more time on screens because they are kept indoors. This is what Richard Louv, who hatched the phrase 'nature deficit disorder', refers to as 'well-meaning, protective house arrest.' Parents and carers prevent children from playing and roaming outside (eg fear of traffic, fear of strangers). It is probably a combination of both.

We hear every day from our community of parents and teachers. Few of them would deny that digital skills are needed, but they tell us repeatedly that THE really big issue is how they can find screen time:wild time balance and this is the question that we continue explore with our community. The pace of change, and opportunity, afforded by the internet has been astonishing, faster than anyone can have predicted. This continuous rapid change has left families, communities and schools to play catch up on how they manage and assimilate ever changing digital technologies on their lives. Amongst our community members there is an

urgent need for deeper understanding about how we might understand the role that the internet has had in displacing other activities, like wild time. We ask the select committee to consider how we can support families, communities and schools to find solutions that take advantage of all that the internet offers whilst balancing this with real play and learning, outdoors - wild time.

Evidence

All the indicators of childhood wellbeing, from myopia, obesity and ability to concentrate to anxiety, loss of motor skills and disconnection with nature, point towards a worsening situation. This is bad not just for people, but for the environment: evidence shows that if our children do not get outdoors in nature, they are unlikely to care enough about it to protect it as adults.

Here is a flavour of the research that informs our own work that specifically relate to children. We have many more about the benefits of nature connection in general.

1. PUBLISHED PAPERS

Health and Wellbeing

- Nature areas can contribute to children's development – notably to their concentration, motor skills, self-esteem, and emotion regulation. Report from the IEEP on The Health and Social Benefits of Nature and Biodiversity Protection.[408]

- For children, greenspaces are an important environmental influence on physical activity and emotional wellbeing.[409]

- Connecting families to nature may positively influence physical activity (i.e., active playtime) and healthy eating routines in children aged 2 to 4.[410]

- Farm dirt is good for children's health[411]

- Worldwide research on health benefits of natural environments, esp in urban environments: neurophysiology, green exercise, community gardens, sustainability, walkability, screen time, children.[412]

---

408 ten Brink, P. et al, 2016. Health and Social Benefits of Nature - Final Report Executive Summary. IEEP.

409 Ward et al 2016. The impact of children's exposure to greenspace on physical activity, cognitive development, emotional wellbeing, and ability to appraise risk. Health and Place 40: 44-50.

410 Sobko, T., Tse, M., Kaplan, M., 2016. A randomized controlled trial for families with preschool children - promoting healthy eating and active playtime by connecting to nature. BMC Public Health 16.

411 Schuijs, Martijn J., et al. "Farm dust and endotoxin protect against allergy through A20 induction in lung epithelial cells." *Science* 349.6252 (2015): 1106-1110. http://www.childrenandnature.org/2015/09/29/study-proves-farm-dirt-is-beneficial-for-childrens-health/ http://www.vnews.com/Archives/2015/09/HealthAllergies-ah-vn-090715

- UNICEF overview of child wellbeing in rich countries.[413]
- Forest School offers enough physical exercise for health and wellbeing.[414]
- Children in the Outdoors – a good literature review.[415]
- Children living in greener neighborhoods had lower BMI, probably because of physical activity or time spent outdoors.[416]

Cognitive Restoration (Attention) / Emotional Restoration (Stress)

- Children responded faster on an attention task after a nature walk than an urban walk.[417]
- The more unstructured time children had while out of school, the better their executive functioning (cognitive skills that support planning and decision-making, memory and academic achievement).[418]
- Forest school can help control anger in young people at risk[419]
- Children with Attention Deficits Concentrate Better after Walk in the Park.[420]
- Preschool children benefit from restorative effects of outdoor spaces. [421]
- Green outdoor settings reduce ADHD symptoms in children.[422]

---

412 Africa, J, and et al. 2014, The Natural Environments Initiative: Illustrative Review and Workshop Statement. Center for Health and the Global Environment: Harvard School of Public Health. http://www.chgeharvard.org/sites/default/files/resources/Paper-NaturalEnvironmentsInitiative_0.pdf.

413 UNICEF Office of Research 2013. 'Child Well-being in Rich Countries: A comparative overview', Innocenti Report Card 11, UNICEF Office of Research, Florence. http://www.unicef-irc.org/publications/pdf/rc11_eng.pdf

414 Lovell, R. (2009). *Physical Activity at Forest School.* London: Forestry Commission.

415 Muñoz. S-A; 2009 Sustainable Development Research Centre Children in the Outdoors: A literature review http://www.educationscotland.gov.uk/images/Children%20in%20the%20outdoors%20literature%20review_tcm4-597028.pdf

416 Bell, J., J. Wilson and G. Liu (2008). Neighborhood Greenness and 2-Year Changes in Body Mass Index of Children and Youth. *American Journal of Preventative Medicine* 35(6): 547–553.

417 Schutte, A.R., Torquati, J.C., Beattie, H.L., 2015. Impact of Urban Nature on Executive Functioning in Early and Middle Childhood. *Environment and Behavior*

418 Barker, J. E., Semenov, A. D., Michaelson, L., Provan, L. S., Snyder, H. R., & Munakata, Y. (2014). Less-structured time in children's daily lives predicts self-directed executive functioning. Frontiers in psychology, 5

419 Roe, J. (2009). Forest School and Restorative Health Benefits in Young People with Varying Emotional Health. London: Forestry Commission.

420 Faber Taylor, A. and F. Kuo (2009). Children with Attention Deficits Concentrate Better after Walk in the Park. Journal of Attention Disorders 12(5): 402-409.

421 Mårtensson, F., C. Boldemann, M. Söderström, M. Blennow, J. Englund and P. Grahn (2009). Outdoor Environmental Assessment of Attention Promoting Settings for Preschool Children. *Health & Place* 15(4): 1149-1157.

- Nature could treat ADHD[423]

- Nearby nature: The more contact a child has with nature, the greater the decrease in stress.[424]

- One-third of the children reported using their favourite places for emotion-regulation.[425]

- Children have better attentional functioning after activities in greener settings.[426]

- The 'greener" a child's play area, the less severe his or her attention deficit symptoms.[427]

Education and Development

- Student Outcomes and Natural Schooling. Pathways from Evidence from the Natural Connections report.[428]

- Nature walk-based teaching was as effective as classroom-based instruction. Students who did a nature walk-based lesson had more positive attitudes toward the material.[429]

- About the barriers re outdoor learning. We need to move from a culture of excuses to a model of encouragement. Educators should view outdoor learning as a pedagogical and problem-solving exercise.[430]

---

422 Kuo, Frances E., and C. Arden Taylor, A. 2004 A Potential Treatment for Attention-Deficit Hyperactivity Disorder. *American Journal of Public Health* 94 (9): 1580-1586.

423 Kuo, F. and A. Faber Taylor (2004). "A Potential Natural Treatment for Attention-Deficit/Hyperactivity Disorder: Evidence from a National Study." American Journal of Public Health 94 (9): 1580–1586.

424 Wells NM & Evans GW 2003. Nearby Nature: A Buffer of Life Stress among Rural Children. *Environment and Behavior* 35(3):311-330.

425 Korpela, K., M. Kytta and T. Hartig (2002). Restorative Experience, Self-Regulation, and Children's Place Preferences. *Journal of Environmental Psychology* 22: 387-398.

426 Taylor AF, Kuo FE & Sullivan WC 2001. *Environment and Behavior* 33(1):54-77

427 Faber Taylor, A., F. Kuo and W. Sullivan (2001). Coping with ADD: The Surprising Connection to Green Play Settings. Environment and Behavior 33(1): 54-77.

428 Articles:
http://www.bbc.co.uk/news/science-environment-36795912
https://www.plymouth.ac.uk/news/report-identifies-ways-to-boost-childrens-quality-of-life-through-outdoor-learning
Report:
https://www.plymouth.ac.uk/uploads/production/document/path/6/6811/Student_outcomes_and__natural_schooling_pathways_to_impact_2016.pdf

429 PC Owen. 2016 Nature Walks as a Tool for Stimulating Learning Outside of the Classroom *The Journal for Research and Practice in College Teaching*

430 H Coe. 2016 From Excuses to Encouragements: Confronting and Overcoming the Barriers to Early Childhood Outdoor Learning in Canadian Schools *Journal of Childhood Studies*

- How schools can tackle the challenges of embedding outdoor learning and integrating learning in the natural environment.[431]
- Connection to nature is also as important to children's achievement in English as life satisfaction and attendance at school.[432]
- Climbing a tree can improve working memory by 50%.[433]
- Access to active play in nature and outdoors is essential for healthy child development.[434]
- Non-formal learning could help to build character and close the attainment gap.[435]
- Literature review. Spending time in nature is part of a 'balanced diet' of childhood experiences that promote children's healthy development, well-being and positive environmental attitudes and values. Play is a good way to do this.[436]
- Understanding the diverse benefits of learning in natural environments.[437]
- Children develop much better motor skills (balance and coordination) in a natural environment than in a traditional playground.[438]

Social and Community

- Family camping reinforces family relationships.[439]

---

431 A Edwards-Jones, S Waite, R Passy. 2016 Falling into LINE: school strategies for overcoming challenges associated with learning in natural environments (LINE) *Education* 3-13, 2016

432 Richardson, M., Sheffield, D., Harvey, C., Petronzi, D., 2016. The Impact of Children's Connection to Nature: A Report for the Royal Society for the Protection of Birds (RSPB).

433 Alloway, R.G., Alloway, T.P., 2015. The Working Memory Benefits of Proprioceptively Demaning Training - A pilot study. *Perceptual and Motor Skills* 120: 766–775. http://www.sciencedaily.com/releases/2015/07/150729102407.htm

434 Tremblay, M. et al. 2015. Position Statement on Active Outdoor Play. *International Journal of Environmental Research and Public Health* 12: 6475-6505. http://www.mdpi.com/1660-4601/12/6/6475
http://www.theguardian.com/lifeandstyle/2015/jun/14/should-i-let-my-child-take-more-risks

435 Birdwell, J., Scott, R., Koninckx, D., 2015. Learning by Doing. http://www.demos.co.uk/files/Learning_by_Doing.pdf

436 Gill, T., 2014. The Benefits of Children's Engagement with Nature: A Systematic Literature Review. *Children, Youth and Environments* 24: 10-34.

437 Understanding the diverse benefits of learning in natural environments. Kings College, London. April 2011. Understanding the diverse benefits of learning in natural environments. Commissioned by Natural England. http://www.naturalengland.org.uk/Images/KCL-LINE-benefits_tcm6-31078.pdf
http://www.monbiot.com/2013/10/07/rewild-the-child/

438 Fjortoft, I. (2004). Landscape as Playscape: The Effects of Natural Environments on Children's Play and Motor Development. *Children, Youth and Environments* 14(2): 21-44.

439 Garst, B.A. et al., 2013. Strengthening Families- Exploring the Impacts of Family Camp Experience on Family Functioning and Parenting. Journal of Experiential Education 36, 65–77.

- What do children learn when camping?[440]
- Wild adventure space has many benefits for young people; the local community and wider society also benefit.[441]

Children's mobilities, independence and play

- We need more effective strategies in balancing children's safety and their need for and right to challenging and risky play.[442]

- England was ranked seventh for child independence in the study of 18,000 seven- to 15-year-olds in 16 countries.[443]

- It's important to engage children in green spaces so that they get into the habit of using them. Eg work with parents and police/rangers etc. to develop a safer environment so that children are allowed to go out alone.[444]

Eco-Literacy

- Direct exposure to the natural world is important for children's understanding of biological concepts and reasoning.[445]

- Local nature (eg tadpoles instead of pandas) is key to linking children to nature[446]

- Children have a huge capacity to recognise creatures (artificial or natural). Pokemon more so than wildlife. Conservationists need to pay attention to this. Games build in 'reward loops' to keep children engaged.[447]

---

440 Camping and Caravanning Club 2013, What do children learn when camping? What-do-children-learn-when-camping%20(2).pdf http://www.campingandcaravanningclub.co.uk/GetAsset.aspx?id=fAAxADkANgA0ADkAfAB8AFQAcgB1AGUAfAB8ADAAfAA1

441 Ward Thompson, C., P. Travlou and J. Roe (2006). *Free-Range Teenagers: The Role of Wild Adventure Space in Young People's Lives.* Edinburgh: OPENSpace.

442 Sandseter, E., n.d. 'We Don't Allow Children to Climb Trees. How a focus on safety affects Norwegian children's play in early childhood education and care settings. *American Journal of Play* 8: 178-200. http://www.journalofplay.org/sites/www.journalofplay.org/files/pdf-articles/8-2-article-we-dont-allow-children-to-climb-trees.pdf

443 Shaw, B., Watson, B., Frauendienst, B., Redecker, A., Jones, T. with Hillman, M., 2013.Children's independent mobility: a comparative study in England and Germany (1971 2010), London: Policy Studies Institute. http://www.bbc.co.uk/news/education-33847890

444 Bell, S. (2005). "Nature for People: The Importance of Green Spaces to East Midlands Communities." In Ingo Kowarik and Stefan Körner, eds. *Wild Urban Woodlands: New Perspectives for Urban Forestry*. Berlin: Springer, 81-94

445 SE Longbottom, V Slaughter 2016. Direct Experience With Nature and the Development of Biological Knowledge *Early Education and Development:* 1-14.

446 Battisti, C., 2016. Experiential key species for the nature-disconnected generation. Animal Conservation.

- Experiences of nature affect children's willingness to conserve biodiversity[448]

- Children's attitudes to invertebrates, esp insects, will improve if primary schools include local invertebrates and species knowledge in the curriculum and allow for real-life experience.[449]

- Positive experiences in nature relate to children's environmental behaviours.[450]

- Nature immersion experiences could address the risk of 'nature-deficit disorder,' improve health, and prepare future environmental leaders.[451]

- Ants help children understand insect biology. Children are more influenced by media than by personal encounters. School-curriculum developers should encourage direct contact with ants.[452]

- The relationships between children's perceptions of the natural environment and solving environmental problems[453]

- Children's disconnection from nature is a problem – the Natural Childhood report that launched TWN.[454]

- Children's connection to nature influences future choices for nature-based activities[455]

---

447 Balmsford et al 2002. Why Conservationists Should Heed Pokémon. Science Now 295 (5564): 2367

448 Soga, M., Gaston, K., Yamaura, Y., Kurisu, K., Hanaki, K., 2016. Both Direct and Vicarious Experiences of Nature Affect Children's Willingness to Conserve Biodiversity. *International Journal of Environmental Research and Public* Health 13: 529.

449 Schlegel, J., Breuer, G., Rupf, R., 2015. Local Insects as Flagship Species to Promote Nature Conservation? A survey among primary school children on their attitudes toward invertebrates. *Anthrozoos* 2: 229-245.

450 Collado, S., Corraliza, J.A., 2015. Children's restorative experiences and self-reported environmental behaviors. Environment and Behavior 47: 38-56.

451 Warber, S.L., DeHudy, A.A., Bialko, M.F., Marselle, M.R., Irvine, K.N., 2015. Addressing "Nature-Deficit Disorder": A mixed methods pilot study of young adults attending a wilderness camp. *Evidence-Based Complementary and Alternative Medicine* 2015: 1-13.

452 Sammet, R., Andres, H., Dreesmann, D., 2015. Human–Insect Relationships: An ANTless Story? Children's, Adolescents', and Young Adults' Ways of Characterizing Social Insects. *Anthrozoo*s 28: 247-261.

453 Looks at how children interpret the natural environment: relationships between environmental education, development education and education for sustainable development. O'Malley, S. 2015 The Relationships between Children's Perceptions of the Natural Environment and Solving Environmental Problems *Development Education and Climate Change* http://www.developmenteducationreview.com/issue21-focus4

454 Moss, S., 2012. Natural Childhood. RSPB, Sandy.

455 Chen-Hsuan Cheng, J. and Monroe, M. (2012) Connection to nature: Children's affective attitude toward nature. *Environment and Behavior* 44 (1): 31-49.

- Strong correlation between ecological knowledge and frequency of visits to green spaces; children who have free play in nature retain a connection to nature as adults.[456]

- An adult's attitude to the environment and time spent outdoors in green space is strongly influenced by their experience as a child.[457]

- Contact with nature before the age of 11 predicts a lifelong positive environmental behaviour.[458]

- Time spent outdoors appreciating nature, hunting and fishing, and exposure to books and nature programmes during youth predict later positive environmental beliefs.[459]

- Adolescents who had played in the wilderness as younger children had more positive perceptions of natural environment, outdoor recreation activities and future outdoor occupational environments.[460]

- Time spent in nature between the ages of 7 and 12 yrs was associated with the adult feeling of 'indignation' about insufficient nature protection.[461]

- Immigrant children in the US who as young children foraged for berries, fish, acorns etc had a much deeper understanding of biodiversity as teenagers than their suburban middle-class counterparts.[462]

2. BOOKS

- Louv, R., 2016. *Vitamin N: The essential guide to a nature-rich life.* Algonquin Books: Chapel Hill, North Carolina.

- Louv, R., 2013. *The Nature Principle: Human restoration and the end of nature-deficit disorder.* Algonquin Books: Chapel Hill, N.C.

- Louv, R., 2005. Last Child in the Woods: Saving Our Children from nature-deficit disorder. Atlantic Books: London.

---

456 Outdoor learning develops children's sense of environmental responsibility DCSF (2010) Evidence of the Impact of Sustainable Schools. London: Department for Children, Schools and Families.

457 Pretty et al (2009) Nature, Childhood, Health and Life Pathways. Interdisciplinary Centre for Environment and Society Occasional Paper 2009-02: University of Essex.

458 Wells NM and Lekies KS (2006) Nature and the life course: Pathways from adulthood Nature Experiences to adult Environmentalism. *Children, Youth and Environments* 16(1).

459 Ewert A, Place G and Sibthorp J (2005) Early-life outdoor experiences and an individual's environmental attitudes. *Leisure Sciences* 27: 225-239.

460 Bixler RD, Floyd MF and Hammitt WE (2002) Environmental Socialization: Quantitative tests of the childhood play hypothesis. *Environment and Behavior* 34 (6): 759-818.

461 Kals E, Schumacher D and Montada L (1999) Emotional Affinity toward nature as a motivational Basis to Protect Nature" *Environment and Behavior* 31: 178-202.

462 Chipeniuk R (1995) Childhood Foraging as a means of acquiring Competent Human Cognition about Biodiversity *Environment and Behavior* 27(4): 490-512.

3. FILM

- PROJECT WILD THING. Bond, D, 2013. http://www.thewildnetwork.com/film

August 2016

Young Scot – written evidence (CHI0034)

Response from the 5Rights Youth Commission

1. The 5Rights Youth Commission is a diverse group of 18 young people, aged 14-21 from all across Scotland, who are supported by Young Scot, the Scottish Government, and 5Rigths to raise awareness about young people's rights in the digital world. After being launched in February 2016 by Scotland's Minister for children and Young People, Aileen Campbell MSP, they have now embarked on a 12-month investigation to develop recommendations for the Scottish Government on how Scotland can realise young people's rights in the digital world. To inform their investigation, the 5Rights Youth Commission has been reaching out to experts, professionals, as well as specific groups of young people to gather evidence about their digital world from all angles. Their report on their findings and insights is due to be completed in February 2017.

Question 1: What risks and benefits does increased internet usage present to children and young people, with particular regards to;

Social development and wellbeing

2. The risks of increased internet usage to social development and wellbeing include, but are not limited to:

- increased isolation, as children and young people often stay indoors and choose to interact online, rather than interacting with their peers face to face;
- encouraging dangerous and self-destructive behaviour, for example pro-anorexia/bulimia/self-harm websites, which encourage and/or glamorise very serious illnesses;
- device dependency and a fear of missing out – some 50% of teenagers have admitted feeling addicted to their devices[463]; lack of sleep due to device dependency, which increases the risk of both mental and physical health problems; cyberbullying and harassment and the young person's inability to "shut out" their harassers.

3. However, increased internet usage among young people does bring some benefits to social development and wellbeing. These include:

- more ways to interact with people, and a new means of meeting new friends (admittedly with risks attached);
- in some cases decreased isolation as young people in minority groups such as LGBT and those with physical disabilities can

463 Felt, Laurel J. and Robb, Michael B. Report - 'Technology Addiction – Concern, Controversy, and Finding Balance.' Common Sense. https://www.commonsensemedia.org/sites/default/files/uploads/research/2016_csm_technology_addiction_executive_summary.pdf

connect with those who better understand what they are going through;
- resources such as AyeMind (http://ayemind.com/) which support and advise those with mental health problems and websites such as ChildLine, which offer a safe place for children and young people to get advice on a wide range of issues which may be affecting them.

Neurological, cognitive and emotional development

4. The impact of increased internet use on emotional development is different for each young person and depends entirely on their experience and circumstances.

5. For some, the internet is comforting, as they realise that they are not alone in their problems and can talk to others going through the same. For others, they feel that the internet gives them confidence, as they can show and express parts of themselves they may have to conceal at school or home through an anonymous web profile. Many feel the internet allows them to feel connected to the rest of the world, as it can be used both to find friendships locally (e.g. through alerting them to events in their area, location based social networking, etc.) and internationally, through public social networking sites such as Twitter and Tumblr.

6. However, not every young person reports a positive experience of the web; some feel that increased internet usage is stressful, as they are expected to always be online and always be available. Many report that the pressures they face in the real world are still very close online. There is still a pressure to "fit in" in online communities; those who harass them at, for example, school or college have a powerful tool with which to continue their harassment; wishing to be left alone or disconnect from the web for a short time is often met with concern or even annoyance from their peers.

Data security

7. Each and every child and young person online is being tracked by numerous technologies and unlimited companies. The use of "cookies", a data package used to track users' browsing activity across sites and platforms, begins to create a profile of the user, mostly without their knowledge. This, along with the data that the user has volunteered online via social media: the information they have shared, the media they have uploaded, and the items that they have 'liked'; can all be sold to advertising companies and data brokers, to name a few. Advertising companies use these profiles to personalise online advertisements, to maximise their traffic and therefore profit. This is impactful on susceptible children and is commercial exploitation of young people. By contrast, this can also create a more personalised and better experience online. These online profiles can (and have been) be sold to future employers and educators, so online habits are

increasingly effecting young people's future chances.

8. Mobile app permissions can also be a cause of concern. A magnitude of apps require location access, without it being part of the service. This data is easily exploitable and crosses a child's online life to their real world one.

9. This practice leads to many accusations of commercial exploitation as well as lack of privacy online, as tracking is constant and easy. As of yet, there are no regulations in place to prevent this.

Questions 2: Which platforms and sites are most popular among children and how do young people use them? Many of the online services used by children are not specifically designed for children. What problems does this present?

10. For children aged over 10, the most popular sites include Facebook, Twitter, Snapchat, Tumblr, Musical.ly, YouTube, Instagram, Skype, Steam, Kik, and more. These are generally used to socialise with existing friends, as well as meet new ones, find guidance and advice (rightly or wrongly) on issues that may be affecting them, to express themselves, or just to have fun.

11. Many children who are not quite old enough to know or understand how to increase privacy settings or the dangers of not doing so, may be putting themselves at risk of being the "prey" of online predators, potentially endangering themselves or others. They may also forget that what is posted online is near-impossible to fully delete, so may land themselves in trouble for problematic social media posts in later life.

12. Other sites commonly used by young people are more educational, and are often recommended or required by their school, such as Edmodo, Schoology, School Things, and DuoLingo. While these do not carry the same risks as social networking sites, they may further encourage device dependency by making it harder for young people to limit time in front of the screen, as well as disadvantaging those who maybe cannot access the internet or afford phones or laptops.

Question 3: What are the technical challenges for introducing greater controls on internet usage by children?

13. The main challenge lies in the determination and defiance of the young people themselves: if they truly want to be online, they will find a way around any restrictions placed on them. Children in primary school already know how to forge parental consent and "fake their age" in order to access social media sites they would otherwise be banned from, and many young people are even more able to deviate from the rules placed on them. They may access internet sites through encrypted services such as TOR, or use the "Browse Incognito" feature on their browsers in order to prevent parents or carers from tracking

their internet history.

14. Furthermore, limiting young people's online use may do more harm than good. According to a Huffington post article[464], young people do indeed recognise that they are addicted to their devices, but feel that time limit control takes away their sense of trust and control online.

Question 5: What roles can schools play in education and supporting children in relation to the internet? What guidance is provided about the internet to schools and teachers? Is guidance consistently adopted and are there any gaps?

15. Schools play a very important role in supporting young people on the internet. The curriculum must be kept up to date, and is regularly updated every two years at least in order to keep up with the rapidly changing nature of online life. Internet safety and cyber resilience must be taught much earlier – mid to late primary school – and be covered fully and treated with utmost importance in the education system. Internet safety should include protection against predators, awareness of online dangers, etc., and must *not* say nor even imply that children should be avoiding the internet altogether. Cyber resilience should cover hacking, phishing, data profiling and mining, key loggers, GPS tracking, and access to personal data.

16. Digital skills must be consistent, comprehensive, and at the forefront of modern education, but according to our evidence session with Education Scotland, primary school teachers feel unequipped to teach digital skills as resources are either outdated or non-existent.

Question 6: Who currently informs parents of risks? What is the role for commercial organisations to teach e-safety to parents? How could parents be better informed about risks?

17. Parents are currently informed of risks through news, television documentaries, and their own children or children's school. Some may also learn of online risks from websites such as the Ofcom website, ParentZone Scotland, or other online communities and blogs.

18. This is rather limited as far as parents' knowledge is concerned: documentaries and online communities may scare-monger and make parents feel unnecessarily uneasy about their child's online life, and young people often don't inform parents fully for fear that they will restrict their online activities.

19. Parents could be better informed about risks through personalised advertisements for parents online, or perhaps a more official way of young people teaching their parents about the digital world – for

---

464 Report - 'Impact of e-Discipline on Children's Screen Time' http://www.huffingtonpost.com/entry/teens-feel-addicted-to-their-advices-but-say-their-parents-are-the-same-way_us_57291f31e4b016f378940715

example through workshops held at school or community events. This would give parents a chance to ask questions and receive perhaps a less biased or one-sided view.

Question 7: What are the challenges for media companies in providing services that take account of children? How do content providers differentiate their services for children, for example in respect of design?

20. Media companies may struggle to keep track of how many young children are using their website; even if they do implement age restrictions, many children ignore them and forge parental consent and use a fake age. It is thought that 7.5 million children under the age of 13 use Facebook, where the age restriction is 13; however Facebook claims to be removing 20,000 of these children every day.

21. Currently implemented in the United States is a law called COPPA (Children's Online Privacy Protection Act), which forbids the collection of children's ("children" meaning "under the age of 13 years") data without parental consent, which may be achieved through a parent's email or credit card number.

22. COPPA is seen by many critics as only the "bare minimum" – the EU would rather raise the age of those covered to 16. Critics also point out slightly questionable parts of the law – the website says that COPPA would "provide parents access to their child's personal information to review and/or have the information deleted"[465], which raises concerns about children's right to privacy.

25 August 2016

[465] "Complying with COPPA: Frequently Asked Questions" https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions

YouthLink Scotland – written evidence (CHI0006)

1 About YouthLink Scotland

1.1 YouthLink Scotland is the national agency for youth work. We are a membership organisation, representing over 100 regional and national youth organisations from both the voluntary and statutory sectors. We champion the role and value of youth work and represent the interests and aspirations of both the voluntary and statutory sector.

1.2 Scotland's youth work sector is as rich and diverse as the nation itself. Our sector has a workforce in excess of 75,000 – including over 70,000 adult volunteers. We reach in excess of 380,000 young people in youth work opportunities each week. Youth Work has three essential and definitive features:

- Young people choose to participate
- Youth work must build from where young people are
- Youth work recognises the young person and the youth worker as partners in a learning process

1.3 YouthLink Scotland champions the role and value of youth work, challenging government at national and local levels to invest in the development of the sector for the benefit of our young people. Our vision is of a nation which values its young people and their contribution to society, where young people are supported to achieve their potential.

1.4 As the national agency for youth work, and in our role as an intermediary we have endeavoured to respond to this response in the best interests of the youth work sector, however the views contained within this response may not be held by each of our individual members.

1.5 YouthLink Scotland, as the National Agency for Youth Work in Scotland has been leading on developments in the field of digital technology and social media in relation to youth work. Our role spans both policy and practice, working closely with Education Scotland, Scottish Government and our members – statutory and national voluntary youth work organisations to implement the National Youth Work Strategy 2014-19 (Scotland). Alongside partner organisation Young Scot, we established the Digital Youth Network. This is a practitioner network for those working with young people in online spaces or using online tools.

1.6 YouthLink Scotland was the lead partner in developing the Digitally Agile National CLD principles alongside Scottish Community Development Centre and Learning Link Scotland. We are also a representative member on the European Commission Expert Group on Digitalisation and Youth.

1.7 It is critical that throughout this inquiry and the resulting actions that follow that influencers and decision makers prioritise the fundamental principles

of the UN Convention on the Rights of the Child (UNCRC) whilst also maintaining an agile mind set. Online trends fluctuate rapidly and as a result, detailed research, legislation or regulation on specific platforms or sites can become quickly outdated.

2 Risks and benefits

2.1 We are concerned that there is not sufficient research on the impact of increased internet usage alongside increased usage of digital devices on children and young people's development and mental health. We would welcome a longitudinal study of children and young people in the UK that examined the impacts on health and wellbeing.

2.2 The opportunities and benefits offered to children and young people from the internet are ever-expanding. Alongside these opportunities come risks. Broadly these can be grouped into:

2.2.1 Information and education

Children and young people are exposed to alternative media outlets and endless sources of information exponentially increasing the learning opportunities. However members were keen to point out that children and young people were often ill-equipped to contextualise information they come across or identify factual from fake information. Organisations such as Young Scot provide support for young people to access the information they need in an accessible format.

The way in which selected information is presented to children and young people through the use of algorithms is also a concern.

2.2.2 Play and creativity

The importance of play for people of all ages cannot be understated and the internet is a popular playground for children and young people. On the internet children and young people today have the unprecedented opportunity to be content producers, rather than purely consumers. This will contribute to the exploration and development of their identities and media literacy.

With regards to vulnerability to commercial pressures, online gambling and pay-to-play games are designed to attract and entrap younger players which could result in financial risks and concerns around misuse of personal data.

2.2.3 Communication and connectivity

Platforms and sites are being used innovatively to facilitate social interaction and communication for those on the autistic spectrum.

Increased communication can also carry the risk of exposure to age inappropriate content for example violence or pornography. Young people may be receiving this but also may be producing and sending to others. Cyberbullying is often pointed to as one of the main internet problems facing young people online. Research in Scotland showed that 91% of those experiencing online bullying know the person bullying them.[466] This dispels the myth of the anonymous threat and reinforces the need for anti-bullying work in person with young people.

2.2.4 Political and civic participation

One of the most important benefits from our members' perspective is that young people have access to youth work online, often in the form of support and advice services.

Social media provides a platform for young people to express their opinions and be heard. It is narrowing the traditional generational gap of whose voices are heard in decision making. It is also changing the way in which young people engage politically through organising and taking part in social media campaigns and other 'clicktivism'. It is also important that young people's rights are realised in relation to the digital world. 5Rights have worked with young people to develop a framework and resources around children and young people's rights online.[467]

2.3 Concerns were also raised by members regarding the increasing amount of time young people spend online. Risks of excessive use can manifest as social isolation, sleep deprivation and dependency. There was also discussion on the time young people spend online compared with time outdoors. Rather than polarising this debate, our members found it more helpful to find ways to combine digital learning with outdoor environmental engagement. It is possible to use technology designed to enhance rather than distract from time spent outdoors and engage with technology collectively (with real people in real time) rather than singularly.

2.4 The popularity of platforms and sites online is fleeting and much time should not be spent listing these. Of more use is to be familiar with shared principles, common terminology and cross-cutting trends. This will allow decision makers to be agile and for legislation to be sustainable. Net Aware by NSPCC is a useful guide for parents and carers to popular social networks. It provides brief explanations and has a user input function for parents/carers to share their experiences.

2.5 Our members had strong feelings that introducing greater blanket controls on internet usage by children and young people was the wrong approach. Their preference was for improved guidance, education and support in order to help children and young people navigate their lives offline and online safely. Furthermore, excessive controls on children and young people's internet usage

---

466 Respect*me,* Bullying in Scotland 2014, p.3, http://www.respectme.org.uk/about-news.html

467 http://5rightsframework.com/

may contravene their rights.[468] Some members had suggestions around banning mobile devices in school classrooms. Members also raised the point that controls can often be bypassed by young people. An indicator of this in action is the age limit for most social media sites. The standard age limit is 13 years old but many young people under this age have active profiles. In this instance, although controls are in place, young people have found a way around them and as such should be adequately prepared to use the sites in a safe and responsible way.

Taking risks and pushing boundaries is how children and young people gain resilience and therefore decision makers should take a balanced approach to increasing online controls.

3 Education

3.1 Educating and supporting children and young people in relation to the internet also takes place outside of school within youth work settings. Digital youth work engages young people using conventional youth work models and supports young people in developing their offline/online agency. Internet usage amongst young people will not decrease therefore youth work has to also be online. It is crucial that informal education through youth work is recognised and included in further action.

3.2 One of the essential features of all youth work is that it builds from where young people are, taking their knowledge and skill level as a baseline. Young people today do not differentiate between their online/offline lives or relationships and have to navigate the same challenges in both realms. Using this approach youth work has been leading the way in harnessing digital spaces to engage with young people. Alongside key partners we are working towards a youth work sector in Scotland that is well equipped to support young people to navigate the online aspects of their lives as well as to capitalise on the opportunities that digital and online tools offer to enhance their practice. In order to do so effectively, the youth work sector needs continued funding to upskill workers.

3.3 A central benefit of digital youth work includes the accessibility for geographically or socially isolated young people. Digital youth work provides opportunities for young people to access support they otherwise would not feel comfortable accessing in person. LGBT Youth Scotland's online chat service run by youth workers provides support for young people around any issue, but in particular around identity and sexual orientation. It is a unique service and as a result young people from outside of Scotland also access it, proving the need for more similar services.

3.4 Some members have produced guidance on using the internet for young people involved in their organisation. GirlGuiding UK have different age appropriate web safe codes for Rainbows, Brownies and Guides.[469]

---

468 It is suggested that greater controls may contravene UN Convention on the Rights of the Child Articles 12, 13, 15, 16, 17.

469 GirlGuiding UK, *My Brownie Web Safe Code*, http://www.girlguiding.org.uk/brownies/websafe/

3.5 One member pointed out that the UK should expect to produce the next wave of digital tech innovators. In order for them to be responsible, sustainable and considerate, they need to understand e-safety, digital rights and the importance of being raised online through guidance. With the popular estimate that 65% of jobs young people will be employed in do not exist yet, digital literacy education at all levels needs to be flexible and dynamic. Digital literacy education should also include teaching children and young people to be critical consumers in order to understand how and why content is created. This increased transparency would likely correlate with increased understanding amongst children and young people of online risks.

3.6 It is often taken for granted that children and young people today are 'digital natives' and are equipped to use the internet and digital technology. This is not always the case. There is also the risk that young people who are not using the internet will be left behind when it comes to finding work and operating in an increasingly online world.

YouthLink Scotland believes that work needs to be done across the UK to increase availability of internet access, especially in rural areas. Investment in digital participation was included as an ask in our Youth Work Changes Lives manifesto, including widening access to free Wi-Fi in public and community spaces.

3.7 Our members thought there was a potential for youth workers to provide some form of e-safety education for parents because the majority of internet usage will be in the home. However it should not be an extra task for teachers or youth workers without additional resource allocation. In Scotland there is an opportunity for community learning and development (CLD)[470] to engage with parents to teach digital literacy and e-safety. Our members cautioned that appropriate funding and consideration is given to teaching e-safety to parents. We believe that more should be done by the UK Government to support this work, including funding for upskilling the CLD workforce, and improved community connectivity and accessibility.

3.8 Members also raised the issue of partnership working across communities to better facilitate the education, support, and where necessary prosecution, of children, young people and adults. Funding to facilitate multi-agency approaches to addressing this would be welcomed.

4 Governance

4.1 We encourage media companies, in particular social media companies, to work closely with informal educators in order to ensure the design of their site or platform enhances young people's safety and security. Current restrictions can cause difficulty for youth workers, for example creating separate youth worker profiles. It compromises youth workers' own safety and privacy as well as that of

---

470 Within the Scotland, community learning and development encompasses youth work, adult learning and community capacity building.

the young person. In order to maintain appropriate boundaries, it is crucial to have buy-in from platform and site developers.

5 Legislation and Regulation

5.1 Our members do not think current legislation and regulation alter the way children and young people use the internet. This is primarily due to a perceived lack of knowledge and education. A young person may come into contact with legislation when a site they are accessing is shut down but they do not understand their rights or responsibilities in relation to this. There should also be recognition that not only can children and young people be victims of online crime, they can also be perpetrators (e.g. hate crime, cyberbullying, hacking, illegal downloads etc). As perpetrators they may be vulnerable or victims themselves. There needs to be an examination of how legislation can work to protect them. YouthLink Scotland suggests that the UK Government should increase the transparency and awareness of relevant legislation for young people and those around them (parents/carers, teachers, youth workers).

5.2 As mentioned previously, young people do not distinguish between their online/offline lives and as such, we recommend that future legislation and regulation reflects this. An agile mind set is required in order to future proof legislation. Rather than referring to specific platforms or sites, legislation should focus on the common elements and principles.

5.3 YouthLink Scotland would urge that Child's Rights Impact Assessments are carried out on future legislation in order to ensure that children and young people will not be adversely affected. This is in line with the recent UN Convention on the Rights of the Child Concluding Observation 9a[471].

5.4 The General Data Protection Regulation closely mirrors the 5Rights framework[472] with regards to individual's data. YouthLink Scotland supports implementation of the rights from the General Data Protection Regulation with the addition of the Right to Digital Literacy and the Right to Safety and Support, as laid out in 5Rights framework. Our members had particular concerns about the way in which young people's personal information and digital habits can be used in sophisticated ways without the young person realising how or why it has happened. This concern would be somewhat alleviated by the GDPR Rights in relation to automated decision making and profiling.

18 August 2016

---

471 UN Convention on the Rights of the Child, Concluding observations [CRC/C/GBR/CO/5), http://tbinternet.ohchr.org/_layouts/treatybodyexternal/SessionDetails1.aspx?SessionID=987&Lang=en

472 http://5rightsframework.com/