uOttawa

Surveillance: Privacy or Security?

Prepared for: Professor Sibbald
In completion of the requirements of the course SEG/CEG2911
Due: March 14th 2019

Report Authors:
Eric Dam
Mahyar Gorji

Table of Contents:

Contents:

The following report objectively discusses surveillance in both positive and negative contexts, used for both privacy and security. Unfortunately, having one without the other in the context of individual versus state is nearly impossible, and has created a divide amongst denizens of different countries.

In this report, we discuss surveillance as it pertains to the United States of America and its people, but will also draw legal connections and comparisons amongst other countries that have similar regimes or goals. We also discuss briefly a few different forms of surveillance and the breadth of options both parties have, as well as a high profile whistleblower case where intent to protect individuals from surveillance has landed the whistleblower and their native country in massive legal and ethical implications.

Potential limitations will be discussed objectively, using other countries and their laws as a baseline to develop an opinion, and whether or not these can solve the problem of public distrust.

1. Introduction

1.1 Background Information

In modern society, security and safety have always been two core values that have been emphasized. Surveillance on its own is one of the many ways in which the security and safety of people can be protected. By monitoring people, the activities of people can be tracked which would in turn allow for a greater safety net, however this increased protection brings up the controversial issue regarding the line between the privacy and security of the general public. In this report, the unequal compromise of security and privacy that can occur between the government and the general public is researched. The motive of such a report would be to inform the general public on where one would like to balance the two moral values as the government's use of surveillance affects us all. This report has been drafted from objective online resources.

Public surveillance has been prevalent for a long duration of time, with a large influence on this being from the terror attack on September 11th 2001. This attack launched by the terrorist group 'al-Qaeda', would affect the identity of Americans forever. It consisted of 3 different planes being hijacked by 19 terrorists, where they were all flown into the World Trade Center buildings**[1]** . Due to this attack, there would be many lasting effects on the United States. One of these major effects was the drastic increase in US intelligence. The National Security Agency (NSA), on its own, would start to look at 56000 different emails of Americans each year. This event would increase the government surveillance of the public in the efforts to track and monitor and suspected terrorist activity. From this instance and onwards history, government surveillance has been at an all time high, in which people began to question how much surveillance was too much in which it would be deemed an invasion of privacy. The increase by the US government in government surveillance is known as the Patriot Act and has divided communities based off their individual values.
[1][2][3]

In the succeeding sections, the different uses of surveillance employed by the government is discussed, followed by real life incidents with security and privacy and finally where the line between the two moral values should be had.

2. Analysis

2.1 Types of Surveillance

When government surveillance is discussed, usual suspects of these devices would usually be security cameras and phones, however in the 21st century technological advancements have allowed for many more faucets for surveillance to be had. Nowadays more methods are available the Patriot Act which acted as a crutch allowing for the increased government surveillance methods**[4]**.

2.1.1 Emails

In modern day, the internet has become a prevalent tool that has evolved into a large part of many people's lives. With this in mind, it has also become a large point of exploitation for individuals due to the sheer amount of information(**see: figure 1.0**).The FBI has actively acknowledged that they have in fact monitored emails and other forms of electronic communication. Such an example would be when the government implemented "Carnivore" in 1990. This software would scan emails in mass, searching for keywords provided by the FBI through documents. In doing so, it allowed the FBI to be notified if any suspicious emails containing the keywords were being sent **[2]**. This software in comparison to today's is fairly primitive as since then, more advanced software has been used, ultimately replacing "Carnivore".

2.1.2 Cellular Tracking

Another way the government would monitor its citizens was through the use of gps tracking on cell phones. Due to advancements in cellular hardware, gps tracking in phones have become a viable source of information for the government. RCMP official Chief Supt. Jeff Adam confirmed the government's use of cellphone tracking**[5]** if a person's activity is deemed suspicious by the government. Such instances could be done by a device known as IMSI catcher (***see figure 2.0***) which acts as a cellphone tower in which phone's would send signals to the device in which the number could be identified. Due to the fact that each phone has its own

specific id associated with it, the intercepting of these signals allows the device to detect that specific user's phone**[5]**.

2.1.3 PRISM Surveillance

One of the larger pieces of knowledge released by Edward Snowden (***see: case study, section 2.2)*** in his infamous case against the government, PRISM was a large scale operation in which it was revealed that many popular companies such as Facebook, Yahoo and Microsoft gave the NSA access to the personal information of its users. Beginning in 2007, PRISM was passed by the U.S Congress as part of an act called the Protect America Act. This act was passed as it allowed for the intelligence community of the US government to acquire special tools in order to obtain the needed means in identifying potential terrorist threats**[1]**. Due to the widespread acceptance from these large companies, although not all voluntary, it became a central part in intelligence reports even becoming a part of one in every seven reports. The first company that was onboard with the PRISM project was Microsoft in which, soon after, various other companies slowly trickled in. In 2008, Congress would then give the Justice Department special authority which forced companies to comply with their demands for the sake of the PRISM project**[1][6]**.

2.2 Case Study: Edward Snowden

Rarely can one speak on the issue of surveillance without mentioning the high profile Snowden case. Snowden is a "30-year-old whistleblower and former NSA contractor"**[7]** who leaked important documents and NSA programs designed to "collect and store personal communications both within the US and abroad"**[7]**.

Snowden released documents to journalists to selectively analyze and release which in turn has caused multiple legal, social, and ethical implications for both the United States and Snowden. Because this action was outside the boundaries of the constitution, and unknown to the general public, the United States faced several internal investigations and calls for legislative reform and transparency during the Obama Era. Countries like the United States, Brazil and those within the European Union, all have ongoing investigations, while "nineteen proposals for substantial legislative reform of laws enabling US surveillance are currently pending in the US"**[7]**.

More importantly, this case provided a solid foundation for the informal public debate and privacy precautions that users are employing. Users became more weary of social media presences on Facebook and Twitter, and were more concerned with data being shared through their mobile devices. One such reaction came from Brendan Eich of Mozilla.
Eich began raising concerns shortly after the Snowden leak, and concerned with the future security of the Firefox browser, called on its developers and its users to keep it safe from the government**[8]**.

Snowden, however, sought asylum amongst over 27 countries, finally finding safety in Russia. His actions, having embarrassed the United States, made him the target for U.S. extradition where, when returned to the States, he would face a possibility of thirty years in prison. However, "...Snowden risks an unfair trial as there is no public interest or whistleblower exception under the Espionage Act [of 1917]"**[9]**. This means that Snowden cannot rely on his intents as a valid defense, and would be at risk of both legal and, potentially via loopholes in torture law, physical punishments.

This case provides insight into the debate between privacy and security. What the NSA accomplished with their monitoring programs was more akin to spying on the people "just in case", rather than to defend national security. Public outrage at this action taken by the government, as well as the public's outrage for its own ignorance has undeniably lead to progress in privacy rights for human beings.

2.3 Security from Surveillance

Privacy and security are two defining factors in how a society is shaped. Each possess an intrinsic relation to the other, as both together govern where the line should be placed between the two. Increased surveillance, although it does theoretically mean the society is safer due to more eyes watching, realistically increased surveillance does not. This can be mainly attributed to the sheer number of people in which mass surveillance does not prove to be an effective method.

Edward Snowden, a former NSA contractor, when referencing the “Boston Bombing” event, knew the perpetrator even before the event would occur, however due to a non-focused outview on surveillance, the NSA was not able to catch him before the event. Increased surveillance itself is simply a construct that does not definitively make a safer society. Edward would go on and state that if more traditional tactics of surveillance were employed over the mass surveillance technique used, the perpetrator could have been apprehended as missed leads were resultant from the large scope of information**[10]**.

2.4 Where limitations should be placed

Ultimately, the use of increased government surveillance on the general public would in theory in return provide a safety net, protecting citizens, this solution brings up another issue in the potential distrust materializing between the government and the public. Increases in security, though it would save lives in the long run, does infringe upon the rights of the public. It directly goes against the laws in place for citizens, in particular the Privacy Act in 1974. This act itself governs the release of information towards the government in which due to the increased security, conflicts with it**[11]**. The need to maintain trust between the two sides is crucial as trust allows for the evolution of the society. Many benefitting factors such as better economic prosperity or more public services, allow for the growing of the community**[12]**. The acts of increased surveillance go against these values as it can potentially increase the distrust between the two. The correct manner in finding balance is through surveying what the general public wants and seeing where on the spectrum of surveillance and privacy they lie.

2.4.1 The United States In Comparison To Other Countries (Canada)

The United States is on the lower end of the scale when comparing its privacy laws to other countries in the world. Countries like Canada have statutory privacy protection, through the existence of the "Personal Information Protection and Electronic Documents Act" for the private sector and the "Privacy Act" for the public sector**[13]**.

In these protective acts, no personal information can be shared without prior consent, or the sharing entity faces a large fine, in addition to a negative public view. These strict privacy laws cannot be found in the U.S., and are protected and enforced through a privacy ombudsman or commissioner**[13]**, which also is not the case in the U.S.

The Europeans Union recognizes these strict privacy laws in Canada as adequate and responsible. For example, if a company in Canada did not disclose a privacy breach, they face a $100,000 fine**[14]**, and negative public opinions. Because the U.S. lacks a single, comprehensive law to govern personal data sharing**[14]**, the U.S. faces struggles to protect user data, and enables the type of monitoring (i.e the NSA programs) that causes a lack of trust within the public.

2.5 The Benefits of Surveillance:

While many argue that surveillance is bad, and privacy is good, the argument is rarely that simple. The growing debate against surveillance is that governments can begin to become all-powerful autocracies that have information on you that you weren't aware existed **[15]**. The 'Big-Brotherism' doctrine that scares people into motioning against surveillance, while a valid concern, does not portray the positive side.

Automated cameras, for example, help catch speeders and red light runners (**see: figure 3.0)**, and police used cameras with face recognition technology at the Super Bowl to catch known fugitives. But these cameras aren't violating privacy, as they are in public locations**[15]**, where license plates and faces are made public and visible to everyone. In this scenario, surveillance is helping maintain the law and public safety, at no privacy cost to the general public.

In other cases, surveillance helps provide evidence of wrong-doings, that can be held up in a court of law, where verbal evidence normally would not suffice. Where legal to record, an

individual can record their private property for security against theft, or perhaps record an authority figure to keep their interactions honest.

Privacy is an important aspect of human rights, and no human being deserves to be unlawfully and nonconsensually recorded or observed. However, where lawful and just, surveillance can have the power to improve the quality of life of all denizens.

Conclusions

This report discussed the opportunities and oppositions regarding surveillance, as well as its methods in doing so, using the United States as an example. This has recently become an issue with denizens of the U.S., as well as other countries, and has caused a divide between their peoples as privacy and security are often on opposite extremes.

The legal and ethical implications and comparisons between countries like the United States, Brazil, and European countries assisted in providing an understanding of surveillance as it pertained to the U.S.

As well, the Edward Snowden case showed that even when in the moral right, the issue of surveillance is so massive on the legal and ethical scale that Snowden's intent is not enough to protect him under both the Espionage Act and the Patriot Act. This leads to question whether surveillance is a right granted to autocracies, and whether the basic human right to privacy could be overridden. A positive result of this is the progress made in most first world countries in regard to individual privacy, and people have become weary of what data they share and where.

Potential limitations were discussed objectively, using other countries and their laws as a baseline to develop an opinion, and whether or not these can solve the problem of public distrust. On the other hand, it is also important for people to recognize the value that lawful and objectively just surveillance provides and adds to their quality of life. There is a delicate balance to be struck between privacy and security, which can, in unlawful situations, be difficult to find.

Appendices

Daily Email Traffic	2013	2014	2015	2016	2017
Total Worldwide Emails Sent/Received Per Day (B)	182.9	191.4	196.4	201.4	206.6
% Growth		*5%*	*3%*	*3%*	*3%*
Business Emails Sent/Received Per Day (B)	100.5	108.8	116.2	123.9	132.1
% Growth		*8%*	*7%*	*7%*	*7%*
Consumer Emails Sent/Received Per Day (B)	82.4	82.6	80.2	77.5	74.5
% Growth		*0%*	*-3%*	*-3%*	*-4%*

Figure 1.0: Email Traffic Graphic (in billions)

Figure 2.0: Mobile Phone IMSI Tracker Infographic

Figure 3.0:Red light camera

References [IEEE]

[1] "How 9/11 Changed America: Four Major Lasting Impacts (with Lesson Plan)," *KQED*, 11-Sep-2018. [Online]. Available: https://www.kqed.org/lowdown/14066/1-years-later-four-major-lasting-impacts-of-911. [Accessed: 14-Mar-2019].

[2] S. M. Poremba, "10 Ways the Government Watches You," *NBCNews.com*, 30-Aug-2011. [Online]. Available: http://www.nbcnews.com/id/44329996/ns/technology_and_science-security/t/ways-government-watches-you/#.XIgfDihKg2w. [Accessed: 14-Mar-2019].

[3] A. Taylor, "9/11: The Day of the Attacks," *The Atlantic*, 08-Sep-2011. [Online]. Available: https://www.theatlantic.com/photo/2011/09/911-the-day-of-the-attacks/100143/. [Accessed: 14-Mar-2019].

[4] H. Editors, "Patriot Act," *History.com*, 19-Dec-2017. [Online]. Available: https://www.history.com/topics/21st-century/patriot-act. [Accessed: 14-Mar-2019].

[5] D. Seglins, "RCMP reveals it uses cellphone trackers in wake of CBC report | CBC News," *CBCnews*, 05-Apr-2017. [Online]. Available: https://www.cbc.ca/news/technology/rcmp-surveillance-imsi-catcher-mdi-stingray-cellphone-1.4056750. [Accessed: 14-Mar-2019].

[6] "PRISM, Snowden and Government Surveillance: 6 Things You Need To Know," *Cloudwards*, 19-Apr-2017. [Online]. Available: https://www.cloudwards.net/prism-snowden-and-government-surveillance/. [Accessed: 14-Mar-2019].

[7] "Frequently asked questions," *Courage Snowden*. [Online]. Available: https://edwardsnowden.com/frequently-asked-questions/. [Accessed: 14-Mar-2019].

[8] Brendan Eich, "Trust but Verify," *Brendan Eich*. [Online]. Available: https://brendaneich.com/2014/01/trust-but-verify/. [Accessed: 14-Mar-2019].

[9] "Threats overview," *Courage Snowden*. [Online]. Available: https://edwardsnowden.com/threats-overview/. [Accessed: 14-Mar-2019].

[10] M. Guariglia, "Too much surveillance makes us less free. It also makes us less safe.," *The Washington Post*, 18-Jul-2017. [Online]. Available: https://www.washingtonpost.com/news/made-by-history/wp/2017/07/18/too-much-surveillance-makes-us-less-free-it-also-makes-us-less-safe/?utm_term=.77b510e11213. [Accessed: 14-Mar-2019].

[11] "Trust in Government," *OECD*. [Online]. Available: http://www.oecd.org/gov/trust-in-government.htm. [Accessed: 14-Mar-2019].

[12] *What is the Protect America Act?* [Online]. Available: https://www.justice.gov/archive/ll/index.html. [Accessed: 14-Mar-2019].

[13] "Countries Ranked by Privacy," *BestVPN.org*. [Online]. Available: https://bestvpn.org/countries-ranked-by-privacy/. [Accessed: 14-Mar-2019].

[14] "How Canada's Privacy Laws Differ from Those in US, Europe," *Techvibes*. [Online]. Available: https://techvibes.com/2014/10/09/how-canadas-privacy-laws-differ-from-those-in-us-europe-2014-10-09. [Accessed: 14-Mar-2019].

[15] *The Benefits of Surveillance*. [Online]. Available: http://www2.law.ucla.edu/volokh/camerascomm.htm. [Accessed: 14-Mar-2019].

Privacy Vs. Security
-crime rates()/Where the line of privacy and security should be//
-Snowden case **

Types of Surveillance
-webcams/phones//
-Google Home and Amazon Alexa//
-Video (MTL security surveillance)