Encryption: What's The Problem?

Dr Victoria Baines, IT Livery Company Professor of IT

14th February 2023

On St Valentine's Day, February 14th, we may be in the mood for romance. That mood may be enhanced with music and lighting, and rather spoiled by the thought that someone else might be able to read messages intended for the object of our affection. We may not want our parents, our siblings, our children to see these, for fear of embarrassment. So how might we feel about the idea of them being intercepted by the government, or by an employee of a social media company?

A (Very) Brief History of Cryptography

For thousands of years, people have practised the art of cryptography, writing in code or cipher to keep their communications secret, and the science of encryption, which is how we encode that information. According to the Roman historian Suetonius, Julius Caesar used a substitution cipher, which shifted the letters of the plain text of his communications one by one.

"If he had anything confidential to say, he wrote it in cipher, that is, by so changing the order of the letters of the alphabet, that not a word could be made out. If anyone wishes to decipher these, and get at their meaning, he must substitute the fourth letter of the alphabet, namely D, for A, and so with the others."

— Suetonius, *Life of Julius Caesar* 56

A	B	C	D	E
F	G	H	I	K
L	M	N	O	P
Q	R	S	T	V
X	Y	Z	A	B

Note: The Roman alphabet had just twenty-three letters! Hence the repetition of A and B in the bottom right of the grid.

The problem with this kind of encryption, is that once you know how the substitution is made you can crack the whole message. And if the substitution instructions are not changed regularly, you can read all other messages encrypted in this way. As a result, over time cryptography became more complex. For instance, the Playfair cipher used by the British military in the early part of the 20th century split messages into pairs of letters that were then swapped according to their positions in a 5x5 grid:

F	W	Q	B	P
I	A	Z	T	K
E	C	O	X	H
R	L	Y	G	N
M	U	D	V	S

The Vigenère cipher applied a series of simple Caesar-style substitutions one after the other. Rotor machines, such as the Enigma machine used by German forces in the Second World War, performed this series of substitutions mechanically. Where encoded information had a potential value to someone other than its intended recipient, this gave rise to cryptanalysis, code breaking. One of the most celebrated examples of this is the Bombe project at Bletchley Park in the UK, which cracked the code used by operators of the Enigma machine.

Later in the twentieth century, digital encryption became the dominant method for concealing text, and its success was due largely to the increasingly complex algorithmic calculations that computers could quickly perform, over and above those that could be performed using pen and paper or rotor machines. Rather than keeping the keys and algorithms private, digital encryption has largely relied on public key exchange. In particular, the key exchange scheme published by Whitfield Diffie and Martin Hellman in 1976, and that is widely used to secure Internet communications, allows two parties not previously known to each other to generate a pair of keys – one public and one private. They can then share the public key with each other while keeping hold of the private key.

As we came to rely on the Internet for transfer of sensitive data including financial information, internationally recognised standards developed for encryption algorithms. Among these, the Data Encryption Standard (DES) used a 56-bit key to encrypt data, the Advanced Encryption System (AES) multiple rounds of encryption with 128-bit, 192-bit, or 256-bit keys, and Rivest–Shamir–Adleman (RSA) variable keys between 1024 and 4096 bits in length. Services using a recognised standard could reassure their customers and partner organisations that they were using the strongest security available. But because encryption was only possible when the message was in transit, as soon as the message reached the servers of the message platform, it could be read in the clear.

The solution proposed was End-to-End (E2E) encryption. As the name suggests, this encrypts the message for the entirety of its journey from the sender to the intended recipient(s). This means that even people working for the messaging service can't read it, because the version of the message 'at rest' on its servers is still scrambled.

On Secrecy, Privacy, and Surveillance

A saying often used in this context is, "If you have nothing to hide, you have nothing to fear." But this arguably confuses privacy with secrecy. Hiding suggests concealment for nefarious purposes, being dishonest or otherwise lacking in transparency, which is something that helps us to build trust with other people. But we all have things we want to keep to ourselves. Perhaps it's something in our past about which we now feel embarrassed; a thought that we worry might be shameful; an opinion with which others might not agree. Keeping things to ourselves can be an act of self-regulation: it can prevent us hurting other people or speaking inappropriately.

We may be asked to keep secrets for or about other people in order to protect them. Earlier in my career, I signed the UK Official Secrets Act, and was cleared to access documents marked Secret. The secrecy of the information to which I was privy was determined on the basis of national security. Sharing intelligence beyond a very strict circulation was deemed to pose a risk to the country. Far from being a threat to people, secrecy in this context was deployed in the interest of protecting them from harm.

Whatever is secret is kept from the knowledge of the public or from specific persons. It is either not allowed to be known, or is only allowed to be known by selected persons. Privacy, in contrast, is the "The state or

condition of being alone, undisturbed, or free from public attention, as a matter of choice or right; seclusion; freedom from interference or intrusion." (*OED*). Unlike secrecy, privacy is a human right, enshrined as Article 12 of the *Universal Declaration of Human Rights* proclaimed by the United Nations General Assembly in 1948:

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

The word 'arbitrary' is doing quite a lot of work here. It suggests that there may be times when interference with one's privacy is permitted, as long as it subject to certain restrictions and oversight. The *European Convention on Human Rights* probes these exceptions further. Article 8 of the Convention states that:

> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.

But also that:

> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The right to privacy is the reason the police need a warrant to search your house. They are not otherwise permitted to intrude on your private life and private space. The same applies – or at least should apply - to your communications and online activities. Generally speaking, in democratic countries with rule of law, a search warrant or similar legal order is required to compel phone companies, internet providers and social media platforms to disclose the content of your communications. Many government authorities also have the legal power to intercept your messages. In the digital equivalent of a telephone wiretap, they can effectively 'listen in' live to what you do and say online. This has relied precisely on the fact that data was encrypted when on the move between two different points, but not when it came to rest on the servers of the app or platform being used to send the message.

The fact that service providers can see your messages when they are at rest on their servers of course means that those communications are not completely private. Being able to read messages in the clear allows online providers like social media companies to identify what you are interested in, to serve you ads based on the content of your conversations. For the last decade at least, this kind of access has been a standard feature of the business model of Big Tech. While many of us may suspect that Facebook et al. are listening to our offline conversations through our phones, the more practical alternative has so far been to mine our text chats for keywords that correspond to products we may want to buy.

Information that is plain text or unencrypted is also vulnerable to unauthorised access. If someone is able to hack into the servers, they too can read our messages in the clear. Some of this information could be valuable to criminals, such as our dates of birth, home addresses, credit card and bank account numbers, passwords for a whole host of services. From a security perspective, encrypting data so that it is unreadable for the entire length of its journey makes a whole lot of sense. If message content is unreadable, it's of no value to the bad guys. It cuts off one major avenue for them to profit from our data and do us harm.

So, What's the Problem?

End-to-end encryption has become the new industry standard for messaging platforms because it provides great security. But it also presents a practical challenge. Because companies can no longer read the content shared on their platforms, they also can't identify when people are engaged in activity that violates their terms of service and/or breaks the law. And this is understandably a concern to governments who want to know when their citizens are committing serious crimes, of which their messages may provide crucial evidence. Consequently, safety advocates, police and intelligence agencies in many countries would rather E2E wasn't deployed at all on the most popular messaging apps and social media platforms.

In the first instance, it prevents service providers detecting illegal content using existing tools. Until now, service providers have relied on being able to scan the content of messages in order to identify serious crimes like sharing images and videos of child abuse or terrorist propaganda. Large scale, global mechanisms have developed that enable photos and videos assessed as clearly illegal to be given a unique signature or 'hash value', which allows this content to be identified and removed from many different apps,

and reported to law enforcement in many different countries.

This process is enshrined in US law, and some of the largest US-based platforms make millions of reports of suspected child abuse material to the National Center for Missing and Exploited Children (NCMEC). NCMEC then refers reports to law enforcement all over the world, on the basis that distributing, downloading and possessing images of child sexual abuse is itself a criminal offence in many countries.[1]

Secondly, government authorities cannot read someone's messages if they are E2E encrypted. They can still intercept the data themselves or request it from the company, but they cannot unscramble it so that it reads as plain text. Whether the latter is a good thing or a bad thing very much depends on your perspective. A parent of a child in a democratic country with rule of law may understandably want that child's safety to be prioritised above all else. A journalist who risks their life to report the truth under a repressive regime may depend on the privacy and security of their online communications simply to survive. Because encryption is either on for everyone or off for everyone, it's not possible for companies to decide that they will turn it on for journalists but not for criminals. There is also a further complication that – as we explored in the first lecture in this series - different countries do not always agree about what constitutes criminality. We have internationally accepted definitions of child abuse material, but not of terrorist content, and certainly not of prohibited speech. Our imagined journalist may in fact be considered a criminal simply for criticising the government.

Of Backdoors and Workarounds

One proposed solution has been to give government authorities keys to decrypt encrypted communications in exceptional circumstances, for example, where there is legitimate suspicion that a serious crime is being committed using the app in question. But as soon as we consider how that might work in practice, we have to admit that it also presents several challenges. And in the case specifically of E2E encryption, where the service providers themselves don't have keys to decrypt the messages, this would require vulnerabilities that don't currently exist to be built into the protocol specifically for the benefit of law enforcement and intelligence agencies.

We already have a real life example of this in the investigation into the December 2015 terrorist attack at San Bernardino, California. The FBI issued a court order demanding that Apple write software that would enable them to unlock the iPhone of one of the suspects. Apple opposed this order on the basis that this tool would create a backdoor to all iPhones, not just the one belonging to the suspect. In the event, the FBI gained access to the phone, reportedly with the help of a third party hacking service. And this raises further considerations about the impact and knock on effects of E2E encryption.

When technology presents obstacles, humanity has a way of finding workarounds. To get around the fact that E2E encryption makes message content unreadable for the entirety of its journey, a large number of governments have purchased software that effectively hacks into people's devices, the endpoints of communication, where content is still readable. Research in 2018 by the Canadian civil society organisation Citizen Lab (see Further Reading) found that Pegasus spyware produced by the Israeli company NSO Group had been installed on people's smartphones in 45 countries, precisely so their messages could be read in the clear. Although the company has claimed that the software is only intended for use against criminals and terrorists, targets have included French President Emmanuel Macron, Amazon founder Jeff Bezos, UAE-based human rights defender Ahmed Mansoor, murdered Mexican journalist Cecilio Peneda Birto, and Hanan Elatr, the widow of murdered Saudi journalist Jamal Khashoggi.

Data analysed by the Pegasus Project, a team of researchers from The Guardian, Le Monde, The Washington Post and other media partners identified a number of governments believed to be NSO customers, including Mexico, Saudi Arabia, Hungary, India and the United Arab Emirates.[2]

Some industry and government stakeholders have proposed a different, legitimate workaround that also exploits the fact that data is not scrambled on our devices. This is known as Client Side Scanning, and it uses the processing power of your phone, tablet or computer to scan for known child abuse material. When in August 2021, Apple announced that it would run just such a system on the Camera Roll in iCloud Photos,

[1] National Center for Missing and Exploited Children (2022), "2021 Reports by Electronic Service Provider (ESP)". https://www.missingkids.org/content/dam/missingkids/pdfs/2021-reports-by-esp.pdf
[2] https://forbiddenstories.org/case/the-pegasus-project/

this was met with approval from child protection advocates but consternation from leading privacy advocates, respected academics and people who had contributed to the development of public key cryptography. One of the concerns expressed was that Apple would come under pressure to point a workaround developed for a very specific use case to other types of content such as political speech or anti-government activities.

Technology with a backdoor in it is necessarily no longer as secure as it was. And for a back door ever to be proportionate, we would have to be assured that governments would never misuse it, that individual law enforcement and national security agents would have the utmost personal integrity at all times, and that large organisations have perfect oversight and control of who can access their systems and networks. It's impossible for us to be certain of any of these, because as we know from our explorations of internet governance and fake news (the first and third lectures of this series), different countries have different ideas about what is criminal or dangerous; that government authorities are made up of humans, and some humans break rules; also, that nothing is unhackable.

A War of Words

In October 2019, UK Home Secretary Priti Patel, US Attorney General William Barr, acting US Secretary of Homeland Security Kevin McAleenan, and Australian Minister for Home Affairs Peter Dutton sent an open letter to Facebook CEO Mark Zuckerberg concerning the company's plans to apply to E2E encryption to all of its services. It opened as follows [with emphasis added]:[3]

> We are writing to request that Facebook does not proceed with its plan to implement end-to-end encryption across its messaging services without ensuring that there is no reduction to user safety and without including a means for lawful access to the content of communications to **protect our citizens**.
>
> In your post of 6 March 2019, "A Privacy-Focused Vision for Social Networking," you acknowledged that "there are real safety concerns to address before we can implement end-to-end encryption across all our messaging services." You stated that "we have a responsibility to work with law enforcement and to help prevent" the use of Facebook for things like child sexual exploitation, terrorism, and extortion. We welcome this commitment to consultation. As you know, our governments have engaged with Facebook on this issue, and some of us have written to you to express our views. Unfortunately, **Facebook has not committed** to address our serious concerns about the impact its proposals could have on protecting **our most vulnerable citizens**.

The ministers saw only one viable solution to the problem, which was continued government access to people's messages in the clear. Facebook's failure to guarantee this is portrayed as endangering people. At no point do they acknowledge the impossibility of ensuring the security and integrity of E2E encryption while building in backdoors for government agencies. Indeed, statements such as "We support strong encryption", and "Law abiding citizens have a legitimate expectation that their privacy will be protected" only serve to highlight an approach that has been identified – correctly, in my opinion – as 'cakeism' by Ciaran Martin, the former head of the UK's National Cyber Security Centre (see Further Reading). The letter continues [emphasis added]:

> Companies should not **deliberately design** their systems to **preclude** any form of access to content, even for preventing or investigating the most serious crimes. This **puts our citizens and societies at risk by severely eroding** a company's ability to detect and respond to illegal content and activity, such as child sexual exploitation and abuse, terrorism, and foreign adversaries' attempts to **undermine democratic values** and institutions, **preventing** the prosecution of offenders and safeguarding of victims.

The Ministers clearly imply that i) the recipient of this letter has somehow been directly involved in the design of E2E encryption, which is untrue; ii) E2E encryption itself - as opposed to bad actors using it - puts citizens and societies at risk; and iii) platforms that deploy E2E are deliberately obstructing criminal justice and safeguarding. The letter closes with words that present the issue as a crisis point [emphasis added]:

> As you have recognised, it is critical to get this right for the future of the internet. Children's safety and law enforcement's ability to bring criminals to justice must not be **the ultimate cost** of Facebook

[3] US Department of Justice (2019) "Open Letter: Facebook's 'Privacy First' Proposals". https://www.justice.gov/opa/press-release/file/1207081/download

taking forward these proposals.

The debate is reduced to a binary choice between E2E on the one hand, and safe children and effective criminal justice on the other. The future of child safety and enforcement of law and order are depicted as hinging on Facebook's decision alone. One would be forgiven for thinking that Zuckerberg invented E2E encryption and that Facebook was the first major tech company to propose using it. He didn't, and it wasn't.

When a letter of reply appeared on Facebook's website in December 2019,[4] E2E was depicted instead as essential to people's safety rather than opposed to it [with emphasis added]:

> As the Heads of WhatsApp and Messenger, we are writing in response to your public letter addressing our plans to **strengthen** private messaging for our customers…**We all want people** to have the ability to communicate **privately and safely**, **without harm or abuse** from hackers, criminals or repressive regimes. Every day, billions of people around the world use encrypted messages to stay in touch with their family and friends, run their small businesses, and advocate for important causes. In these messages they share private information that they only want the person they message to see. And it is the fact that these messages are encrypted that forms the **first line of defense**, as it keeps them **safe** from cyber attacks and **protected** from falling into the hands of criminals. The core principle behind end-to-end encryption is that only the sender and recipient of a message have the keys to "unlock" and read what is sent. No one can intercept and read these messages - not us, not governments, not hackers or criminals.

Where the ministers depicted E2E encryption as a threat, Facebook casts the Ministers' demands in that role [emphasis added]:

> Cybersecurity experts have repeatedly proven that when you **weaken** any part of an encrypted system, you **weaken** it for everyone, everywhere. The 'backdoor' access you are demanding for law enforcement would be a gift to criminals, hackers and repressive regimes, creating a way for them to enter our systems and **leaving every person on our platforms more vulnerable to real-life harm**. It is simply impossible to create such a backdoor for one purpose and not expect others to try and open it. People's private messages would be **less secure** and the real winners would be anyone seeking to take advantage of that **weakened security**. That is not something we are prepared to do.

The mention of repressive regimes here raises an important point. Where the so-called "Five Eyes" ministers would doubtless consider their countries to be 'good' democracies, there is no way for tech companies to build an encryption backdoor that can only be used by 'good' countries, and no universally accepted, objective way to distinguish 'good' countries from 'bad' ones in any case. This was summed up very succinctly by Harvard cryptography lecturer Bruce Schneier in 2019: "You have to make a choice. Either everyone gets to spy, or no one gets to spy. You can't have 'We get to spy, you don't.' That's not the way the tech works."

In this very public exchange between some governments and one of the world's largest tech companies, E2E encryption is presented as simultaneously the most irresponsible choice and the most responsible; the safest and the least safe; the strongest and the most vulnerable; in citizens' best interests and their worst.

Speaking for Citizens vs. Asking Citizens

Both the Ministers and Facebook/Meta presumed to speak for citizens. But actually asking the public what they think gives rise to answers that reflect the complexity of the moral and ethical choices surrounding E2E encryption. There appears to be some public expectation that online communication be private. In 2016, a Reuters/Ipsos poll found that 46% of Americans agreed with Apple's decision to oppose the federal court order requiring them to unlock the phone of the San Bernardino suspect: 35% said they disagreed, while 20% said they did not know.[5] A 2019 YouGov survey in the UK and US found that 64% of respondents

[4] Facebook (2019) "Facebook's Public Response to Open Letter on Private Messaging". https://about.fb.com/wp-content/uploads/2019/12/Facebook-Response-to-Barr-Patel-Dutton-Wolf-.pdf

[5] Jim Finkle (2016) "Solid support for Apple in iPhone encryption fight: poll" *Reuters Technology News* 24/02/2016. https://uk.reuters.com/article/us-apple-encryption-poll/solid-support-for-apple-in-iphone-encryption-fight-poll-idUKKCN0VX159

believed that E2E encryption could help protect their digital privacy.[6]

In January of this year, The Sun newspaper very kindly launched a couple of online polls to explore these issues for us. We asked readers in the UK two questions. The first was 'Should Facebook encrypt all of your chats?' 15,570 votes were cast in just three days, split as follows:

Q. Should Facebook encrypt all of your chats?

Definitely	47% (7,437 votes)
No, absolutely not	28% (4,387 votes)
I'm not sure	24% (3,746 votes)

We then asked a second question, 'Should the government have access to your online chats?' 33,240 votes were cast as follows:

Q. Should the government have access to your online chats?

Yes they should	6.93% (2,302 votes)
No, absolutely not	84.02% (27,929 votes)
Hmm... I'm not sure	9.05% (3,009 votes)

What people's responses here arguably show is that the decision to deploy or not deploy E2E encryption is ethically complex, and not as straightforward as presented by some of the most ardent advocates for and against it. The people who voted 'I'm not sure' are as interesting as those whose opinions were certain. It is possibly the most difficult ethical decision the global community has faced in regard to information technology, prompting some to consider a utilitarian approach that seeks to identify the greatest good for the greatest number of people.

The Limits of Logic and Ethics

Since it is alleged that E2E encryption increases the risk to some members of society and reduces the risk to others, we may be tempted to apply a utilitarian evaluation, one that draws on Jeremy Bentham's philosophy of the Greatest Happiness for the Greatest Number. But a large scale cost/benefit analysis comes up against significant obstacles. We simply don't have the data to quantify people harmed versus people unharmed for the UK, and we certainly don't have them for the wider world.

Even where we do have partial data – for instance the reports of child abuse material made to NCMEC in the US by mostly US platforms – it's not possible for us to verify the direct impact of E2E encryption on report numbers until it is actually deployed, and even harder for us to quantify its impact on the safety of individual children. As Ian Levy and Crispin Robinson of UK intelligence agency GCHQ commented on the 29.4 million reports received in 2021 (see Further Reading):

> In the same year, the NCA [National Crime Agency] received 102,842 reports from NCMEC (accounting for the vast majority of reports from industry), but some of these were incomplete or, once investigated, not found to be child abuse. Of the 102,842 reports, 20,038 were referred to local police forces and started (or contributed to) investigations—in 2021 more than 6,500 individuals were arrested or made voluntary attendances due to offenses related to child abuse and more than 8,700 children were safeguarded.

Now, if we were to cynically evaluate these numbers statistically, we might come to the conclusion that this process is successful in safeguarding children in about 1 in 12 cases, and in identifying offenders in about 1 in 16. But that's an imprecise calculation for a number of reasons: reports could relate to more than one child; equally several reports could relate to a single child, and additional children could have been identified and

[6] Tresorit Team (2019) "Trust in Tech Giants is Broken" *Tresorit Blog* 24/04/2019. https://blog.tresorit.com/trust-in-tech-giants-is-broken/. Data provided by YouGov (2307 UK respondents, 1273 US, between 03/04/2019 and 05/04/2019.

safeguarded at a later stage in an investigation, over and above those linked to an initial report.

And in fact, the more we go down the route of trying to quantify harm, the more distasteful the endeavour becomes. Insisting on a tally of those harmed is understandably unacceptable to child protection specialists and child rights advocates, for whom each instance of child abuse and each child death is one too many. At the same time, arguments that pit child safety against privacy bully us into an unholy reckoning, forcing us to weigh the life of a child against the life of a human rights activist. As a human, as a citizen, I don't ever want to be put in that position. In fact, I object to it, particularly when different parties in the debate appear to underplay the fact that end-to-end encryption presents a wicked problem, one that cannot be solved by simple appeals to logic, ethics, or emotion.

Binary Code, Nuanced Considerations

So, is E2E encryption the best thing ever or the worst thing ever? This is arguably the wrong question. Whether secret communications are 'good' or 'bad' very much depends on perspective and context. For an intelligence agency, secrecy is a good thing, transparency a risk. For human rights activists concerned about government surveillance, secrecy is seen as counteractive to the greater transparency required to hold the authorities accountable. The ideal response – to aim for a balance between operational secrecy and transparency that is sufficiently accountable to the public, while protecting the techniques and assets of those charged with keeping us safe – is no simple feat to achieve.

And as soon as we accept that deployment of secure messaging is not simply a battle of absolute safety versus absolute privacy, we are confronted with the need to come up with solutions that also don't promise the impossible of absolute safety *plus* absolute privacy. This may in turn require a change of mindset: for governments to stop arguing with the laws of mathematics, and for all involved to take a longer view of the potential consequences. We may be relatively comfortable with the idea of government authorities intercepting our text messages or calls. But what about our eye movements, physical gestures, and thought patterns? A tool to decrypt encrypted communication might also give governments the future ability to read encrypted data generated on next-generation virtual and augmented reality platforms, and by brain-computer interfaces, all of which are already being developed. As the data collected on us becomes more and more intrusive, debate will intensify about how that data is processed, stored, and accessed by governments and companies alike.

So, tech companies will need to find new ways of keeping their users safe and demonstrating how they do that. Among these are user-centric tools like StopNCII, that empower people to restrict the circulation of intimate images they have shared in good faith.[7] Government agencies used to comparatively easy and regular access to the content of our communications will need to find new routes for evidencing online crimes – or perhaps return to the tried and tested method of using human investigators to infiltrate criminal groups active online. The criminal justice system may need to refocus its evidence gathering on suspects' and victims' devices.

Two thousand years ago, the Roman satirist Juvenal asked, *quis custodiet ipsos custodes?* – "Who will guard the guards themselves?". This maxim is still regularly applied to modern surveillance conducted by governments and tech companies. Oversight is only possible if authorities lift their customary secrecy to such an extent that it is possible to scrutinise their methods and hold them accountable. Likewise, companies may wish to protect their intellectual property because how they do what they do has a commercially competitive value. Making public what they do to make platforms more secure, e.g. how they identify criminals and terrorists, can also give bad actors valuable information on how to game their systems. But if they keep everything secret, we the people cannot judge if they are abusing their power or overstepping their bounds.

Paradoxically, it may be the opposite of privacy and secrecy – transparency – that helps us determine how to proceed with securing our communications and overseeing surveillance in the future.

[7] https://stopncii.org/how-it-works/?lang=en-gb

Resources

Some of the largest technology companies publish transparency reports, which include statistics on government requests for user data and removal of online content. Here are a few of them.

- Meta (formerly Facebook; includes WhatsApp and Instagram): https://transparency.fb.com/data/
- Google: https://transparencyreport.google.com/?hl=en_GB
- Microsoft: https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report
- Apple: https://www.apple.com/legal/transparency/
- Twitter: https://transparency.twitter.com/
- Snapchat: https://values.snap.com/en-GB/privacy/transparency
- TikTok: https://www.tiktok.com/transparency/en/reports/

A number of civil society organisations also publish reports on government access to digital communications. These include:

- The Electronic Frontier Foundation: https://www.eff.org/
- Privacy International: https://privacyinternational.org/
- Big Brother Watch: https://bigbrotherwatch.org.uk/

Further Reading

Hal Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Jon Callas, Whitfield Diffie, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller Bruce Schneier, Vanessa Teague, & Carmela Troncoso (2021) *Bugs in our pockets: The Risks of Client-Side Scanning*. https://www.cs.columbia.edu/~smb/papers/bugs21.pdf

Martin Kleppman & Mitch Seymour (2022) *Secret Colors: A gentle introduction to cryptography*, Round Robin Publishing.

Ian Levy & Crispin Robinson (2022) "Is It Possible to Reconcile Encryption and Child Safety?", *Lawfare*, July 21, 2022. https://www.lawfareblog.com/it-possible-reconcile-encryption-and-child-safety

Bill Marczak, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, & Ron Deibert (2018) *Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries.* https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

Ciaran Martin (2021) "Ex-security chief: the government must prove its encryption plans work—or abandon them", *Prospect*, November 23, 2021. https://www.prospectmagazine.co.uk/science-and-technology/ex-security-chief-ciaran-martin-gchq-government-encryption-plans-facebook-apple

Alec Muffet (2022) *A Civil Society Glossary and Primer for End-to-End Encryption Policy in 2022*. https://alecmuffett.com/alecm/e2e-primer/e2e-primer-web.html#the-purpose-of-encryption

Irina Raicu (2016) "Ethical Questions About Encryption", Markkula Center for Applied Ethics at Santa Clara University. https://www.scu.edu/ethics/focus-areas/technology-ethics/resources/ethical-questions-about-encryption/

Eric Roberts (n.d.) *The History of Cryptography*. https://cs.stanford.edu/people/eroberts/courses/soco/projects/public-key-cryptography/history.html

© Professor Victoria Baines 2023