Privacy and Law Enforcement

Julian Stampfli

Department of Information Technology, Berner Fachhochschule

December 19, 2018

The importance of Privacy

Privacy is not a new topic and as such it was always important to protect the humans from an arbitrary invasion of this basic right. This is of such high importance that it has found its way into the UN Declaration of Human Rights, the ECHR and the federal constitution of Switzerland. (*1–3*) However, the playing field is changing. With the strong trend towards digitalization, the amount of data that is available for private citizens is ever growing. With it grows the importance of data protection to protect the citizens from totalitarian powers. (*4*)

With proper encryption and high data protection, citizens can communicate with each other without a third party knowing about it, which is one aspect of privacy. Thus they can say what they want without fear of punishment. This ability is a vital part of our society and an essential pillar in democracy. However, is this right undermined? In Switzerland, the telecommunication provider has to keep records of all phone calls and SMS and other metadata (who, when, what, where) for all of their customers for 6 months. The current law and jurisdiction consensus values privacy concerns less important than the ability of law enforcement agencies to find criminals using this data. (*5*) If this law is extended in such a way that the government can access all communication data, then they could easily censor opposition and control the masses. Even

if those laws come with restrictions like it is only applicable to major crimes, the definition of a major crime could be adjusted in such a way that suits the current government. Thus the protection of our privacy is of paramount importance. (*6*)

An additional risk is that all this data could be made public by criminals or by some other means. This release would result in many attack possibilities for private citizens. Big data sores tend to be interesting targets for criminals since their data enables various criminal actions. The impact on society is mostly ignored. With the Ashley Madison leak, many people had to suffer grave consequences such as broken marriages, financial consequences and a higher risk of suicide. (*7*) People got extorted and should they not pay up they were threatened with shaming. (*8*) Considering that this was a leak on a small portion of society; the impact of the release of all the telecommunication metadata would be inconceivable.

Those data stores are mostly well protected against such a data breach. But this could change. Law enforcement agencies wish to build backdoors and weaken encryption in general so that they can access data that is sent directly between two suspects. Should this be implemented our privacy could be circumvented. This circumvention might be acceptable enforcement as long as there won't be any misuse and the access would be proportionate. However, we don't want criminals sniffing in our data. Weakening protection enables them to access our data without our knowledge. Which might create an even bigger impact than if the data from those stores would be released. (*9*)

There is always an outcry when new laws get introduced that aim to weaken encryption and create backdoors in systems. Australia has just passed such a law named the Bill Assistance and Access Bill. (*10*) This bill aims to increase the potential to find criminals, mainly terrorists and child exploiters. It requires technology companies to implement backdoors or weaken encryption so that all data can be examined in case of suspicion. However, it has widely received bad press and is the first anti-encryption law worldwide. (*11, 12*)

The importance of Law Enforcement

After reading the first part one might think that law enforcement is the root of all evil; it is not. The primary goal of law enforcement is to protect society from harm by weighing the need of the many against the need of the few. They must follow the law and can be punished if they go against it. (*13*)

Criminals tend to change habits and adapt to new markets when they see the money. The digital world gives them a lot of new possibilities to hide their tracks, connect securely and internationally or commit new offenses. Due to secure end-to-end encryption law enforcement agencies are unable to investigate suspicious behaviour on the internet. With that restriction, their ability to protect and detect is seriously weakened. (*14*)

Similarly to citizens who had suffered when their privacy was broken, there are also cases where people suffered because the criminals couldn't be caught in time because of data protection concerns. Public victims of such crimes are children that have been or still are victim to child exploitation. The children are abused, and the material is shared throughout the world with the use of anonymization and encryption. It is hard to catch the criminals when they are cautious. Law enforcement and other actors still try hard and fight with what they have and thus there have been successes in the past. (*15*) But many of those crimes are unsolved, and many children might still be in the hands of the criminals. (*16*)

Another important issue is terrorism. With the aid of the internet, terrorists can easily communicate and plan attacks cross-border. Additionally, it is easier for them to recruit new followers. Online activity can identify some of those aspiring followers. (*17*) For that, the law enforcement needs access to this activity data so that they can act on the information and prevent acts of terrorism. (*18*) Law enforcement agencies also always try to find new ways to prevent terrorist attacks using digital technologies. (*19*)

Should law enforcement gain more potential to access anonymized and encrypted data they could prevent more attacks and solve more cases. Thus they could protect society as a whole better by preventing attacks and solving crimes. (*14*)

Privacy vs. Law Enforcement

As discussed above both the need for privacy and the ability of law enforcement agencies to solve crimes are essential for society. Without the first we would always have big brother watching us, without the latter we would sink into anarchy. Both are not ideal states for society. However, why do they conflict this much?

As mentioned, with the ability to communicate securely and anonymized citizens can talk about political or social issues privately. The identical communication channel can be used by criminals to plan an attack, share data or discuss ways to exploit humans. With that, they take the good things about data protection and use it for illegal actions. Usually, the law enforcement agencies would have the possibility to invade the privacy of a suspect with judicial approval. They can go to his house and search for evidence, or they can tail him and spy on him. This strategy doesn't help them though if all his communication is encrypted and he has taken the necessary precautions. Such a criminal could be committing a crime while being physically watched without anyone knowing or being able to prove it.

Many parties see this as a big issue. Law enforcement agencies are some of the most vocal about this. Fedpol, as a national player, reminds people yearly about the difficulty of solving crimes in a digital world. (*14*) They seem to be successful as they have much weight into the political discussion. Just recently the Swiss law was adopted in a way that weakened data protection. (*20*) Most major parties accepted this new policy. Interestingly the young generation of those parties mostly opposed it. (*21, 22*)

However, there are also non-political parties involved in this discussion. The most vocal

against any weakening of privacy rights are the Chaos Computer Club and various technology companies that specialize in data protection like Threema and various foundations that advocate for privacy like the pep foundation. (*23*) The opposition is not limited to technology companies specializing in security, other technology companies stand with them. For instance, Microsoft, Apple, and Google openly opposed the assistance and access bill from Australia. (*24*) One smaller contestant called Signal states that they could not comply with the bill even if they wanted because they don't store any data, often not even metadata. (*25*)

Both sides are well represented with strong arguments and strong influence. This equilibrium might be part of the reason why the discussion doesn't progress the way it should. No policy was passed that wasn't met with firm opposition from either side, while this is common in political discussions, it is very frustrating that such an important topic cannot be resolved to any satisfactory outcome. (*9*)

Where to go from here?

As positions have become entrenched a solution seems far off. Especially when both sides have valid points, it is hard for private citizens and public figures alike to come up with a solution that satisfies all parties.

What many parties don't consider is the fact that encryption and anonymization are part of a service. Many technology companies either offer high privacy with strong encryption and anonymization protocols or they use the customer data to display relevant advertisement and content. Law enforcement could be allowed access to a certain part of the collected data, which in turn should be communicated transparently to the users by the company. Apple currently has published information about what the government requests they get and how they reply to them. (*26*) By doing that the citizens can make a qualified choice on which services they want to use and how.

Another important factor is that criminal gangs can be infiltrated and as they are working with anonymization tools they cannot easily identify law enforcement officers either. Thus the job of an undercover cop in a digital society is easier and less dangerous. It is easier because they have multiple tries. In the real world, one officer can't try to infiltrate the same gang multiple times because he would be recognized. In the digital world, he can easily change his username and try again. Also because he can't be identified he deals with a smaller risk to end up dead. These infiltrations are one way to gain access to this encrypted data without the need to weaken the encryption or create a backdoor, simply because the law enforcement officers receive the data as well in an unencrypted form. There have been many criminals who have been convicted this way, especially criminals who tried to lure children by chatting them up. (*27*)

Important to note is that law enforcement needs to get lucky once to catch a criminal. The criminals need to be lucky every time with one mistake where they send messages over an insecure channel, and they can be caught. Moreover, when one criminal gets caught many others could fall as well because of metadata or other unencrypted communication data that is found by directly accessing the devices of the caught criminal. This way one arrest could lead to multiple convictions. Especially if the arrested can be turned against the other members.

Thus limiting the privacy of all citizens by including backdoors and weakening encryption is not needed for law enforcement to do a good job. They can already access a wealth of information publicly that never would have been available in the past. Moreover, by working with the service providers to better understand the publicly available information and to clearly define how to access the restricted data, they could catch many criminals without harming the whole population.

Privacy should categorically be protected as it is a fundamental human right. Invasion of privacy should always only be possible after exhaustive weighing of interests. Backdoors and weakened encryption, even though powerful, are not proportionate as there are other ways to

access the required data. It would also need to be reasonable which has to be decided from case to case. However, weakening the data protection of all citizens is not in their best interest and thus should be avoided.

References and Notes

1. Universal Declaration of Human Rights, http://www.un.org/en/universal-declaration-human-rights/. [Accessed; 2018-12-17].

2. European Convention on Human Rights, https://www.echr.coe.int/Documents/Convention_ENG.pdf. [Accessed; 2018-12-17].

3. SR101 Bundesverfassung der Schweiz, https://www.admin.ch/opc/de/classified-compilation/19995395/index.html#a8. [Accessed; 2018-12-17].

4. Digitalisierung braucht wirksamen Datenschutz, http://www.privatim.ch/de/digitalisierung-braucht-wirksamen-datenschutz/. [Accessed; 2018-12-17].

5. Speicherung und Aufbewahrung von Randdaten der Telekommunikation. , https://www.bger.ch/ext/eurospider/live/de/php/clir/http/index.php?lang=de&type=show_document&highlight_docid=atf://144-I-126:de. [Accessed; 2018-12-17].

6. Personal data, privacy and the totalitarian state, https://www.theguardian.com/world/2016/oct/18/personal-data-privacy-and-the-totalitarian-state. [Accessed; 2018-12-17].

7. Don't gloat about the Ashley Madison leak. It's about way more than infidelity., https://www.washingtonpost.com/news/morning-mix/wp/2015/08/19/

dont-gloat-about-the-ashley-madison-leak-its-about-way-more-than-infide
?utm_term=.d2a10a8ae580. [Accessed; 2018-12-17].

8. I got caught on AshleyMadison.com, https://www.latimes.com/home/la-hm-la-affairs-rick-thomas-20170111-story.html. [Accessed; 2018-12-17].

9. Internet Society-Chatham House Roundtable on Encryption and Lawful Access, https://www.internetsociety.org/resources/doc/2018/internet-society-chatham-house-roundtable-on-encryption-and-lawful-acce [Accessed: 2018-12-17].

10. Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6195. [Accessed; 2018-12-17].

11. AUSTRALIA'S REVISED "ASSISTANCE AND ACCESS" BILL: STILL A BAD IDEA, https://cyberlaw.stanford.edu/blog/2018/10/australias-revised-assistance-and-access-bill-still-bad-idea. [Accessed; 2018-12-17].

12. Australian government passes controversial world-first anti-encryption law amid broad criticism, https://newatlas.com/australia-encryption-law-passes-controversy/57560/. [Accessed; 2018-12-17].

13. Polizeiliche Aufgaben auf Bundesebene, https://www.fedpol.admin.ch/fedpol/de/home/polizei-zusammenarbeit/national/polizeiarbeit_auf.html. [Accessed; 2018-12-17].

14. Jahresbericht Fedpol 2017, https://www.fedpol.admin.ch/dam/data/fedpol/publiservice/publikationen/berichte/jabe/jabe-2017-d.pdf. [Accessed; 2018-12-17].

15. AntiPedoFiles, http://www.actioninnocence.org/antipedofile/. [Accessed; 2018-12-17].

16. Crimes against children, https://www.interpol.int/Crime-areas/Crimes-against-children/Crimes-against-children. [Accessed; 2018-12-17].

17. Phasen der Radikalisierung, https://www.fedpol.admin.ch/fedpol/de/home/terrorismus/terrorismus-aktuelle-lage/Phasen.html. [Accessed; 2018-12-17].

18. Terrorism, https://www.interpol.int/Crime-areas/Terrorism/Terrorism. [Accessed; 2018-12-17].

19. International experts meet on potential threat posed by new technologies, https://www.interpol.int/News-and-media/News/2018/N2018-143. [Accessed; 2018-12-17].

20. Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs, https://www.admin.ch/opc/de/classified-compilation/20122728/index.html. [Accessed; 2018-12-17].

21. Müssen die Überwachungsinstrumente des Staates gestärkt werden?, https://www.nzz.ch/meinung/debatte/debatte-zur-revision-des-buepf-1.18312367. [Accessed; 2018-12-17].

22. Das Nachrichtendienstgesetz auf einen Blick, https://www.nzz.ch/schweiz/abstimmung-vom-25-september-das-nachrichtendienstgesetz-auf-einen-blick-ld.111204. [Accessed; 2018-12-17].

23. Stop BÜPF, https://stopbuepf.ch/. [Accessed; 2018-12-17].

24. US tech giants decry Australia's 'deeply flawed' new anti-encryption law, https://techcrunch.com/2018/12/10/silicon-valley-denounce-australia-encryption-law/. [Accessed; 2018-12-17].

25. Encrypted Messaging App Signal Says It Won't Comply With Australia's New Backdoor Bill, https://motherboard.vice.com/en_us/article/nep5vb/signal-app-australia-encryption-backdoor-bill. [Accessed; 2018-12-17].

26. Privacy - Government Information Requests - Apple, https://www.apple.com/lae/privacy/government-information-requests/. [Accessed; 2018-12-17].

27. 134 IV 266, https://www.bger.ch/ext/eurospider/live/de/php/clir/http/index.php?lang=de&type=show_document&highlight_docid=atf://134-IV-266:de. [Accessed; 2018-12-17].