Case For Privacy

A real life example of why privacy matters

Sippo Rossi and Irfan Kanat

25/04/2021

We have covered how individuals and companies can track people online in the previous modules. There is also a third source of tracking, the governments. Now the course moves from stalking (personal) and tracking (corporate) to surveillance (government).

Audience and Teaching Objectives

The target audience of this case is high school students and young adults, but the key points are relevant to all people who use the internet.

The case is meant to teach the audience about how governments and specifically intelligence agencies collect data on citizens with legal or illegal methods. This topic is discussed so that students can understand that their data and internet activities cannot be totally private as local or foreign agencies have been caught collecting large amounts of data of regular citizens. This also should help the students think and discuss about classical ethical dilemmas related to mass surveillance and whether "ends justify the means".

Suggested Teaching Format

We recommend the following approach to teaching this topic. First, the students are given an introduction to the topic with a video and/or a lecture by the teacher and then are given a chance to read the first article about the US and discuss it with peers as well as the teacher. The students should be encouraged to actively participate in discussions and talk their minds on the ethical issues regarding the case. Then they will be asked to read the second case which is about Denmark followed by discussions and reflection.

The Case

Background Part 1

Government surveillance is a fact of life and it exists to different degrees in every country. The extent of government surveillance on her citizens can be seen as a test of Democratic norms in the country. Surveillance often increases with authoritarianism (e.g. Eastern Germany, China, United States of America).

Take the Snowden revelations (2013) for example. Edward Snowden leaked a huge treasure trove of NSA (an intelligence agency in the United States) documents that revealed the extend of NSA's spying. It was shocking that (1) all American phone companies were sharing phone records (who called whom, when) with NSA. Millions of American Citizens' information was shared with secret court orders. The

court orders were broad and allowed NSA to collect information on thousands of unrelated citizens for each foreign suspect they were interested in. This is a big deal as normally spying on American citizens is legally more complex. (2) Through a program known as PRISM, NSA could compel American companies to give NSA access to their records. Google, Apple, Facebook… All of these companies were sharing information with NSA and were not allowed to speak of it. (3) XKeyscore program allowed NSA to access records of your online activity. The records included browsing history, searches, emails, chats, metadata. NSA training materials promoted the program as covering "nearly everything a typical user does on the Internet." What was the most shocking was that this program did not require prior authorization. NSA could tap into this information without a warrant, or a court clearance. (4) NSA tried to undermine encryption. (5) PRISM required some tiny legal hurdle. When NSA couldn't get what they wanted through PRISM, they went through their backdoors into links between American tech giants datacenters directly.

Reading Piece 1

Please read the following article from the year 2014: https://www.bbc.com/news/world-us-canada-23123964

Take a break here for in class discussion. Proceed with the rest only after you have completed the related class activities:

Topics

- Online surveillance
- Cooperation between companies and governments

Learnings

- National intelligence agencies have access to almost all data

Discussion Questions

1. Are there legitimate reasons a government may want to investigate its citizens?
2. Is there a material difference between mass surveillance, and targeted surveillance? Is one more legitimate than the other? Targeted in this case means that the individual(s) being monitored are specified rather than collecting e.g. all traffic within a region.
3. Should the citizens expect their government to respect their privacy?
4. Your letters and telegrams are protected from warrantless government surveillance, can you expect this protection to extend to your e-mails and text messages?

5. What about the cases where security collaboration between your government and others put your privacy at risk? Should you expect your government to protect your privacy against other governments?

Background Part 2

While Snowden revealed the extent of governments' capabilities, the surveillance and government's abuse of surveillance is not a uniquely American phenomenon. Danes can expect the government to respect their privacy as it is enshrined in the 72nd article of the Danish constitution and the laws based on this. Yet Denmark too had its share of intelligence faux pas. Since 2014, there have been revelations about FE's illegal collaboration with NSA almost every year. Yet somehow nothing seems to change. The spy agencies prevented by law from violating their citizens' privacy rely on each other to spy on their citizens and share the information in the cases that require the most egregious violations of the laws.

Obviously, the intelligence agencies illegally collecting information on citizens is problematic. This brings us to a classical dilemma. If the citizen has nothing to hide is there any reason for her to be worried about government spying?

Some things to consider when discussing the previous argument.

- What you consider a right today, may become illegal tomorrow.
- Can you always rely on your government to always be on your side?
- Legal framework adapts to the society. What we considered illegal in the past is now fast becoming normal (e.g., interracial marriage, same sex relations, marijuana). Unless the citizens have freedom to explore the boundaries of the law, the laws would remain static, and many changes generally deemed beneficial today would not have happened,
- Online surveillance is way more intrusive than surveillance of the past. It is said that in Eastern Germany, government employed an informer for every six citizens. With our current technology, we each carry our own little informer in our pockets, and the algorithms are automating the task of listening in on us. With this kind of watertight surveillance, society may be locked in stasis.
- The need for a compromise between security and privacy is clear, yet so far have we been compromising our privacy for too little gains in security?

Reading Piece 2

Please read the following article from the year 2020. Do this only after you have read the first one and completed the related class activities: https://www.reuters.com/article/us-denmark-defence-idUSKBN25O1XP

Topics

- Surveillance in Denmark

Learnings

- Denmark is not isolated from the rest of the world when it comes to privacy and surveillance by foreign states

How to respond

- Be an active citizen in voting for politicians and parties that support your views on privacy

Discussion Questions

1. How do you feel about the information regarding Danish agencies collaborating with US agencies?
2. What do you think of the statement “But if the citizen has nothing to hide is there any reason for her to be worried about government spying?”
3. Is compromising the entire populations private messages and information worth it if it for example
    - stops one terrorist attack per year?
    - stops ten terrorist attacks per year?
    - reduced organized crime by 5%?

Note! The numbers above are just made up as examples. The point is to get students to evaluate the acceptable trade off.

4. What possible negative consequences can you see in a government, own or foreign having all your private information?