THE ENCRYPTION DILEMMA: ATTEMPTING TO RESOLVE THE UNRESOLVABLE

BY
KEITH
MARTIN

Professor of Information Security, Department of Information Security and Director of the EPSRC Centre for Doctoral Training in Cyber Security for the Everyday, Royal Holloway, University of London.

TechREG CHRONICLE
JANUARY 2024

Visit www.competitionpolicyinternational.com
for access to these articles and more!

WHO CONTROLS YOUR PHONE: CLIENT-SIDE SCANNING AND THE FUTURE OF OWNERSHIP

By John Bergmayer

The swift rise of Generative AI has brought notable benefits to consumers. Despite this, rising concerns about potential harms and a surge of U.S. litigation, threaten AI's continued progress. This article examines ongoing legal challenges against OpenAI and Stability AI, underlining the unresolved legal issues AI providers face. A close look at these cases shows that fears surrounding Generative AI's alleged consumer harms do not present new legal dilemmas. Existing legal frameworks effectively filter out baseless claims unrelated to Generative AI's nature. Instead, this article argues that lawmakers should focus on promoting the advancement and deployment of Generative AI rather than altering current legal structures to facilitate its demise.

Scan to Stay Connected!

Scan here to subscribe to CPI's **FREE** daily newsletter.

© 2024 Competition Policy International® All Rights Reserved

In September 2023, the UK's controversial Online Safety Bill passed its final Parliamentary debate and is set to become law. Technology Secretary Michelle Donellan declared that "Today, this government is taking an enormous step forward in our mission to make the UK the safest place in the world to be online."[2] Meanwhile Meredith Whittaker, president of Signal, suggested that the implications of the Online Safety Bill for security of the messaging service her company provides could be serious enough that Signal might leave the UK.[3] Safety or security? Do we really have to choose between them?

To be clear, the intentions behind the Online Safety Bill are sound. The internet has created a world where information has never been easier to obtain from anywhere, by anyone. However, a serious downside of this mass availability of data is that content deemed undesirable has never been easier to obtain from anywhere, by anyone. The Online Safety Bill places obligations on digital technology companies to take responsibility for undesirable content by seeking and removing it, or preventing it from being posted onto their platforms in the first place. This sounds like a noble aspiration, one that will surely be lauded by, amongst others, parents of young children. Right?

Alas, there is a catch – on this issue there always will be. This catch concerns encryption, the technology at the center of controversy behind the Online Safety Bill. And the problem with encryption is hard-wired into its very nature: encryption works and has never been easier to use from anywhere, for anyone.

01
ENCRYPTION

Almost all aspects of life now have a digital component, hence cyber security controls are critical to ensuring that digital services operate as intended. Right at the heart of all technological aspects of cyber security are cryptographic controls. Cryptography essentially provides a toolkit of fundamental techniques for providing core security services such as confidentiality (the ability to prevent unauthorized viewing of data), data integrity (the ability to detect modification of data), data origin authentication (the ability to determine the original source of data) and entity authentication (to establish who is involved in a live communication session). Almost everything we engage in digitally relies on a combination of different cryptographic controls being applied. For example, mobile call protection uses cryptography to provide confidentiality (to prevent eavesdropping), data origin authentication (to ensure the validity of critical signaling data) and entity authentication (to clarify who is making the call and to ensure that they are connected to a legitimate mobile base station).

Confidentiality is one of the most important security services, required in any situation where we wish to protect sensitive data from being viewed by unauthorized parties, such as when using secure Wi-Fi, online banking, database protection, secure web browsing and secure messaging services such as WhatsApp and Signal. Confidentiality is provided by encryption techniques. We need encryption whenever we wish to prevent anyone (from anywhere) obtaining information that we are storing or communicating. In other words, encryption enables the keeping of digital secrets.

02
THE MARY QUEEN OF SCOTS PROBLEM

What encryption does is to render data unreadable to anyone other than an intended recipient. But what happens if someone else, shut out by encryption, claims to have a legitimate argument for accessing the data? Or, to use contemporary parlance, what happens if the data being protected is deemed "undesirable" content?

One complicating factor is, of course, under what terms is data deemed undesirable content, and by whom? Encryption has been used throughout history to protect secrets. Famously, the imprisoned Mary Queen of Scots used encryption in the Sixteenth Century to protect the content of letters she exchanged with co-conspirators seeking to overthrow Elizabeth I from the English throne and restore the nation to Catholicism. Whether the content of Mary's letters was undesirable very much depended upon which side of the political/religious divide you lay. For some, not the least Mary, this content represented matters concerning justice, inheritance, and restoration, requiring the highest level of confidentiality. For others, this content was treasonable. Who was right? Who got to decide?

[2] https://www.gov.uk/government/news/britain-makes-internet-safer-as-online-safety-bill-finished-and-ready-to-become-law.

[3] Signal is not leaving quite yet, following a late concession: https://www.wired.co.uk/article/britain-admits-defeat-in-online-safety-bill-encryption.

© 2024 Competition Policy International® All Rights Reserved

In the end, Elizabeth got to decide. Her experts broke the encryption (which was decent for its time, but nowhere near as good as the encryption we use today) and Mary was executed. England remains a Protestant nation, but this story could easily have had a different ending.

This conflict of opinion is just as prevalent today. Encryption is used, prolifically, to protect digital content. Just as in Mary's time, some people, in some situations, might deem some of this content to be undesirable. I think we would all mostly agree that certain content, such as images of child pornography, is almost unequivocally undesirable, although this cannot be agreed internationally since is there is no global agreement on what age childhood legally ends. However, despite the fact that much of the narrative relating to the Online Safety Bill has been about protection of children, the bill itself deals with the more abstract notion of "illegal" content, seemingly including content concerning more subjective and politicized concepts. For example, the UK Government has stated explicitly that technology firms would be required to deem any data appearing to represent a positive perspective on illegal migrant boats crossing the English Channel as undesirable content,[4] which is an issue that many UK citizens might not agree with.

What content is undesirable and who gets to decide? In the UK, it seems that the government sees itself as the guardian of such decisions. James Baker of the Open Rights Group has expressed concerns that the Online Safety Bill will "undermine the freedom of expression of many people in the UK."[5] While his concerns may indeed prove legitimate, this issue is substantively graver in parts of the world currently more hostile to freedom of expression than the UK There are countries, which need not be explicitly named, where simply raising a whispered voice of opposition to the government in power might be regarded as the creation of undesirable content. In such nations, encryption protects the digital activities of the slim remnants of civil society, including the communications of journalists, opposition politicians and non-governmental bodies. Here, the Mary Queen of Scots Problem is even more starkly demonstrated than in the UK. In such situations, as for Mary, encryption may govern, quite literally, matters of life and death.

03

THE ENCRYPTION DILEMMA

Whenever encryption is used there tends to be someone, for whatever reason, who wants to overcome the protection that it provides - why use encryption otherwise? Back in Mary's day, however, the scenario was simpler than today: Mary deployed her own encryption method to protect her information and her enemies then tried to break it. Similarly, during the Second World War, nations on both sides of the conflict deployed their own encryption technologies, and each tried to break those of the enemy (most famously the Enigma technology deployed by the Nazis was famously defeated by the ingenuity of Polish and British cryptanalysts). Importantly, breaking the likes of Enigma had no impact on the protection of Allied communications. Defeating the enemy's encryption was a battle won, and many attribute the overcoming of Enigma to a shortening of the Second World War.

After the war, this situation changed dramatically. The rise of networked computers steadily gave rise to the incredible digital world that we live in today. Encryption has been partially responsible for realizing this, since without digital security techniques it is unimaginable that we could deploy computers for their myriad contemporary uses. The problem we have today that differs notably from the situation during the Second World War is that everyone is using the same shared communication systems and the same associated encryption technologies. Even if we could agree who the enemies are in today's digital world, both we and our enemies share the same networks (Wi-Fi, mobile telecommunications, etc.), most importantly the internet. Consequently, and significantly, we use the same encryption technologies as our enemies do. Indeed the fact that the same encryption techniques can be used for both good and harmful purposes has long been recognized, with encryption technology classified as a dual-use good under the Wassenaar Arrangement.[6]

So here is the dilemma. If someone, for whatever (legitimate) reason, wants to overcome the protection provided by today's encryption technologies, then anything they are able to do to overcome that protection represents a weakening of everyone's digital security. If someone breaks today's versions of Enigma, then they also break the security of the likes of Wi-Fi, mobile telecommunications, and the internet. The dilemma is that encryption works, for everyone. If it is engineered not to work for some then, strictly speaking, it does not work for anyone.

[4] https://www.computerweekly.com/news/366552774/Parliament-passes-sweeping-online-safety-bill-tech-companies-still-concerned-over-encryption.

[5] https://www.openrightsgroup.org/press-releases/org-warns-of-threat-to-privacy-and-free-speech-as-online-safety-bill-is-passed/.

[6] https://www.wassenaar.org/.

© 2024 Competition Policy International® All Rights Reserved

04
ALGORITHMS AND KEYS

Before reflecting on some past approaches to addressing the encryption dilemma, a quick encryption primer might be helpful. Encryption provides the digital equivalent of a physical lock, enabling data to be secured away from prying eyes. Just like a physical lock, encryption involves two separate components. An encryption algorithm is the equivalent of a locking mechanism. Just like most locking mechanisms, most encryption algorithms are well understood, standardized, and are shared by many different applications (just as the same locking mechanism is likely be installed on every door of a block of flats). In fact the vast majority of daily uses of encryption rely on one single encryption algorithm, the Advanced Encryption Standard ("AES"), whose details are published and readily obtained.

For physical locks, what differentiates one instantiation from another is not the locking mechanism itself, but that different instantiations require different keys to open the locking mechanism. Likewise, while many applications use the AES encryption algorithm, what distinguishes the genuine recipient of an AES-encrypted message from anyone else is knowledge of a unique digital (decryption) key. Thus, for example, billions of mobile phones users around the world use the same encryption algorithm to protect their calls, but each of these mobile phone users has a unique digital key stored on a SIM card in their phone. The strength of security provided by encryption is associated with the length of these keys, since the more possible keys there are, the harder it is to try them all out.

05
BRIEF HISTORY OF IMPERFECT APPROACHES

The UK's Online Safety Bill is far from the first attempt around the world to address the encryption dilemma. Indeed, ever since the Second World War there has been a constant battle (some have even deemed it a "Crypto War")[7] over how to develop approaches that enable encryption to be used for good purposes whilst enabling its protection to be overcome when the same encryption is used to protect perceived harms. All of these approaches tend to have three things in common – they are controversial, far from perfect and are, at best, temporary approaches that evolving circumstances soon render inappropriate.

Arguably the earliest approach to overcoming the encryption dilemma arose after the Second World War, when there was an increase in demand from governments around the world for encryption technology to protect their communications. At that time there was limited global expertise and very few suppliers of quality encryption hardware devices. Suppose a global military-grade encryption hardware supplier located in Country A, which has good geopolitical relationships with powerful Country B, receives an order from Country C that Country B has a more distant relationship with.[8] The encryption dilemma presents itself as follows: Country A wants to appear to be selling a top-quality product to Country C, but Country B would like access to the communications that this technology is going to protect. The historical approach to addressing this dilemma was to sell Country C hardware containing the military-grade encryption algorithm, but to rig the accompanying technology that generated the digital keys in such a way that these keys could easily be determined by Country B. This solution only worked through Country C's naivety and inability to assess the effectiveness of the purchased product. It essentially only worked because there was insufficient global cryptographic expertise at that time to detect the fraud.

Deploying rigged encryption hardware ceased to be a viable option as we moved into the 1970s and 1980s for two reasons. Firstly, encryption started to be used on a wide scale in commercial environments, particularly in the financial sector, where deploying dodgy technology was clearly not viable. Secondly, global cryptographic expertise outside of government agencies started to grow, meaning that encryption technologies became subject to significant public scrutiny. Increased use of encryption technology around the world also heightened the encryption dilemma. The main approach adopted at this time by governments around the world was to subject encryption technology to import and export controls. This was feasible because encryption was deployed in hardware devices, which could be controlled at borders. This meant that any government could prevent export and import of any product whose key length offered what that government perceived at the time to be "too much" security.

During the 1990s and the early expansion of the internet, this regulatory approach ceased viability as encryption became widely available in software, a commodity impossible to control at physical borders. Instead the U.S. Government (and others) attempted to introduce centralized control of

[7] https://en.wikipedia.org/wiki/Crypto_Wars.

[8] For one such scenario, see: https://www.theguardian.com/us-news/2020/feb/11/crypto-ag-cia-bnd-germany-intelligence-report.

use of encryption technology by proposing a key escrow system, whereby users of encryption would need to lodge copies of their keys with trusted agencies. If protected content was later deemed undesirable, under warrant these agencies would release the relevant keys to appropriate authorities. This cumbersome approach to addressing the encryption dilemma seems preposterous from today's perspective, but the fact that it was even contemplated shows how seriously the encryption dilemma was considered. Key escrow was not well received at the time and ultimately defeated, deemed unworkable by, amongst others, technology companies who were trying to expand their international markets rather than have them constricted by systemic controls.

And so we moved into the Twenty-first Century and a booming internet with strong encryption widely deployed. Yet, the encryption dilemma remained, with no apparent approach in play to address it.

06

THE SNOWDEN BOMBSHELL

In 2013, former National Security Agency contractor Edward Snowden released a mass of classified information that revealed, amongst many other things, many different ways that some intelligence agencies had been using to address the encryption dilemma. What we essentially learnt from Snowden was not just that the encryption dilemma remained a problem that governments were trying to tackle, but that they were adopting almost any means possible to do so.

The Snowden revelations largely acted as a wakeup call regarding the complexity of our modern digital ecosystem, which relies on uncountable systems and networks, complex supply chains, multiple suppliers of technology, and mass generation of potentially valuable (and occasionally undesirable) data. The encryption dilemma was seemingly being addressed through a messy combination of deals with technology companies, interference in backbone networks, deploying vulnerabilities, essentially whatever it took. This included exploiting poor implementation of encryption, weaknesses in key management and seeking data at its endpoints (before encryption or after decryption). Every technique deployed to overcome the protection offered by encryption also represented a weakness in our overall digital security.

The fallout from Snowden's revelations was a significant introspection as to how we build security into our digital systems. One response has been the rise in popularity of secure messaging services offering end-to-end encryption, meaning that there is no capability for anyone other than the genuine sender and receiver to decrypt the protected data, including the messaging service provider itself. This, in turn, has given rise to regular calls for secure messaging services to weaken their security somehow, or to be subject to legal controls. Which, of course, is precisely where the Online Safety Bill attempts to wade in, leaving controversy in its wake. How, indeed, can a technology company take responsibility for undesirable content by seeking and removing it, or preventing it from being posted onto their platforms in the first place, when they are deploying strong encryption for security purposes that makes this task nigh on impossible? To be clear, what these technology companies are being asked to do is resolve the unresolvable encryption dilemma.

07

A LOOK INTO THE FUTURE

There are two truths worth keeping in mind before we consider any prognosis for the future.

Firstly, debates about safety versus security concern a false dichotomy. Cryptography in general, and encryption in particular, underpins digital security. Without encryption, we, and our children, cannot be safe online. Online safety cannot possibly arise from online insecurity.

Secondly, the encryption dilemma is unresolvable. All attempts to do so are imperfect and ephemeral. We will be ruminating over the encryption dilemma forever, and certainly long after the Online Safety Bill has faded from the legislature.

So what prognosis for the latest milestone in the history of the Crypto Wars, the Online Safety Bill? I have no idea, but let me play with three imagined futures.

Authoritarianism? The Online Safety Bill has real bite and the UK Government places enormous pressure on technology companies to redact some of their current digital security measures. This might mean, for example, storing copies of keys protecting all digital content, intensively monitoring all digital content before enabling it to be encrypted, or even creating separate access channels to enable law enforcement to monitor data sent on their platforms. Companies who pride themselves in supporting strong digital security, such as Signal, eventually withdraw from the UK market. The citizens of the UK graciously accept a reduction in their digital security, freedom of expression, and technology market choice in order to allow

© 2024 Competition Policy International® All Rights Reserved

the technology providers and the government of the day to determine precisely which digital content is desirable and which digital content is not.

This future seems unlikely as the likes of Signal have already been given some reassurance that the proposed measures, for now, will not be enforced against their end-to-end encryption services. I struggle to imagine this future ever really panning out.

Crypto-anarchy? Once the practical consequences of the power of the Online Safety Bill are better understood following some high-profile withdrawals of service providers from the UK, the media stirs up further controversy and there is some backlash from the public. The public adopt open source encryption products to protect their communications, including tools supporting a degree of anonymity such as Tor. There are widely-publicized campaigns against a so-called Big Brother state, and the UK Government is forced to consider a major revision of relevant legislation.

Hmmm… pretty unlikely. The public response to the Snowden revelations was barely audible – I do not see a crypto revolution coming anytime soon.

Business as usual? The Online Safety Bill's wording and surrounding rhetoric continues to make some people uncomfortable, but there is no serious attempt made to force all service providers to weaken their digital security. The Online Safety Bill serves as a declaration of intent to tackle content deemed undesirable and to seek co-operation of content providers when appropriate. Some content providers amend their practices to tighten up on processes for responding to certain types of content appearing on their platforms, while others do not. There is an occasional prosecution, or at least a threat to do so. The legislation is not debated much in the media expect when issues flare up over undesirable content that is, inevitably, still appearing on digital platforms. Life rumbles on.

Given the late non-enforcement concession to the likes of Signal, the early signs are that some version of this prognosis seems most likely. Pragmatism wins the day.

There may well be other possible futures. And, of course, I may well not be correct in my deductions. What I am certain about, is this. However the Online Safety Bill pans out, it is just one episode in an unfolding story which, since the encryption dilemma is unresolvable, will never have an ending.

> “*Business as usual? The Online Safety Bill's wording and surrounding rhetoric continues to make some people uncomfortable, but there is no serious attempt made to force all service providers to weaken their digital security*

08 CONCLUSION

The controversy over the UK's Online Safety Bill needs to be placed in historical perspective, alongside previous regulatory attempts to respond to the encryption dilemma. This is not a debate about safety versus security, and neither is it really a discussion about cryptography. By acting as the enabler of digital secrets, encryption is only a facilitator, not the central issue. What this matter really concerns is where power lies in society. Who gets to keep secrets, and from whom? Should freedom of expression have boundaries? If so, where are they and who decides upon them? And who governs digital information – the state or the technology providers? These are age-old questions and they will never have universal answers. Of course, this does not mean that we, as a society, should not try to address them. However, we, as a society, should also be mindful that we are attempting to resolve the unresolvable, and must be prepared for the complexity and messiness that will inevitably unfold.

© 2024 Competition Policy International® All Rights Reserved

CPI SUBSCRIPTIONS

CPI reaches more than **35,000 readers** in over **150 countries** every day. Our online library houses over **23,000 papers**, articles and interviews.

Visit competitionpolicyinternational.com today to see our available plans and join CPI's global community of antitrust experts.

© 2024 Competition Policy International® All Rights Reserved

CPI COMPETITION POLICY® INTERNATIONAL