Personal Privacy, Police Investigation, and Encryption

Marc Christen
Bern University of Applied Sciences
Module BTI7545-18/19 - Cybercrime
Tutor: Prof. Dr. Bruce Nikkel

December 10, 2018

Personal Privacy and Encryption

The right to privacy is considered a human right and is anchored in all modern democracies [1]. Human rights apply in virtual, digital space as well as in real life. What does privacy actually mean? Well, that depends a lot on who you ask that question to. If you would ask the Sentinelese from the North Sentinel Island in the Bay of Bengal, they would probably say it is their right to separate (isolate) themselves from the outside world. In the digital age where personal information is recorded, collected and misused almost everywhere, I would personally say it is my right to protect my personal information. This includes my private web-surfing behaviour as well as my private data or communication over various channels such as e-mail, telephone or instant messaging. The famous NSA whistle-blower Edward Snowden made a fitting quote in this context: «*I do not want to live in a world where everything I do and say is recorded. That is not something I am willing to support or live under.* [2]»

Strong encryption offers a way to secure our data and communication against eavesdroppers like criminals, totalitarian governments or other threats. For many individuals it is the only way to secure information in a digitally highly connected and monitored world. Journalists can securely communicate with their sources or citizens of a repressive country can share their experiences and observations without getting arrested. Encryption also holds risks and sometimes you are weighing yourself in false security. For example, if encryption is used incorrectly (or is incorrectly implemented) it can lead to data breaches.

In the history of the Internet there have been several data breaches and personal privacy scandals. One of the worst Internet privacy scandals was made by Sony BMG. They ran into a major privacy flap in fall 2005 because of the anti-piracy measures called XCP that they added to music CDs. When a customer played one of these CDs on a Windows PC, the CD installed hidden rootkit software onto the PC. This software informed Sony the CD has been played and

sent the IP address of the PC. This so-called spyware also created vulnerabilities on PCs for worms or viruses to exploit. The U.S. Federal Trade Commission required Sony to pay $150 to any consumer whose PC was damaged by the software as part of a settlement for violating federal law [3].

However, the right of privacy can be restricted because of the public interest in a person or for law enforcement purposes as we can see in the next sections.

Police Investigation and Encryption

With the ongoing digital transformation, the organised crime is increasingly spreading on the Internet. Criminals are committing a wide range of cybercrimes that know no borders (physical or virtual) and are a very real threats to the victims worldwide. Because of the Internet «classic crimes» such as robbing a bank have moved to cyberspace. Financial institutes face thousands of attacks nowadays, as well as government agencies are being spied on and attacked. Even crimes against children are facilitated by the Internet.

All larger police organisations such as INTERPOL, Europol or national police agencies like the well-known Federal Bureau of Investigation (FBI) have built specialised departments to investigate cybercrimes. However, just as anyone can use encryption to protect their privacy, criminals and terrorists have the same opportunities to shield their illegal activities and that poses major problems for law enforcement today. Today the strong encryption is so sophisticated it is hard for the law enforcement agencies to decrypt and access secured evidences. In order to mitigate or even bypass the «strong encryption problem», law enforcement agencies in the USA in particular are demanding that tech-companies like Apple, Google or Cisco be forced to install backdoors in their products. This makes it easier to break into encrypted devices or connections during a case or investigation. Corresponding James B. Comey, a former FBI director, is one major argument that they cannot protect the general public from terrorist activities under all circumstances or are unable to access the evidence they need to prosecute crime even with lawful authority [4].

How encryption can have a significant impact on a cybercrime investigation is reflected in the following example: Operation Achilles was a joint investigation between the United States Federal Bureau of Investigation (FBI) and the Australian Federal Police (AFP). This international investigation had the goal to uncover a massive child pornography distribution ring. The members of this ring used the Tor network for an anonymous communication and hide their identities as well as Pretty Good Privacy (PGP) which is considered as a strong cryptographic scheme [5]. Without the proper PGP keys the investigators were not able to decrypt the information shared among the members and the usage of Tor made it even harder for them to trace the trails. It was an informant who gave law enforcement the information they needed to bring down the group. A man was arrested unrelated to the case and bargained a deal with the police. He provided the

authorities with the necessary information and keys to infiltrate the ring and bring them down one by one. The encryption software did its job and without the information received from the informants arrested in this case law enforcement would have been unable to uncover the ring and arrest the individuals [6] [7].

Conflict of Interests

Cyber security is a huge public safety concern. On the one hand, law enforcement is confronted with its current dilemma of gathering evidence in a criminal or terrorism case. They can hardly keep up with the modern technology and the amount of cyber crimes. They therefore require simplified access to encrypted data. Tech companies such as Apple, Microsoft or Google are to be legally forced to release the decrypted data of their customers or the key themselves. As an example, the Australian parliament has recently passed a corresponding anti-terrorism monitoring law, which comes into operation at the end of the year [8]. The new law provides for the decryption of messages (WhatsApp and Co.) and the subsequent installation of backdoors in software. This would massively affect data security. The originators of such laws come mainly from intelligence institutions and the police. The former FBI director James Comey was one of the strongest promoters of such laws.

On the other hand, data protectionists, experts of cryptography and computer security around the world criticise this trend sharply. The popular American computer security professional Bruce Schneier for instance, says the following about the new law of Australia: «Never mind that the law 1) would not achieve the desired results because all the smart "terrorists and drug traffickers and pedophile rings" will simply use a third-party encryption app, and 2) would make everyone else in Australia less secure. But that's all ground I've covered before [9]». Another point of criticism often mentioned in this context is that such laws empower states to extend the mass surveillance of citizens as it is already the situation in China. Backdoors can also be used by terrorists or criminals against the institutions that are supposed to protect us.

While the technical debates about whether encryption can be securely backdoored are interesting, they only represent one part of the argument for why these proposals are a terrible idea. The use of encryption technologies has been widely recognized as a core component of freedom of speech, as well as the right to privacy. While these rights are not absolute, a broad mandate requiring backdoors that would impact anyone other than specific targets in investigations would likely be considered a violation of human rights standards. Fundamentally, we all have an interest in a safe and secure Internet. Modern technology is fluid and fast moving. To keep up, law enforcement needs to adapt. But seeking to undermine encryption only looks backward instead of focusing on where technology is going. Both sides should discuss more about the potential of new investigative possibilities instead of insisting on the hardened fronts.

Possible Solutions

There exist no easy solutions or just one to end the debate about protecting personal privacy versus law enforcement it is just a too complex topic. Only from the point of a technology view this cannot be fixed. However, the technology companies, the data protectors and the authorities should get together and discuss the respective privacy requirements and the investigations together in a forum. A joint task force could be set up to improve criminal investigations together and at the same time independent privacy watchdogs could monitor whether the action and suspicion is legitimate to release information in a case. This does not necessarily mean breaking up encrypted data, but also passing on meta information that can be useful in an investigation. The use of synergies may also lead to new investigation methods, without weakening existing technologies through backoors. The independent privacy watchdogs are elected by the public and can only be in power for a certain period of time. Similar to the term of a presidential mandate. The public must be informed regularly and transparently about what is going on in the task force.

This solution is not technological, like backdoor access built by manufacturers or service providers, but a human solution built around user control. Such arrangements provide robust protection from criminals hacking the service, but they also prevent customer data harvesting by service providers. In a next step, as soon as the forum around the task force has been established, a kind of trust circle could also be created. Customers of technology companies such as Google, Apple, Microsoft etc. should then be able to split their keys for decrypting the data into several keys and hand them over to different instances of the task force. Only if all instances agree, the encrypted data will be decrypted. This form of secret sharing (or also called secret splitting) could help law enforcement to access encrypted data for evidence ensurance.

However, this method and solution cannot prevent criminals or terrorists from simply using individual, strong encryption such as PGP or AES to protect their messages. Technology is used by honest and dishonest people. Just punching holes into encryption or installing backdoors on computers will not fix any of our problems with privacy and digital crime investigation. It makes things even worse.

References

[1] European Court of Human Rights, 1950 *European Convention of Human Rights: Article 8 privacy.* Available online: https://www.coe.int/en/web/human-rights-convention/private-life

[2] The Guardian, 10. June 2013 *Edward Snowden, NSA files source: If they want to get you, in time they will.* Available online: https://www.theguardian.com/world/2013/jun/09/nsa-whistleblower-edward-snowden-why

[3] Dirk Martin Knop, 1. November 2005 *Sony BMG's copy protection with rootkit features.* Available online: https://www.heise.de/newsticker/meldung/Sony-BMGs-Kopierschutz-mit-Rootkit-Funktionen-143366.html

[4] James B. Comey, Federal Bureau auf Investigation Director *Going Dark: Are Technology, Privacy, and Public. Safety on a Collision Course?,* speech delivered to Brookings Institution, October 2014. Available online: http://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course

[5] Wikipedia *Strong Cryptography.* Available online: https://en.wikipedia.org/wiki/Strong_cryptography

[6] Smoke, 19. June 2015 *Encryption Software and Combating Cyber Crime.* Available online: https://www.cybrary.it/0p3n/encryption-software-and-combating-cyber-crime/

[7] FBI, 28. May 2010 *Operation Achilles.* Available online: https://www.fbi.gov/audio-repository/news-podcasts-inside-operation-achilles.mp3/view

[8] The Parliament of the Commonwealth of Australia, 2018 *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* Available online: https://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r6195_first-reps/toc_pdf/18204b01.pdf;fileType=application/pdf

[9] Schneier on Security, 17. July 2017 *Australia Considering New Law Weakening Encryption.* Available online: https://www.schneier.com/blog/archives/2017/07/australia_consi.html