Online Privacy

and the Dangers of Surveillance

What is Government Surveillance of Technology?

As the name suggests, Government Surveillance of Technology is when the Government has the authority to monitor all types of technology. This includes phone calls, emails and text messages, webcams or microphones, keystrokes, web searches, gps and much more. Every type of privacy you thought you had is all gone when you can be spied on you at any time.

This is **Edward Snowden**, if that name sounds familiar that’s because a movie was made about him in 2016. He is relevant to this topic because he worked with the **CIA** during the Obama administration and leaked data being assembled to track all forms of digital communications by the **NSA**. Not just foreign Governments and terrorist groups were subject to this surveillance but also regular American citizens. He fled to an undisclosed location in Moscow Russia after this leak due to multiple charges by the American Government. To some he is seen as a hero but to others as a terrorist.

Does this occur in Canada?

Bill C-51 is an anti terrorist legislation put in place by the Harper administration which gives the **CSIS** (Canadian Security Intelligence Service) expanded power to monitor technology. Under this bill promoting terroristic acts becomes an offence under the criminal code. A larger crackdown on terrorist propaganda in the form of online and computer files will happen. Police can now arrest people for suspicion without warrant. **CSIS** can interfere with terror plots. And finally, your personal information is shared with more departments.

What type of message can lead to an arrest?

The vagueness of this bill doesn’t specifically state what is against the criminal code. What is considered promotion of terrorism can be considered differently between what you think and the Government thinks. Therefore if you make a sarcastic threat online you could be arrested without a warrant under suspicion of terrorism. The Government doesn’t know the true intent behind a message. Because of this, society has to conform to a restriction on free speech to avoid being imprisoned.

Is the Government morally justified when monitoring online activity and messages?

I feel as if the results of my research questions will prove that government surveillance of technology is on average immoral and harmful. People don't act the same way they do online as in person. There for legal action should not be put in place when people exercise their right to free speech online. For that reason it is ineffective in finding the actual criminals but instead puts regular citizens at risk which is immoral and harmful.

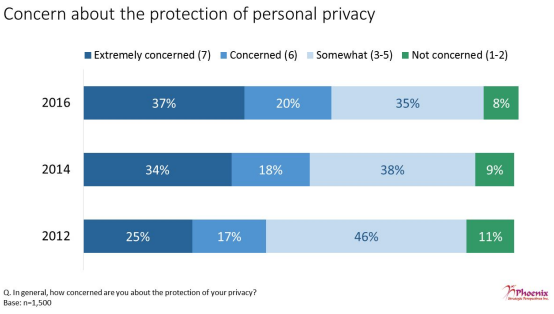
Puts regular citizens at risk

With more power being put in the hands of the Government in terms of online activity, the margin of error goes up as well. Whatever the authorities deem “suspicious” online gives them the authority to now arrest you immediately. These lack of precautions will cause a influx in innocent citizens getting in trouble with the law even if not guilty in intent.

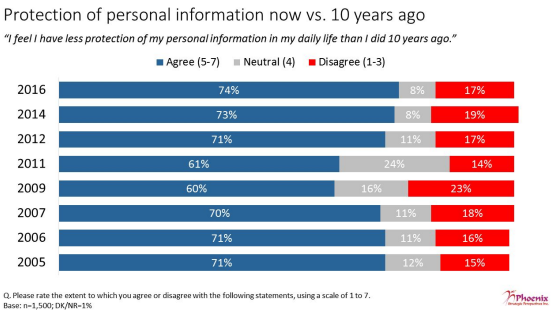
The majority of citizens don’t want to be monitored

If most citizens don’t want laws inhibiting their privacy uselessly, it is immoral to force legislation upon them. There hasn’t been shown to be a need for Bill-C51 in Canada and yet the Harper government in 2015 put it in place. Because it isn’t needed and citizens disagree with it, it is immoral. However if there was a clear problem with terrorism and there was a strong correlation between terrorists and online activity then it would be moral.

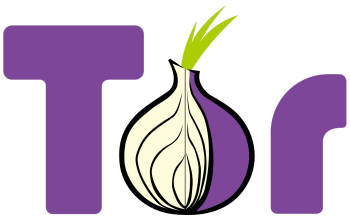
A random sample of 1500 Canadian adults of different races and provinces that were phoned for these surveys.



92% of the participants are somewhat to more concerned about their personal privacy.



74% of the participants feel as if they have less protection of personal info now than they did 10 years ago.



Many people are now using browsers such as Tor which enables full anonymity to users. The government can track you through your IP address. Think about your IP address being like the address of your network. Tor encrypts your IP address multiple times making it look like a random one every time you go on a new page. This guarantees full anonymity up to a degree, there are still ways to get tracked however Tor will notify you beforehand if you might be doing something that makes you vulnerable. Millions of people monthly use Tor to escape the government spying on them for ethical reasons as well as unethical reasons. On tor you also have access to the Deep Web which has every uncensored website. Search engines like Google blacklists websites that break laws such as Online Gambling, Drug Dealing, and Gun shop websites to name a few of the less unpleasant ones. Tors main search engine is DuckDuckGo which has no blacklisted websites.

Hinders free speech

People have to conform to the government's vague standards through the social change they made passing this bill. What you once could say may no longer be allowed and may land you in jail. Everyone has to change their innocent habits in order to not get penalised. You have to message and search things appropriately so you don’t potentially get in trouble with the law. Free speech suggests you are allowed to say anything without restraint as long as it is reasonable (In Canada). However Bill-C51 defines new phrases that are illegal and can land you in prison over online messages.

Ineffective

Because the vast majority will have to conform to this social change people will use the internet as the government sees fit. However the people who don’t know what the government sees fit will get in trouble for things they didn’t know about. While the criminals will be doing their online activity anonymously in order to stay hidden from authorities. There’s been no evidence to suggest government surveillance of technology works nor if it’s a need in Canada making it ineffective in finding actual criminals. Also because the government interprets online words with intent, people who have never committed crimes before and were not likely to do anything are now at risk.

It’s Unethical

Regardless of the positives or negatives to Government Surveillance of Technology the primary indicator of whether a system should be in place is whether it’s ethical. The fact that your material possessions can be ceased, you can be put on the no fly list, you could go to jail for 5 years and all your private information is gone is downright unethical. Even the sheer fact that government is surveilling you is unethical. People don’t want to worry about the fact that the government is viewing all there information and judging their messages and searches. Terrorism isn’t a problem in Canada and yet the Harper government put this in place. The internet is an escape for most people. But now they have to figuratively worry about someone beside them viewing their information and waiting for them to do something suspicious to where they can get consequences. The ethical reasoning matters the most, what good are the positives or negatives if unethical laws and legislation are passed.

Ideal Solution

The ideal solution would be to end Government Surveillance of Technology altogether, however obviously this can't be done. Ways to improve Bill-C51 would be firstly to make it more specific. What the government defines as "promotion of terrorism" may not be what you define it as. Secondly, the Government shouldn't be able to view your searches at all. The fact the Government can see your searches allows them to gather circumstantial evidence for suspicion of terrorism. Most people search things that the government may find suspicious out of curiosity. The ones who don't search things out of curiosity will do it on an anonymous browser like tor. Thirdly, the government should only have access to messages that contain keywords or phrases that are suspicious. If someone sends a suspicious text, the Government should only have access to that text. The government doesn't need anything else and it eliminates some of the concerns with privacy. Lastly, the government can't be so easily reactant. Authorities should do background checks and have multiple cases where the person did something fishy in order for action to be taken. This action being an in person check up with the police not an arrest just to make sure there is no actual bad intent.

Citations

Bill C-51. (2015, October 22). Retrieved November 01, 2017, from http://www.parl.ca/DocumentViewer/en/41-2/bill/C-51/first-reading

Anti-terrorism Act, 2015. (2014, February 11). Retrieved November 01, 2017, from https://en.wikipedia.org/wiki/Anti-terrorism_Act,_2015

Surveillance Technologies. (2015, September 02). Retrieved November 01, 2017, from https://www.eff.org/issues/mass-surveillance-technologies

Edward Snowden | US news. (2017, October 28). Retrieved November 01, 2017, from https://www.theguardian.com/us-news/edward-snowden

Watters, H. (2015, June 18). 5 things that change now C-51, the anti-terrorism bill, is law. Retrieved November 01, 2017, from http://www.cbc.ca/news/politics/c-51-controversial-anti-terrorism-bill-is-now-law-so-what-changes-1.3108608

Project, I. T. (2016, August 28). Tor. Retrieved November 01, 2017, from https://www.torproject.org/docs/faq.html.en

New poll results show support dropping for Bill C-51. (2016, June 11). Retrieved November 01, 2017, from https://www.vancouverobserver.com/news/new-poll-results-show-support-dropping-bill-c-51

Top 6 ways you will be affected by Bill C-51. (2016, March 13). Retrieved November 01, 2017, from http://www.cjfe.org/c51andyou

Office of the Privacy Commissioner of Canada. (2017, January 26). Public opinion survey. Retrieved November 01, 2017, from https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/por_2016_12/