Internet Society-Chatham House Roundtable on Encryption and Lawful Access

26 October 2017

"We all want to hear that there is an engineering solution, but there isn't."

Introduction

The debate surrounding lawful access to encrypted content is polarising and has no easy answer. Too often the public debate is over simplified into a general battle between those "for and against encryption". Additionally, the public debate frequently lacks appreciation of the intricacies of the digital communications and data storage landscape, and how it has evolved.

On 26 October 2017, the Internet Society and Chatham House convened an experts' roundtable under the Chatham House Rule[1] to deconstruct the debate[2] and explore ways to bridge two important societal objectives: the security of infrastructure, devices, data and communications; and the needs of law enforcement. The meeting brought together a diverse set of experts with different interests and perspectives, engaging them in an open and frank conversation. Participants included experts with backgrounds in law enforcement, policy, civil society, academia and the tech sector. This report summarises the conversation.

During the roundtable, experts proposed that the first step toward a more productive dialogue is to address knowledge and communications gaps between the law enforcement community and other key stakeholders, including technical communities, civil society and companies that offer encrypted services.

The participants also moved the conversation forward by successfully reframing the problem into several related challenges with different considerations. (This aspect is discussed in more detail below.) Additionally, participants highlighted an opportunity for technical communities and other stakeholders to help build capacity among law enforcement to identify other sources of information and alternative tools at their disposal, while preserving the protections provided by encryption. One path forward, identified at the meeting, would be to seek to agree on a set of foundational principles, acceptable to a broad range of stakeholders, to guide law enforcement investigations in the presence of encryption.

Participants emphasised that the role of encryption goes beyond privacy and that the debate about lawful access must include consideration of its impact on security, innovation and the economy. Encryption is a technology that is fundamental to e-commerce, government services and underpins trust in the growing digital economy. It is fundamental for securing critical infrastructure, communications and information for business and society. Some experts observed that, with innovation in artificial intelligence, quantum computing and the Internet of Things (IoT), encryption technologies—and our means of breaking them - are quickly changing.

Although the technology has changed, some participants recalled that many of the issues that are being discussed today are similar to those that were at the heart of the encryption debates of the early 1990s. Questions around how, when and under what circumstances law enforcement agencies should be able to access encrypted information remain contested. However, participants in the roundtable regarded identifying nuances and dividing the problem into manageable pieces and discussions as a step forward in the debate.

A participant noted that, in addition to public debate, discussions where experts can speak frankly without fear of attribution, as in this roundtable, are important for making progress around these challenges. Participants expressed an interest in keeping the communication channels open and welcomed the opportunity to build on the outcomes of this dialogue.

---

[1] When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.

[2] https://www.internetsociety.org/blog/2017/04/securing-our-digital-economy/

Different types or uses of encryption raise different policy issues and challenges for law enforcement

Participants noted that the encryption debate is often carried out in an overly simplified manner or in metaphors that mean different things to different people. There are many types of encryption and each type can be used for different purposes by legitimate users, governments, businesses, law enforcement agencies and intelligence communities, as well as by criminals. Some participants argued that a single policy approach to lawful access to encrypted content is unworkable.

Encryption is a toolbox. Participants stressed that it is important that discussions distinguish between the different types and contexts in which encryption is relevant. One person suggested starting with the following broad categories:

- **Device encryption**, which helps protect data that is *stored* on devices, such as pictures, messages, emails, spreadsheets, or other information that people save in relation to their personal life or business.
- In contrast, **end-to-end encryption** secures data and information *in transit,* as it flows across the network, from one device to another.
- **Anonymised technologies**, such as Tor, which make use of multiple layers of encryption to mask the identity of individuals online.

Participants also identified the need to differentiate between the parts of government that want access, the different kinds of encrypted communications or data they would like access to, and for what purposes. For example, it was noted that law enforcement and intelligence agencies often have different goals when it comes to accessing encrypted information. For example:

- law enforcement agencies might be more focused on obtaining access to *device encrypted information* to aid in *prosecution*, whereas
- intelligence agencies often work on *intercepting end-to-end communications* to *prevent* crime and terrorism.

The challenge of encryption is not encryption: it's the challenge of accessing data. Some argued that law enforcement and intelligence agencies are continually finding it much harder to get penetrative intelligence. However, others disagreed, arguing that it is not the citizen's responsibility to live life in a way that makes the job of law enforcement easy.

As a practical matter, it was noted that different technologies and how they are accessed and used by government and law enforcement agencies differs across countries, and even across democracies. One example that was given was the United Kingdom, where the government is focused more on regulating access to end-to-end encrypted communications rather than device encryption. In the United States, however, access to device encryption was said to be the government focus instead. This was attributed to differences in powers of government, as well as in the rules around assisting law enforcement in the investigation of crime. One person pointed out that the UK Investigatory Powers Act requires that individuals help law enforcement by removing passcodes, whereas US constitutional protections do not compel this.

The approach to lawful access in other parts of the world, according to another expert, varies even more. In some countries, there is a belief that the United Kingdom and the United States have control over major platforms, making access to encryption a "non-issue" for them. These countries place less emphasis on ensuring their own lawful access to encrypted content, instead believing they can gain access to data in plain text through mutual assistance from the US or UK.

Understanding Encryption: Old Debates, Contemporary Challenges

Ethics and Human Rights

Participants also pointed out that the public debate around encryption and lawful access is often framed around trade-offs between security, privacy and public safety. They noted that discussions about encryption are not only relevant to the fights against crime and terrorism, but are entrenched in

deeper conversations about security, human rights and ethics. There was an understanding that the starting point in these conversations must be a common one.

Freedom and privacy were recognised as essential to democracy and society. Some experts argued encryption technologies provide the means for individuals to express themselves freely online. Another noted that, for those under authoritarian regimes, the protection given by encryption is essential for not only supporting freedom of expression, but also for physical safety. In democracies, the trade-off is often framed around privacy and public safety, where law enforcement needs access to information to protect society from crime and terrorism.

One person cited a survey in the UK, which indicated that most citizens (59%) would trade-off some privacy rights for strengthening national security. But, another expert cautioned against overreliance on public opinion to justify positions – as public opinion can be fickle and change rapidly in response to events. Some participants emphasised that encryption and security are not mutually exclusive. Presenting the encryption debate as strictly a zero-sum game of security vs. privacy or security vs. security makes it seem like they are finite things that must be traded off, when, in reality, encryption can enhance both security and privacy simultaneously.

Some speakers were keen to point out that weakening encryption standards has implications beyond privacy and national security, such as for the security of the economy. Thus, it is important to frame the debate around encryption and lawful access to data as a much broader societal problem.

While national security and safety are important issues, encryption also ensures the security of our financial transactions online, and the ongoing security of the Internet more broadly. Some concluded that solutions need to be measured to find a balanced ground that looks beyond privacy and security in a narrow sense.

Others raised human rights and inequality concerns around who has access to encrypted technologies. Some companies, such as Apple, are strong defenders of encryption. However, Apple products are expensive. One participant reasoned that affluent people are more likely to have easy access to encryption technologies. Poorer communities would not have access to devices that were as secure. Some recommended that solutions concerning encryption and lawful access should consider these inequalities surrounding encryption technology.

Investigative Practices

Some participants reported that encryption is having an impact on how law enforcement agencies conduct investigations. They noted that more data is being encrypted in-transit, on devices or in the cloud, making it inaccessible to law enforcement. Several experts argued that there are many devices being held by law enforcement agencies that cannot be processed for evidence due to encryption. The argument is that investigating crimes requires piecing together many, seemingly disparate, pieces of information, and encryption is hindering or stopping investigations.

In contrast, others pointed out that because our lives have become increasingly digital, there is much more data available to law enforcement now than in the past. Although encryption does not allow third party access to the actual content of a message or a stored file, some noted that law enforcement can access metadata, which can be used as effective evidence in investigations. Some conceded that metadata might not be as valuable as the content of communications but noted that it can still be used to determine where people were, who they were talking to, for how long and at what time. Some participants proposed that this kind of data could be used more often and more effectively by law enforcement.

One expert commented that, in the past, valuable communications data was not always available to law enforcement agencies. For example, if there was a wiretap, individuals who did not want to be heard could always turn up the radio. Disappearing Snapchat messages is not a new issue: criminals have always had access to fireplaces.

Some participants concluded that law enforcement agencies are generally in a much better position for conducting investigations today than they were 15 years ago. The reality for contemporary investigative practices is that law enforcement will not be able to access all the data all the time. They argued that other forms of police work will still need to be used. Many agreed that the main challenge for investigative practices is not a lack of data, but a lack of resources and training for conducting investigations in an increasingly digital world. The participants considered that there is an opportunity to improve training on digital evidence and forensics for law enforcement agencies.

Exceptional Access: Weakening Encryption, Backdoors, and Escrow.

The roundtable discussed several approaches to exceptional access, focusing on three possible scenarios: weakening encryption, master keys and key escrow – all of which were identified to have serious pitfalls.

Weakening Encryption

The first approach would be to weaken encryption systems. Weakening algorithms or the systems that support key distribution would permit law enforcement to circumvent encryption and read the content of communications. However, several participants noted that it is not possible for there to be access for law enforcement without weakening everyone's encryption. Thus, the use of weaker encryption systems creates vulnerabilities that could be used by good actors and exploited by bad ones.

Master Keys or "Backdoors"

The second approach to exceptional access that was discussed would involve creating a master key (also known as a "backdoor") that would enable the holder to bypass encryption controls and read communications. However, experts noted that a master key is simply another entry point into a system that could be used by bad actors, and thus serves as a functional equivalent of weakening the algorithm.

Some participants highlighted that master keys for internal industry use and customer support are fairly commonplace. But, others argued that master keys are often used for authentication, not to decrypt content. They explained that the damage caused by an encryption master key being compromised is much worse than for an authentication master key because, while authentication keys are used to verify an identity, an encryption key unlocks the contents of encrypted data. Some made it clear that anything with a "backdoor" is a threat to user trust.

Key Escrow

The third approach that was discussed would require all users to securely escrow their encryption keys – giving law enforcement or other parties the ability to access someone's key and read their communications. In contrast to the approaches that weaken encryption standards or create master keys to access communications content, some participants argued escrow does not weaken the encryption technology itself. One person mentioned that during the clipper chip debate of the 1990s, a partial escrow was proposed where, of the 128-bit encryption key, the company stored 64 bits and the two parties in communication stored 32-bits.

Although there have been some suggestions as to how escrow could work in practice, there were also several questions to do with scale and whether it would be possible, beyond whether it is a good idea. Most participants made it clear that escrow raises critical security concerns for the user that cannot be overlooked. This included the point that incidents like large scale data breaches demonstrate that there is no way to securely escrow an encryption key without the database becoming a target for theft.

Lawful Hacking, Hoarding Zero Days, and Creating Network Vulnerabilities

The job of law enforcement has changed as a result of innovations in technology, changes in criminal behaviour, and how individuals secure their information and communications. Lawful hacking—or sometimes termed "equipment interference"—refers to lawful access to information in transit or on a device by exploiting vulnerabilities in the system. According to some participants, governments have traditionally had the right to lawfully hack devices to access data during an investigation. But, one other issue raised concerning lawful hacking is that it sometimes uses vulnerabilities that are unknown to the vendor—known as zero days—to exploit the system and access information.

Undisclosed zero-day vulnerabilities can help law enforcement agencies during their investigations, but some experts argued they can have serious consequences for the overall security and stability of the Internet. If zero-day vulnerabilities are left unpatched, the platforms and systems are vulnerable to cybersecurity breaches that are not in the public's interest, and that are not carried out under the rule of law.

While some participants acknowledged that lawful hacking is something that happens under rule of law, others expressed concern about the technique. On the question of the value of the approach for law enforcement, one person noted that lawful hacking is not very useful for the rapid responses necessary during investigations and would not be effective for addressing some of the immediate needs of law enforcement. Another stated that lawful hacking is not sufficient for collecting evidence for investigations, but can still help to a degree.

Others saw the hoarding of vulnerabilities for lawful hacking as easily leading to an arms race. If governments shared vulnerabilities with vendors and developers to patch systems, some participants saw disclosure as equivalent to unilateral "disarmament." This "disarmament" could improve the overall security of our online ecosystem, but potentially make one state more vulnerable to attacks by others who are hoarding zero-days. Nevertheless, participants believed there needed to be an active discussion about vulnerability disclosure, data retention, and law enforcement cooperation.

Strong encryption as a market differentiator

The experts observed that increasingly companies are offering strong encryption as a default design feature of their products and services. Although there is currently a market—and demand—for stronger security and privacy-enhancing features, encryption is also seen as a long-term security solution. Security is part of the culture of some companies, especially as they become more digital. Some participants stressed that end-to-end encryption and device-based security is about enhancing protections for users and improving the trust relationships between companies and individuals, as opposed to stopping law enforcement and governmental access. This cultural and organisational shift around user-centric privacy and security has only just begun. They felt that we are currently in the early days of change, and encryption affords the best security and privacy for users. Thus, developments in encryption will continue. One person made it clear that, in the meantime, companies could also take steps to educate users on best practices for cybersecurity, allow reporting of abuse and follow through with appropriate actions and not weaken encryption standards.

Surveillance based business models

Discussion around lawful access to encrypted communications has generally focused on law enforcement (i.e. government access), alongside market trends towards stronger security and privacy. However, one participant noted that some view the discussion as too narrowly focused and even hypocritical, given the private companies with "surveillance-based" business models. They noted that big technology platforms amass information about users, which is then used to attract advertisers for profit by enabling fine-grained matching of individuals' profiles with advertisers' goods, services or political campaigns. Yet, they observed there is very little discussion about what companies do with the data they collect, and how that information should be shared with law enforcement and under what conditions.

Metrics and Measurement

Several participants raised the lack of data on the impact of encryption on law enforcement as a concern. Although data is increasingly being secured with encryption, there is very little public information on what impact this is having on law enforcement's ability to prosecute criminals and prevent crime. They proposed that more data on the impact and scale of encryption on investigations, prosecution and prevention is needed for a full consideration of the issues.

International Consequences/ International principles or norms

The participants identified potential international consequences of national decisions as one of the big challenges surrounding the encryption debate. Global companies face the challenge of implementing country-level laws and regulations surrounding encryption. Do companies weaken encryption in their products for everyone, or create multiple products with different levels of encryption for different countries?

Some argued the implementation of different national laws and standards surrounding encryption could help fragment the Internet. Thus, many thought it is important that the story of lawful access be told in a global context.

When it comes to creating laws, principles and norms around lawful access to encryption, several experts noted that one must take into consideration the different kinds of political and legal regimes around the world. It was argued that democratic countries generally have in place strong legal systems with more checks and balances on the exercise of power that protect individuals' fundamental rights. However, authoritarian regimes do not. If democracies begin to introduce laws and regulations that weaken encryption, some were concerned it could legitimise the actions of authoritarian regimes. For example, one participant noted that China recently passed a law undermining encryption and said it was following the lead of the United Kingdom.

Another participant pushed back, arguing that democracies do not want to be left unsafe, with their law enforcement agencies having minimal power to access communications content, just because other countries lack checks and balances. Another person also noted that authoritarian countries will not care about what democracies do with encryption laws: they would be happy to use democracies as an example, but they will not be constrained by creating their own laws on encryption adoption and use.

Public and Private Cooperation

Some participants stated that law enforcement requests for data from private companies have increased drastically in recent years. Several viewed companies as capable of playing a key role in shaping cooperation between law enforcement agencies that can protect user trust, while supporting law enforcement efforts and investigations. One person noted that some big companies have begun to publish guidelines on what kinds of data law enforcement can and cannot access. For example, Apple has published such guidelines for both US and non-US law enforcement. Other companies, such as Google, have provided training and advice for law enforcement agencies to help them get the data they can have access to. Participants consider that there needs to be more engagement between law enforcement and the private sector.

At the regional level, a participant noted that the European Union report on terrorism has made calls to establish a more structured dialogue between industry and law enforcement agencies. Some viewed these kinds of initiatives as important first steps for defining norms around cooperation, but also concluded that still more needs to be done to improve cooperation between law enforcement and industry, involving education, communication, and policy.

Several participants added that government and industry have already made several compromises to balance some of the competing rights and goals of law enforcement with user security, trust, privacy and the stability of the Internet. For example, one person gave the example of lawful access to metadata under national security laws as a compromise that has now been deemed as not enough for governments. Another expert noted that there need to be firm lines on where compromises are drawn in terms of what is considered acceptable information for law enforcement to access.

Participants concluded that there need to be more technical conversations between law enforcement and companies to close the communication gap. Companies need to help law enforcement understand the range of tools and information they can use in investigations, rather than – as one participant put it – 'fetishising encryption'.

Having an open and ongoing discussion with industry and other stakeholders will help law enforcement to better understand how to operate and make the best use of information in a ubiquitously connected society, while preserving the protections afforded by encryption.

Towards agreed principles on lawful interference, encryption and privacy

Although the encryption debate has many different perspectives and interests, some raised the idea that there could be a collection of principles that regulators, judges and law enforcement agencies could act upon with regards to lawful access to encrypted content. One participant suggested the following principles:

- The solution must be targeted.

- The solution must not weaken security.
- The solution must not change the trust model between the lawful user and companies.
- Law enforcement needs access capabilities.
- Any solution won't always work.
- Any solution relies on cooperation between companies and law enforcement.

Several added that, given the international consequences, any principles around lawful access must have international application. Although some participants thought that the G20 or G7 process could be helpful, others noted that these groups are voluntary and non-binding.

Nevertheless, the participants agreed that there is value in norms or principles, and that the debate does need to take place at the international level. However, they also noted the challenges in finding consensus at the international level. Thus, a more regional or local focus may prove a more pragmatic starting-point to develop principled frameworks for lawful access to encryption.

Conclusion

The debate around encryption and lawful access is over twenty years old and still has no easy answers. Yet, through identifying nuances, areas for improvement and dividing the problem into manageable pieces, the experts provided a clear set of issues that will each require focused effort from stakeholders to solve.

Using the outcomes of this roundtable as a starting point, the Internet Society and Chatham House will continue this dialogue in 2018. The aim of this joined work in 2018 will be to explore concrete steps towards a societal consensus around encryption and lawful access.