
Case for Privacy Online

The main idea here is two folds:

1- Move from stalking (personal), tracking (corporate), to surveillance (government). 2- Make the case that individuals today should have the rightful expectation that their privacy online is respected as much as it was in real life.

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.

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. Snowden leaked a huge treasure trove of NSA documents that revealed the extend of NSA's spying. Most shocking was (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, 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.

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 egggregious violations of the laws.

Obviously, the intelligence agencies illegally collecting information on citizens is problematic. But, if

the citizen has nothing to hide is there any reason for her to be worried about government spying? It is my personal opinion that the argument, you should not be worried if you have nothing to hide is a bad argument. First off, the rules of what is legal and what is illegal change. What you consider a right today, may become illegal tomorrow. You can not always rely on your government to always be on your side. Second, 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 we deem 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 water tight surveillance, society may be locked in stasis. The need for a compromise between security and privacy is clear, yet so far we have been compromising our privacy with doubtful gains on security.

This history that I just outlined raises some interesting questions. Which you will discuss in the case discussions in the class.

Are there legitimate reasons a government may want to investigate her citizens?

Is there a material difference between mass surveillance, and targeted surveillance? Is one more legitimate than the other?

Should the citizens expect their government to respect their privacy?

Your letters and telegrams are protected from warrantless government surveillance, can you expect this protection to extend to your e-mails and sms?

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?



This work is licensed under a Creative Commons Attribution 4.0 International License.