Personal Privacy, Police Investigation, and Encryption

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

December 5, 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

Possible Solutions

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