THE FUTURE OF CRIME REPORTING

CAN ANONYMITY BE DELIVERED IN THE DIGITAL AGE?

JENNIFER COLE AND ALEXANDRA STICKINGS

Digital communication leaves traces that can lead back to the person who initiated the communication or their location at the time. Jennifer Cole and Alexandra Stickings explore the challenges this brings for platforms that claim to offer anonymous crime reporting and ask what can be done to assure members of the public that their identity can still be protected.

How data are protected on Crimestoppers systems, including technology standards and organisational processes, cannot easily be discussed in the public domain without compromising the integrity of those systems. This article is therefore not able to provide specific detail on these aspects. The systems have been described in depth to the RUSI researchers and TRILLION project staff responsible for this article, and the wording of the descriptions provided here have been agreed with Crimestoppers.

As the world becomes more digitised and communication through digital applications and social media becomes more prevalent, an interesting question arises as to the effect this is having on the relationship between law enforcement and communities, and in particular on how the public is able to report crime. Allowing for methods of crime reporting to move in tandem with the increase in the percentage of the population that communicates mainly through social media will ensure that those wishing to alert law enforcement to potential criminal activity continue to be able to do so easily and effectively.[1]

Nevertheless, despite the increase in the ways members of the public can report crimes directly to law enforcement, there will always remain a section of the population that, for various reasons, wishes to remain anonymous in such instances. These reasons range from an inherent distrust of law enforcement within a given community, to an individual who may have concerns regarding a family member and therefore does not wish to be identified as having contacted the police, for fear of reprisal if it becomes known that the individual reported a crime.[2]In these instances it is essential that mechanisms exist for such individuals to be able to contact law enforcement, or another organisation, with full confidence that their identity will not be divulged and that there is no method by which anyone – including the law enforcement agency – can trace their reports back to them.

If law enforcement wishes to be informed of criminal activity from all sections of the population, including those with whom it may not have the most constructive relationship, providing a method for anonymous reporting is essential. This may have to be managed through a third party. Independent research carried out by the UK charity Crimestoppers suggests that 95 per cent of those contacting the organisation would not have gone directly to the police.[3] As Crimestoppers passes more than 100,000 reports to law enforcement each year, the removal of this service would be a huge loss of operational intelligence to police forces across the UK. There is therefore a real value to anonymous reporting.

Understanding the benefit of organisations such as Crimestoppers and the reasons for their existence introduces a number of issues into discussions on online crime reporting platforms, such as trust and anonymity. Ensuring that these issues are fully integrated into the design of current and future crime reporting platforms is essential if they are to be used effectively.

Policing in the Digital Age faces a number of challenges, including understanding the staff capacities and capabilities, as well as potential changes in working practices that may result from the need to analyse large volumes of data;[4] how to police digital communities; and how to effectively communicate with the public using social media. Several of these issues were explored at RUSI's recent conference on the subject in June 2016,[5] but one still deserves more attention: that of anonymous crime reporting. Since September 2015, RUSI has been part of TRILLION (Trusted Citizen – LEA Collaboration Over Social Networks),[6] a project funded under the European Commission Horizon 2020 programme's Ethical and Societal call to '[Enhance] cooperation between law enforcement agencies and citizens – Community policing'. TRILLION intends to develop an online platform through which citizens can report crimes, suspected crimes, public safety issues and other information they consider to be of interest to law enforcement agencies and through which those citizens can receive information back from the law enforcement agencies. The project has enabled RUSI researchers to explore these challenges in more detail not only in regard to the proposed platform TRILLION will deliver, but within the context of online crime reporting more generally.

As online communication has become more embedded in society, the options for UK citizens to report misdemeanours through a number of digital platforms have increased – current options include the Anti-Terrorist Hotline,[7] online portals operated by regional police forces such as London's Metropolitan Police Service,[8] victim support organisations such as Somerset and Avon Rape and Sexual Abuse Support (SARSAS)[9] and Tell MAMA,[10] independent charities such as Crimestoppers,[11] and by using an increasing number of apps such as Witness Confident's Self Evident[12] and Facewatch.[13] These systems provide a range of functionality from making a simple text statement to the police, to filing a report, storing photographic and/or video evidence of a crime and enabling business owners to share information on potentially troublesome customers. During the evidence- gathering stage for the Report of the Independent Surveillance Review,[14] there was discussion on whether the way in which digital information can be traced through cyberspace makes the promise of delivering anonymous reporting in the Digital Age possible and therefore ethical, as the digital traces recorded by such technology now make it easier than ever to trace a report back to the person who made it. It is perhaps not surprising, therefore, that of the platforms mentioned above, only Crimestoppers (and SARSAS if it is the victim themselves making the report) offers anonymous reporting. Others, including SARSAS (if someone other than the victim is reporting) and the Metropolitan Police, promise 'confidentiality' themselves, deferring those who want to report anonymously to Crimestoppers. The charity therefore is an interesting case study of how anonymity (the ability of the reporter to protect their identity from the organisation to which they are making the report), as opposed to confidentiality (the promise that the organisation to which the report is made will protect the reporter's identity to the best of its ability) can be embedded into digital crime reporting platforms and also why such anonymity is valuable.

Anonymity in Crime Reporting

Addressing the extent to which such concerns over the potentially diminishing ability to report anonymously in the Digital Age are valid requires examinations of two key factors: the extent to which anonymous reporting is of value (and therefore the extent to which it should be supported if it is technologically possible to do so); and whether it is in fact possible (and therefore ethical to promise) to deliver anonymity over a digital system.

The propensity to report a crime at all – anonymously or otherwise – depends on a number of factors.[15] Some of these relate directly to the crime itself (for example, the seriousness of the offence and type of crime), some to the social context (for example, the level of trust between citizens and the institution of the police, or between individual citizens and individual police officers) and some on the reporting process itself (for example, duration of the process, methods of reporting and possibility to report anonymously). A number of studies suggest that the ability (or not) to remain anonymous is a strong influence in crime reporting,[16] although other research suggests the influence of anonymity on crime reporting is weak or nonexistent.[17] There may be several reasons for this inconsistency, including different objects of study (Carolyn Stone and Madelyn L Isaacs studied US high school counsellors who had been informed of a crime by those they were counselling;[18] Jochem Tolsma et al. studied members of the Dutch population who were provided with fictitious crime narratives), different research methods and study designs and different theoretical points of departure.[19]

Although the importance and role of anonymity for crime reporting in general is unclear, where it has been employed, a number of benefits can be identified. Crime reporting can increase dramatically following the introduction of anonymous police tip lines,[20] and independent research commissioned by Crimestoppers indicates that 95 per cent of people who contact the organisation say they would not have gone to the police, often because they are reporting from within criminal communities or are closely related to criminals. Two examples given were of an individual involved in burglary, who wanted to inform on an accomplice who had beaten an elderly woman during the event because he felt this behaviour was unacceptable (though burglary *per se* was not) and a mother who had informed on her son as he set out to commit an armed robbery because she would prefer him to be arrested by police en route than shot during the act.[21] Those who use anonymous reporting mechanisms are not necessarily law-abiding citizens themselves: as well as feeling vulnerable to crime, they may fear the consequences of other members of their community knowing they have passed information to the police or have something to hide themselves.

Crimestoppers's own history illustrates this. Originally called the Community Action Trust, it was set up in the wake of serious rioting on the Broadwater Farm housing estate in Tottenham, North London in October 1985, during which Keith Blakelock, a police constable with the Metropolitan Police Service, was killed. The events were triggered by the death of a black woman from heart failure during a police search of her home in an area with a community that was highly ethnically diverse and had low levels of trust in the police or authority.[22] Blakelock was surrounded by rioters on 6 October and received more than 40 injuries, dying from a stab wound to the neck. To bring his killers to justice, the police needed information, but as members of the community who might provide it were both mistrustful of the police and scared of any other members knowing they had interacted with law enforcement agencies, the police appealed for this information to be provided with the promise of complete anonymity to any witnesses or informers who came forward. Michael Ashcroft, a businessman, offered a reward to anyone willing to provide information that would help the police, and this eventually led, along with additional funding from other concerned members of the business community, to the charity that became Crimestoppers in 1988.

Crimestoppers receives reports from citizens and passes only the information about the crime or criminal activity, not information about who made the report, on to the police. Encryption on the Crimestoppers system, which contains identifying data such as the phone number or the IP address used by the device from which the report was made, ensures that such information is not available to Crimestoppers staff or system operators. This means, however, that while the charity provides information relating to crimes which may be of intelligence interest to law enforcement, this is not legally considered to be crime *reporting* and the information cannot be used on its own in court to bring a prosecution. Crimestoppers operates under a covenant agreement with the UK National College of Policing which has enshrined the terms under which it can operate, recorded as Authorised Professional Practice and governed by a national policing lead drawn from the executive leadership of one of the UK police forces. This is essentially a memorandum of understanding, reinforced with formal information sharing agreements between the organisation and the National College of Policing which have no additional legal standing.[23]

Disadvantages of Anonymous Reporting

While the main advantage of enabling anonymous crime reporting appears to be an increase in the number of people willing to make a report, and therefore in the information available to the police, there are some disadvantages. Law enforcement agencies may not be able to follow up on anonymously reported crime to see if the reporter has more information as they do not know who made the report and have no way of contacting them. As touched on above, in the UK and across the EU, anonymous reports cannot be used as evidence in court (though in the UK, Anti-Social Behaviour Orders can be issued on the basis of anonymous crime reporting[24]). In the UK, much of the legal debate on anonymity in crime reporting has centred on three key issues: the disclosure of evidence; the legal principle that an accused must be able to question his or her accuser; and whether anonymous reports can be considered as sufficient evidence to convict a defendant.[25] The general pattern in UK courts has been that either the defence requests disclosure (that is, that the anonymous reporter comes forward) or that the prosecution applies for leave of court while it obtains further proof that the accusations made in the anonymous report (that the reports can be 'adduced') are substantiated.

The information provided to Crimestoppers is anonymous and thus inadmissible in court. However, it enables the police to gather further information. For instance, should person A report to Crimestoppers that person B stole person C's handbag in a certain place at a given time, and then tell the police where person B lives, police can then check the CCTV camera at the location of the reported crime. If the CCTV recording shows the person taking the bag wearing a distinctive jacket, police can then go to person B's address and find the stolen handbag and the distinctive jacket. Along with the CCTV footage, this proves that person B stole the handbag. Thus, while the Crimestoppers report is not used as evidence, without it, the conviction would not have been possible.

There are some specific areas in which exceptions are made, such as legislation regarding whistleblowing that allows employees to make confidential and/or anonymous reports of financial irregularity or malpractice. The legal framework in the UK, with provision in the Employment Rights Act 1996, is roughly similar to that of the US, which is based on the Dodd–Frank Wall Street Reform and Consumer Protection Act 2010 and the Sarbanes–Oxley Act 2002. The situation in the UK does raise issues of compliance with EU data protection law which continue to be debated, as some EU directives have yet to come into force.[26] In general, however, anonymous crime reports cannot be used as evidence in court.

Anonymity Online

In addition to general considerations of anonymity in crime reporting outlined above, the extensive literature on anonymity in online systems, particularly from the fields of computer science and human–computer interaction, points to both advantages and disadvantages of allowing users to remain anonymous when using online platforms that need to be considered in this context.

Advantages come mainly from enabling people to adopt 'technical, temporary identities' that enable them to create a separation between their offline and online identities.[27] In the context of an online crime reporting platform, a user from a community or family that is hostile to law enforcement may be afraid of their identity being revealed if criminals hack into the system, or if there are corrupt employees who receive and process the data and who may inform the criminals. Anonymity will help users to feel confident that their identity is protected from such eventualities.

Anonymity has been shown to provide protection for political activists and dissidents, who deviate from the norms and expected behaviour of their society or community.[28] This is similar to the example provided above of the people who report through Crimestoppers: they do not want to be identified by those around them or by the authorities to whom they are reporting. Disclosure of information is higher when the risk to the discloser is perceived to be lower, and online anonymity has been associated with people feeling less intimidated about what they disclose in online platforms compared with face-to-face interactions.[29]

Alex Leavitt suggests that anonymity allows users to feel insulated from how their submissions are received,[30] making them more likely to submit information they are not sure is correct or which they feel may result in their being ridiculed. Crimestoppers can also identify examples where this was a factor in the preference to report anonymously: a woman who thought the description of a rapist matched that of her neighbour (which it did, eventually leading to his conviction) subsequently told the charity she would never have reported had she not been confident of anonymity, in case she had been wrong.[31] She eventually came forward and identified herself following a request to do so which was put out in the media, so that she could be a witness in court. By that time, additional police evidence was sufficient for her to feel confident that she was correct in her identification.

Anonymity in Online Crime Reporting

While current EU legislation does not directly mention anonymous crime reporting, the EU's 2012 Directive on establishing minimum standards on the rights, support and protection of victims of crime does state that 'measures should be put in place to enable third- party reporting, including by civil society organisations', suggesting an understanding of the value of anonymity in protecting victims.[32] However, it does not set out how this must or should be enabled. As a result, there is little consistency in how this is enacted between countries, and in the tools and processes available to citizens. In Europe, only the UK and The Netherlands offer anonymous *online* crime reporting through, respectively, the charities Crimestoppers and Meld Misdaad Anoniem,[33] both of which are affiliated with Crimestoppers International.[34] Others, such as the UK's Anti-Terrorist Hotline, offer confidential reporting, which means that while the police will know who has made the report they will do everything they can under data protection legislation to ensure that information is not available to those without a legitimate need to access it. Others, such as the Community Security Trust and Tell MAMA, which enable anti-Semitic and anti-Muslim hate crimes respectively to be reported, do not promise any level of anonymity or confidentiality.

Anonymity and how it can be offered have changed considerably since 1985, when the Community Action Trust was set up. It offers an excellent case study of the challenges faced in this arena, how they have changed over time and some examples of how they can be overcome.

The technical landscape in which the Community Action Trust was established is very different from that of today. In 1985, the majority of crime reports would have been made by using a fixed line telephone. A concerned citizen calling the police from a public telephone box could realistically have been confident that unless they gave their name and address, the report could not be traced back to them. Even the number of the telephone box from which they phoned would not have been automatically recorded by the system. Today, the same person reporting a similar crime from their mobile phone is likely to find that the system records the number of the device the call is made from (from which the mobile operator may be able to obtain a name and billing address), their exact location at the time the call was made, the time they were at that location and a number of other digital markers that conflict with the concept of a truly anonymous report. Several online systems, such as the survey platform SurveyMonkey,[35] appear to give users the option of submitting information anonymously, but in practice capture information that enables that user to be traced: such as the IP address used by the machine from which the survey was completed in the case of SurveyMonkey, which can be viewed by the user who initiated the survey.

However, in answer to the concerns raised by the Independent Surveillance Review, Adrian Tudway, the current head of operations at Crimestoppers, explained that its platform has adapted to the modern technology landscape and does still provide anonymity to its users, through a combination of data encryption, which strips out identifying markers when the report reaches Crimestoppers, and staff processes.

In addition to encryption, non-technical systems are in place to prevent reports from being traced back to who made them. Crimestoppers keeps no recordings of calls or other data records of its own: information is either passed on to the police as an information log or discarded where there is insufficient detail or the information does not amount to a criminal offence. Metadata (the information about the data, such as the time at which the report was received) is separated from content (what the report says happened). Only content is passed to appropriate police forces. Much of this is air gapped between systems, undertaken in secure environments by operators who are allowed to take no mobile devices of their own, nor even their own pen and writing pad, into their working environment. Pads and pens are provided at work stations and shredded at the end of each shift. Reports are collected into batches, which are then submitted to police four or five at a time, further conflating information on the precise times they were made to Crimestoppers.[36]

Providing anonymity to this level does not come cheap: the Crimestoppers model has considerable operating costs attached which are largely met by a Home Office grant, precepts from police forces and by selling its bespoke whistleblowing service to the commercial sector, to which it provides information on reported energy theft to energy companies and crime involving parcels sent through the postal system to Royal Mail and courier services, for example. A further consideration for Crimestoppers is that as current app technology generally requires data to pass through networks and be stored on servers outside the UK, to which Crimestoppers could not confirm service providers did not have access, online reports have to be made through a web browser and URL, a somewhat old- fashioned technology compared with the user preferences of the disproportionately young demographic from which Crimestoppers receives reports.

Anonymity and Data Protection

Anonymity can be defined in a number of ways, however, and in certain contexts, a less absolute form of anonymity – which this article calls '*relative* anonymity' – may be acceptable and appropriate for online reporting platforms. How this can be achieved is set out below.

First, anonymity can be seen as a tool: in the context of crime reporting, it is a mechanism used to protect the identity of the crime reporter – a form of witness protection. Second, it is a technique: a way of realising certain other values, such as privacy and trust, which are of particular value to the prospective crime reporter and so increase their willingness to report. This is not just data protection, however: while there are strong links between anonymity, privacy and data protection, the differences between them are equally important.

Data protection is generally concerned with the second description given above. It is a way of embedding trust in the system by ensuring the user can be confident that their privacy (rather than their anonymity) will be protected. This is, however, becoming increasingly difficult when digital traces are likely to routinely record the phone number of the smartphone from which the report is made, which may be visible to and recorded by the operating system, or the IP address used by the computer used to make the report. Automatic geotagging – the process of adding geographical identification markers to content, such as the latitude and longitude of coordinates at which a photograph was taken – is automatically built into many smartphone cameras. This may identify a user's home address, if that is where they were when they took a photo they have uploaded (for example of antisocial behaviour on the street below their flat).

This has raised concerns over privacy and anonymity: at the extreme end, governments could trawl online platforms to identify people supporting groups such as Occupy,[37] and within the context of a crime reporting platform, such data could be used to identify the location or machine from which an anonymous reporter made a submission and thus identify the person who made it. While this is true, law enforcement agencies in the UK are not able to even attempt to recover such data from reports made to Crimestoppers without warrants compliant with the Investigatory Powers Act 2016; there has never been a case where this has been considered necessary with Crimestoppers.

Such considerations mean that anonymity is difficult to enact and platforms should be wary of promising it. 'Report anonymously' functions may not be able to provide what they claim to offer, and in such cases terms such as 'confidential' are more appropriate than 'anonymous'. Any person wanting to report anonymously could conceal their identity using Tor, or 'onion router' software – which reroutes internet traffic through a volunteer network of several thousand relays to 'sidestep' traffic analysis and surveillance systems by creating layer upon layer of encryption, like the skins of an onion, which would need to be peeled away one by one to get to the original data. Yet while some of those reporting crimes may already use it, most law enforcement agencies, and organisations like Crimestoppers, tend to shy away from association with such software due to its associations with the dark web and online criminal activity.[38] It is also important for members of the public who are not technically adept to be able to report using systems that are as easy as possible to operate, meaning that the provision of anonymity should be, as far as practicable, the responsibility of the system, not the user.

How and where identifying data are captured and stored within the system, and particularly at which points, are key considerations as this will have a strong bearing on how easy – or hard – it will be for an interested party to follow the digital traces back to the reporter's primary identity. There are likely to be at least two steps in this process – the data captured by the internet service provider, and the data passed on by the internet service provider and which are in turn captured and stored by the platform itself. How this is enabled may be different different contexts and may itself provide barriers to, or enhancements of, relative and absolute anonymity.

Anonymity within an online system requires not only encryption and technology but also people and processes (Tor software, for example, could not work without thousands of volunteers being prepared to join and help maintain its networks). While this has many benefits, encrypted devices and data cannot easily be read, accessed or monitored by law enforcement and intelligence agencies.[39] This may diminish or negate the value of the data to law enforcement officials. Yet not providing this level of protection can lead to a lack of trust in the system and accusations of invasion of privacy. It may also lead to users being unwilling to use the system, particularly the reasons why it is not offered are not fully explained to, or understood by, the user.

Privacy and Data Protection

With regard to privacy in other contexts, data protection often relates to the protection of data which are very personal to the individual, such as health records. Where an individual's identity is not dissociated from the information, it is important to know to whom the data relate and limit who is able to see these data. In the case of health data, a doctor needs to know whose test results they are looking at, but the individual may not want a health insurance company, or another member of their family, to see the same data.

Anonymity goes one step further, breaking the link between the identity and the information so that the information exists independently of any one person. In this context, the information needs to have value in and of itself regardless of who entered that information into the system. In this case, the system may accommodate the individual's wish to remain anonymous. In fact, according to the EU's General Data Protection Regulation, 'the principles of data protection should ... not apply to anonymous information', as this information does not relate to 'an identified or identifiable natural person', and only information relating to such persons should fall under the principles of data protection.[40]

How and where these data are captured and stored within a system, and particularly at which points, are key considerations as this will have a strong bearing on how easy – or hard – it will be for an interested party to follow the digital traces back to the reporter's primary identity. There are likely to be at least two steps in this process – the data captured by the internet service provider, and the data passed on by the internet service provider and in turn captured and stored by the system itself. This second stage may involve different data and act as a barrier to or enhancement of anonymity.

Levels of Anonymity

There are, in this context, two levels of anonymity that might be built into an online crime reporting system. The first is anonymity of the user *from* the system. This relates to the identifiable information which is collected, retained and made accessible by the system. Crimestoppers offers a level of anonymity in this regard. The second relates to anonymity *within* the system: the accessibility of identifiable information of one user by other users of the same system and is more accurately referred to as confidentiality.

To use most online platforms, the user must register with the system (so that the system knows who you are, or rather, who you claim to be) or not (so that the system does not know who you are). The choice to register or not may confer different levels of interaction with the system: for example, anyone can look at items for sale on the online shopping platform Amazon, but in order to make a purchase, a prospective user must register with the site, which requires the submission of personal information that enables the system to recognise who is making the purchase. Cliff Lampe and Paul Resnick have identified an important distinction in how a prospective user will trust a platform dependent on whether levels of anonymity and privacy have to be chosen, or whether they are offered as default.[41] If a user cannot remain anonymous when they are reporting a crime, they may decide not to use the platform at all.

However, registration does not have to be a binary 'anonymous' or 'not anonymous' choice: there are a number of options for the configuration of systems which offer differing levels of anonymity and may confer the advantages of anonymity to some users (for example, the crime reporter) while simultaneously overcoming the disadvantages of anonymity to others (for example, the police). This may be particularly important in online crime reporting platforms where the police want to build an ongoing relationship with an individual or a community where there is reciprocal communication and exchanges of information between both sides.

Online and Offline Identities

Anonymisation in digital environments is complicated further as the relationship between offline and online identities, and between identity and anonymity, is complex.

All users of online systems have an offline, or primary identity, which comprises the legally recognised details of who they are. This includes personal data such as their name, date of birth, gender, current address, occupation, nationality and so on. In the case of many online platforms, the user will also gain a username when they register: thereafter, this username will be the online identity which they use to interact with the system. This becomes their digital, or online, identity.

Imagine a notional user of an online crime reporting platform who aims to not only report crime, but also to inform members of a local community about crime threats and crime reduction programmes in their local area. James Roberts is a 36-year-old British taxi driver, living at Flat 42a Altrincham Road, Manchester. He regularly witnesses fights and disorderly behaviour in the city centre late at night and is willing to report these to the police. He is also keen to receive reports from the police of, for example, road closures due to traffic accidents and planned demonstrations that may require him to plan an alternative route. Depending on how the registration process is configured, and the choices James is able to make when he registers with such a system, varying indicators to his primary identity may be apparent in the username he is assigned or chooses. He could be 'Jamesrobertstaximan', which gives indications of his offline identity, or 'Crimereporter4387', perhaps indicating nothing more than that he is the 4,387th person to have registered to use that platform.

Thus, the online identity James uses when he interacts with the system may closely reflect his primary identity, enabling him to be easily recognised within the system by anyone who knows him offline, or it may not, affording him a level of anonymity from other users of the system, even if the system itself knows who Crimereporter4387 'really' is as it has stored information on the primary identity he entered when registering.

Usernames and Passwords

The two-level username/password system is used by many online platforms to enable users to access and interact with them in a reasonably secure manner.[42] The username is a unique identifier that can be tied to a specific person (for example, Jamesrobertstaximan) or role (for example, DrivertaxiH22), and is paired with a password that should be known only to the person(s) associated with that username. Together, the username and password combination, known as a login, enable the user to access the system they wish to use – often from any mobile or fixed device with internet access and a web browser or appropriate app. The system can be configured so that a person can set up only one username, or may allow them to maintain multiple accounts, or to create temporary accounts which are used only once or in very specific circumstances.

When a user is asked to register with a platform, the login system can be configured to capture as much or as little of that user's personal information – and thus as much or as little about their primary identity – as the system developers and operators have decided is necessary or desirable. Users can be afforded a very high level of anonymity, or none.

For example, RUSI asks for fifteen separate pieces of information about an individual's primary identity when they sign up to an account that will enable them to receive newsletters and information on upcoming events.[43] Of these, ten are compulsory in order to complete the registration process, including a name, telephone number, address (including postcode) and an email address. If the individual is unwilling to provide this information, they will be unable to register with, or use, the system. The level of anonymity within the RUSI system is therefore relatively low: the system and its operators can easily tie a username to a primary identity. Users may, of course, choose to give false information – and the system may or may not include various checks to ensure that information submitted is accurate, such as asking newly registered users to verify the account they have set up following a link sent in an email to the email address they provided – but if a user wishes to remain anonymous, doing so is difficult and the process of being asked to submit so much information may itself deter them from registering.

In contrast, the US-based website Reddit asks users only to choose a username and a password that can, thereafter, be used to log into the account that was created by the owner of that username. While the user is also asked to give an email address which will link back to that username, this is not compulsory and does not prevent registration from being completed. No other information is requested – Reddit does not want to know (or more realistically has decided it does not need to know) the age, gender, home address, occupation, nationality or any other information about its users. They are, in effect, anonymous to the system and to Reddit's owners and operators. The system does, however, record information such as the user's IP address and MAC (media access control) address, the latter being linked to an individual device. These could, conceivably, enable the user to be traced, but for this to happen an active decision (such as a court order) would need to be made.

Regardless of how much information on a user's primary identity is stored, the login system affords users pseudo-anonymity in which the username becomes the user's default identity within the platform. If they interact with the platform regularly, trends associated with their username will soon become recognised by the system itself and the username by other system users, as will regular behaviour patterns they exhibit. Within crime reporting platforms, it may be valuable for the system to capture and store information on users who report regularly in a user profile, which will show to the system (and to certain users of the system) the quality or otherwise of previous reports made by that individual. Other information contained in a user profile could include: how long they have been a registered user; how many reports they have made in that time and on what types of crime; how well received their reports have been; and whether they have led to any convictions. Such a system may enable users to add additional information to their user profile which may be useful to the police, such as whether they are currently working in a security-related job – for example a security officer in a shopping centre or nightclub security guard – that might help to prioritise reports they make to the system or enable additional information to be passed to them which the police may not want to disseminate to the wider public.

Over time, system privileges – such as 'approved user' status, or preferential triaging of reports received from that username – might be awarded on the basis of a user's past activity, even if the system does not know much, or anything, about their primary identity. Knowing that past reports made to the system by that username have been reliable and valuable may be useful in itself. User profiles can also offer a way for law enforcement agencies to follow up with crime reporters, as messages can often be sent via systems' internal messaging systems to the username account, and in fact Crimestoppers uses just such a system to enable anonymous reporters to remain in contact with the organisation by logging into a section of the website where messages can be left and replied to.

The login system can, therefore, provide a pseudo-anonymity that both conceals information about the user and encourages disclosure through dissociation with the primary identity, enabling individuals to disclose with less reservation.[44]

Regardless of how much personal information the system chooses to ask a user for when they register with the platform or how much data are likely to be captured by the system at the time a report is made, it is important to ensure that the system makes clear what level of anonymity – from the system or within the system – is being offered and how this is being enacted.

Anonymity Within the System

If the level of protection provided by Crimestoppers is not available, the pseudo-anonymity of the login system, combined with robust adherence to data protection directives, should be sufficient for a prospective user to trust the system to protect their primary identity, but this will depend on how the data are handled once inside the system.

Any crime report made through an online platform will comprise two elements: content and metadata. Separating the metadata of a report from its content as early as possible in the reporting process will help to provide the strongest possible anonymity for the user *within* the system if absolute anonymity *from* the system is not available.

Metadata are defined as 'data that provide information on other data', such as the time the report was sent, who it was sent by and from which device it was sent.[45] Content comprises the information on what is being reported – essentially the crime report describing what has happened, where and who has been involved.

Within any system, content and metadata may remain tied together, so that one is always visible to an operator who accesses the other, or they may be separated and stored separately, so that a system operator sees only the part of the information they need to see to complete the current action. In the example of Crimestoppers, some metadata (such as the IP address used by the device from which the report is made) are separated from the content by the encryption software, and further metadata (such as the time at which the report is made) are separated by the process through which Crimestoppers passes information on to the police. By the time the report is received by the police, none of the original metadata remain, and thus there is a negligible likelihood of the content revealing the primary identity of the person who made the report. This depends on two separate (and deliberately separated) systems, however: one encrypted and operated by Crimestoppers, through which the report is received; the other operated by the police services to which some of the information provided by that initial report is forwarded.

If absolute anonymity is not necessary or practical, however, metadata and content can still be separated – the content becomes pseudo-anonymised. This is usually achieved by attaching a tag to the content that can link the two 'halves' back together at a later stage. For example, content may be labelled as coming from 'Reporter 001', with a separate record linking Reporter 001 back to that user's primary identity. This may require data to be stored in three separate parts of the system: the metadata in one place; the content in another; and the data linking the content and its metadata back together in a third. This will help to provide confidence that an operator will not be able to determine the primary identity of Reporter 001 from their data, while other operators with higher system privileges may be able to identify them when required. This is a simplification of the system used by confidential crime reporting platforms such as that of the Metropolitan Police.

As metadata are often captured automatically, the separation of metadata and content inside the system is likely to be extremely important if the system is to offer the perception and reassurance of relative anonymity in the context of witness protection to its users.

Conclusions

It is clear that despite the concerns raised during the Independent Surveillance Review, anonymous crime reporting is possible in the Digital Age, but it comes at a high operating cost dependent on sophisticated encryption and robust operating processes. Deciding the extent to which anonymity is necessary and furthermore which level of anonymity – absolute or relative – is necessary and desirable in future online crime reporting platforms depends on whether the aim is to provide anonymity of the platform user from the system, including what information the platform captures from the user at the time of registration and how much this enables them to be identified by the system operators and the system itself; anonymity of the device used to report from the system including what, if any, information the platform captures at the point when a report is made that might be used to identify the device from which the report was made, and the extent to which this could this be used to identify the person who made the report; pseudo-anonymisation of data submitted to the system within the system, including whether or not all data submitted to the platform are stored in one place or some data are separated from others, so that a user may be anonymous in some parts of the system but not to the system as a whole; trust in data submitted under a promise of anonymity or confidentiality in which the identity or anonymity of the individual submitting the data influences how these data are received by the operators of the platform and how the system operators and the system itself can trust anonymous reports; and legal status of anonymous crime reports in criminal investigations and prosecution. If anonymous reports cannot be used as evidence in court, and the provision of anonymous reporting prevents the individual who submitted the information from being traced, there needs to be sufficient value in the information provided by the anonymous reporter to make its collection worthwhile.

The benefit of (perceived) anonymity is that people may feel less at risk and thus be more willing to disclose (more) information. The challenges are that the information they disclose may be of poorer quality: they may abuse the system. Law enforcement agencies may not be able to follow up with them to ask for additional information or clarification. What they give to Crimestoppers can only ever be information and can only support evidence found elsewhere, often as a direct result of that information. Anonymous evidence may not be admissible in court and thus will not itself lead to a prosecution. It is therefore important to consider not only whether anonymous reporting should be enabled through crime reporting platforms, but also *how* that anonymity can be enabled to provide the greatest benefit to all parties.

There are a number of ways in which anonymity or relative anonymity can be provided. Future platforms will have to weigh these against one another to decide whether, on balance, there is sufficient value in anonymous reporting to justify building the functionality that will enable it into the system. This will depend on how valuable reports made anonymously to law enforcement agencies and their partners are considered to be and how important anonymity is to the platform's potential users.■

Jennifer Cole is an Associate Fellow Resilience and Emergency Management at RUSI. She holds a PhD in Computer Science from Royal Holloway, University of London.

Alexandra Stickings is a Research Analyst in Resilience at RUSI. Her research interests include community policing, urban security and space policy and security.

Notes

[1] See Ofcom, 'The UK is Now a Smartphone Society', 6 August 2015, <https://www.ofcom.org.uk/ about-ofcom/latest/media/media- releases/2015/cmr-uk-2015>, accessed 19 January 2017.

[2] See J Hirby, 'How to Stay Anonymous When Reporting Drug Dealing', The Law Dictionary, <http://thelawdictionary.org/article/how-to-stay-anonymous- when-reporting-drug-dealing/>, accessed 20 October 2016.

[3] Jennifer Cole, Alexandra Stickings and Jon Betts interview with Adrian Tudway, Crimestoppers representative, London, 9 August 2016. Betts is a former detective superintendent and previously worked for the Home Office Centre for Applied Science and Technology. He is a consultant working with RUSI on the TRILLION project.

[4] PA Consulting Group and College of Policing, 'Digital Investigation and Intelligence: Policing Capabilities for a Digital Age', April 2015, <http:// www.npcc.police.uk/documents/ reports/Digital%20Investigation%20 and%20Intelligence%20Policing%20 capabilities%20for%20a%20digital%20 age%20April%202015.pdf>, accessed 27 February 2017.

[5] 'The Future of Policing in the Digital Age', conference held at RUSI, London, 21 June 2016.

[6] Further information about TRILLION – Trusted Citizen – LEA Collaboration Over Social Networks is available on the project's website, <http://trillion- project.eng.it/>, accessed 27 February 2017.

[7] Further information about the Metropolitan Police's Confidential Anti-Terrorist Hotline can be found at <https://secure.met.police.uk/ athotline/>, accessed 27 February 2017.

[8] For instance, see the Metropolitan Police's Online Crime Reporting platform, <https://online.met.police. uk/>, accessed 27 February 2017.

[9] For further information, see <http:// www.sarsas.org.uk/anonymous- reporting/>, accessed 27 February 2017.

[10] For further information, see <http://tellmamauk.org/>, accessed 27 February 2017.

[11] For further information about Crimestoppers, see <https:// crimestoppers-uk.org/>, accessed 27 February 2017.

[12] For further information about the Self Evident app, see <https://www. witnessconfident.org/self-evident-app>, accessed 27 February 2017.

[13] For further information about Facewatch, see <https://www. facewatch.co.uk/cms>, accessed 27 February 2017.

[14] Panel of the Independent Surveillance Review, 'A Democratic Licence to Operate: Report of the Independent Surveillance Review', *RUSI Whitehall Reports*, 2-15 (July 2015).

15 Heike Goudriaan et al., ‘Reporting to the Police in Western Nations: A Theoretical Analysis of the Effects of Social Context’, *Justice Quarterly* (Vol. 21, No. 4, 2004); Juha Kääriäinen and Reino Sirén, ‘Trust in the Police, Generalized Trust and Reporting Crime’, *European Journal of Criminology* (Vol. 8, No. 1, 2011); Jochem Tolsma et al., ‘When Do People Report Crime to the Police? Results from a Factorial Survey Design in the Netherlands, 2010’, *Journal of Experimental Criminology* (Vol. 8, No. 2, June 2012), pp. 117–34.

16 Carolyn Stone and Madelyn L Isaacs, ‘Involving Students in Violence Prevention: Anonymous Reporting and the Need to Promote and Protect Confidences’, *NASSP Bulletin* (Vol. 86, No. 633, December 2002).

17 Tolsma et al., ‘When Do People Report Crime to the Police?’.

18 Stone and Isaacs, ‘Involving Students in Violence Prevention’.

19 Tolsma et al., ‘When Do People Report Crime to the Police?’.

20 Sarah C Nicksa, ‘Bystander’s Willingness to Report Theft, Physical Assault, and Sexual Assault: The Impact of Gender, Anonymity, and Relationship With the Offender’, *Journal of Interpersonal Violence* (Vol. 29, No. 2, 2014).

21 Cole, Stickings and Betts interview with Tudway.

22 Tony Jefferson, ‘Policing the Riots: From Bristol and Brixton to Tottenham, via Toxteth, Handsworth, etc’, *Criminal Justice Matters* (Vol. 87, No. 1, 2012), pp. 8–9.

23 Cole, Stickings and Betts interview with Tudway.

24 See <http://www.asbos.co.uk/ AboutASBOs.aspx>, accessed 27 February 2017.

25 See, for example, Tuckers Solicitors, ‘Defendant Anonymity in Sexual Offence Cases in the UK’, 18 September 2014, <https://www.tuckerssolicitors. com/defendant-anonymity-sexual- offence-cases-uk/>, accessed 9 March 2017; and Joshua Rozenberg, ‘The Dilemma Over Anonymous Evidence’, *Daily Telegraph*, 25 June 2008.

26 See, for example, SeeHearSpeakUp, ‘Protecting Data Privacy in Global Whistleblowing Schemes’, 5 April 2016, <https://www. seehearspeakup.co.uk/en/blog/ item/160-protecting-data-privacy- in-global-whistleblowing-schemes>, accessed 9 March 2017; and Audit and Risk, ‘Concerns for Whistleblowers Under New EU Law’, 15 April 2016, <https://auditandrisk.org.uk/news/ concerns-for-whistleblowers-under- new-eu-law->, accessed 9 March 2017.

27 Alex Leavitt, ‘“This is a Throwaway Account”: Temporary Technical Identities and Perceptions of Anonymity in a Massive Online Community’, in Dan Cosley et al. (eds), *CSCW’15: Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work and Social Computing* (New York, NY: ACM, 2015), p. 317.

28 Cody Buntain and Jennifer Golbeck, ‘Identifying Social Roles in Reddit Using Social Network Structure’, in Chin- Wan Chung et al. (eds), *WWW ’14 Companion: Proceedings of the 23rd International Conference on World Wide Web* (New York, NY: ACM, 2014), pp. 615–20.

29 Adam N Joinson, ‘Self-Disclosure in Computer-Mediated Communication: The Role of Self-Awareness and Visual Anonymity’, *European Journal of Social Psychology* (Vol. 31, No. 2, March/April 2001), pp. 177–92.

30 Leavitt, ‘“This is a Throwaway Account”’.

31 Cole, Stickings and Betts interview with Tudway.

32 See European Parliament and Council of the European Union, ‘Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 Establishing Minimum Standards on the Rights, Support and Protection of Victims of Crime, and Replacing Council Framework Decision 2001/220/JHA’, *Official Journal of the European Union* (L 315/57, 14 April 2012). This directive replaced the 2001 Framework Decision on the standing of victims in criminal proceedings.

33 See respectively the website for Crimestoppers, <https:// crimestoppers-uk.org>, and the website for Meld Misdaad Anoniem, <www. meldmisdaadanoniem.nl>, accessed 27 February 2017.

[34] See Crime Stoppers International, <http://csiworld.org/>, accessed 27 February 2017.

[35] See SurveyMonkey, <www. surveymonkey.co.uk>, accessed 27 February 2017.

[36] Cole, Stickings and Betts interview with Tudway.

[37] Angela H Jiang et al., 'A Cliq of Content Curators', in Fabián E Bustamante et al. (eds), *SIGCOMM'14: Proceedings of the 2014 ACM Conference on SIGCOMM* (New York, NY: ACM, 2014).

[38] Cole, Stickings and Betts interview with Tudway.

[39] Panel of the Independent Surveillance Review, 'A Democratic Licence to Operate'.

[40] European Parliament and Council of the European Union, 'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)', *Official Journal of the European Union* (L 119/1, 4 April 2016), p. 5.

[41] Cliff Lampe and Paul Resnick, 'Slash(dot) and Burn: Distributed Moderation in a Large Online Conversation Space', in Elizabeth Dykstra-Erickson and Manfred Tscheligi (eds), *CHI '04: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (New York, NY: ACM, 2004), pp. 543–50.

[42] See TechTerms, 'Username', <http:// techterms.com/definition/username>, accessed 12 July 2016.

[43] See RUSI, 'Welcome to RUSI.org', <https://my.rusi.org/sslpage. aspx?pid=406&bm=-1084586396>, accessed 19 January 2016.

[44] Frederic D Stutzman and Woodrow Hartzog, 'Boundary Regulation in Social Media', in Steven Poltrock et al. (eds), *Proceedings of the ACM 2012 Conference on Computer Supported Cooperative Work* (New York, NY: ACM, 2012).

[45] For further information, see Cabinet Office, 'e-Government Metadata Standard', Version 3.1, August 2006, p. 6, <http://www.nationalarchives. gov.uk/documents/information- management/egms-metadata-standard. pdf>, accessed 20 February 2016.