Internet Surveillance

Is Internet Surveillance Ethical?

Alanis Watz Alconcel
Makati, Philippines
aaalconcel@student.apc.edu.ph

Kimuel Jun Romero
Makati, Philippines
ucromero@student.apc.edu.ph

Jan Michael Bernardo
Makati, Philippines
nrbernardo@student.apc.edu.ph

Fatima Audrey Valencia
Makati Philippines
favalencia@student.apc.edu.ph

***Abstract*—The Internet has been around for twenty years, and over the past two decades it has grown to be bigger than what we could have imagined. As the internet gets bigger, it also poses a lot of threat for online users. Crime rates on the internet have been increasing for the past few years. Some countries want to prevent the increase of online felonies by having internet surveillance. Some people consider that doing so, would be a breach of privacy and it would cause fear among the people using the internet despite the security benefit it can give.**

This research wants to prove that conducting internet surveillance is invasive and prone to abuse by the said individual and institution doing it. The aim of this research is to identify whether or not Internet surveillance is ethical and what are the “acceptable” ways of surveillance.

***Keywords:* Surveillance, Internet, Privacy, Unethical**

I. Introduction

When Netcraft conducted a survey last March of 2012, there were approximately 644 million websites. [1] With how fast the internet is growing it is sure that there are already more than 644 million by 2015. With that being said, it is probable that there will also be risks of being a victim of online illegal activities. According to the Department of Justice of the Philippines in 2010, they were able to get a report from a Symantec security software that almost 9 out 10 Filipinos are to fall for online felony. That is 87% of the Filipinos who use the internet. [2] Therefore, it is not surprising that governments from different countries believe that Internet surveillance is necessary for the safety of their people.

After the attack on the Twin Towers during September 11, 2011, U.S. President George W. Bush passed the Patriot Act. [3] This gave the National Security Agency (NSA), and other associated agencies, power to get people's personal information by putting them on surveillance. Another questionable act of the said law is the ability to impede messages coming from the Internet. [4] Edward Snowden, a whistleblower from NSA, leaked his former agencies secrets on how they were able to weaken privacy on the Internet.

II. PROBLEM STATEMENT

Internet surveillance is a preventive measure to lessen the possibility of innocent citizens from being victimized by illegal online activities and online felonies. With the use of the Patriot Act, the government is given the power to attain people's personal information without their consent. Implementing Internet surveillance can be harmful as the information or data they attain may slip into the wrong hands and be used for personal purposes.

This may lead to identity theft, black mailing, terror threats and other malicious activities.

III. Results and discussion

As discussed in the introduction, the web is not the same as it was years ago. The capabilities of the internet in terms of storing, processing, assessing, and selling large amounts of personal information and usage behavior data [5] is becoming almost uncontrollable and it is because with the undeniable fact that technology is rapidly developing.

Since the World Wide Web (WWW) contains huge amount of confidential and vital data, the latest technologies and equipment have the capability to give the users the privacy and security of their information, but the web is not limited to users who are law abiding citizens. People who have different intentions, use the technology's capability as a tool to do their suspicious transactions, as what happened in the tragic 9/11 attacks. This is when the government concluded that internet surveillance is necessary in relation to the increasing amount of crimes that are now affecting the security of the people.

Normal people could protect their data from other people like them, by setting up security measures such as passwords, fingerprint scans, voice recognitions, or even a face detection to secure the data in their accounts and devices. Some even pay money for services that would monitor their accounts to know if there are malicious attempts of intrusion. In the end, all of these security measures are useless to those higher officials who have the legal authority to access all confidential information which people have the right to remain private.

There had been propositions to revise the laws regarding internet surveillance since some claim that these laws violate the privacy and liberty of those people who are affected. There were also issues about how the government conducts the surveillance, and some protest that the government's actions are unethical as it violates their civil liberties. But the other side of the party claims that these surveillance laws are necessary in order to preserve the national security because in the end, the one that will be held accountable for the uncertainties will be them. [6]

The United States National Security Agency (NSA) have programs called PRISM which serves as their main source of raw information and XKeyscore which can monitor real-time events on the internet. They are partnered with the nine major American internet companies which includes Google, Microsoft, Yahoo, Apple, Facebook, PalTalk, AOL, Skype and YouTube. The partnership between NSA and these companies allows NSA to have direct access to their servers that contains video, audio, photographs, e-mails, documents and connection logs [7] in which they are allowed to access the data of those who they suspect to be doing international felony, such as terrorism and drug dealing.

On September 2011, Jörg Leichtfried and his legislative resolution to disapprove of general EU authorization of exports to certain countries of telecommunication technologies that can be used "in connection with a violation of human rights, democratic principles or freedom of speech (...) by using interception technologies and digital data transfer devices for monitoring mobile phones and text messages and targeted surveillance of internet use". [8]

Based on the discussion of the definition of the laws of internet surveillance and its concerns to protect and prevent the nation from experiencing more traumatic events, the law is still unacceptable to the majority of the people who are concerned.

One of the main reasons why people are so opposed to the law is because they do not trust a stranger to carry out the surveillance, even if it is someone from the higher rank of the government. The result will be that it will seem unethical for those people who will be watched because of the thought that some stranger knows every move and every little information about the person/people being watched, yet they do not know anything about the person who is watching them. [9]

These surveillance laws in the United States of America (USA) started to be implemented by the NSA after the 9/11 incident [10]. The attacker was announced to be one with an ethnic race. The surveillance will be another rising issue to the people who have middle-eastern features in relation to the current racism issues about them. It would not be ethical for these foreigners and converted citizens to be automatically discriminated and labelled as terrorists just because of their race.

"One day they arrested me and they showed me everything. They showed me a list of all my phone calls and they played a conversation I had with my brother. They arrested me because we talked about politics on the phone. It was the first phone I ever owned, and I thought I could finally talk freely.
— Former member of an Oromo opposition party, now a refugee in Kenya, May 2013" [11]

The interview is about the internet surveillance and censorship in Ethiopia. This example shows the unethical reasoning of the government to accuse someone of crime just because of suspicion in the eavesdropped conversation without conducting further trials and research.

There was once an issue about a former Special Agent for the Department of Commerce, Office of Export Enforcement, Bureau of Industry and Security named Benjamin Robinson which used the Treasury Enforcement Communications System (TECS), a government database, for about 163 times to track his ex-girlfriend and her family's travel patterns. [12] Given such power and authority to someone who has personal intentions to use the government's capability to access such data is no doubt wrong and unprofessional. There is no means that the civil liberty of the victim has been violated. This is another reason for people to claim that the laws are unethical and useless since instances like that mean that they are exchanging their liberty for nothing. It goes with the quote stated by a well-known Stanford professor, "It's a mistake to say that there is a balance between liberty and security. They are integral parts of the same whole." [13]

The fourth Amendment ensures that a person has the right to have privacy, and security against invasive acts, such as Internet Surveillance.

IV. CONCLUSION AND RECOMMENDATIONS

This case study concludes that through all the unethical ways that underlie within the laws of internet surveillance and the process in conducting the surveillance the law should be either be modified under the terms that it would be ethical for those who will be involved or revoke and nullify the law if the government does not comply with the terms.

Until the law exists and remains unmodified, the authors of this research recommend the following to protect the people that are being watched: (1) Laws that will support the victims that are unjustifiably accused. (2) Do's and don'ts in providing information in the internet.

And below is a table on which how this paper assess the level of severity of surveillance

Situation	***Passive/Active***	***Intentional/Unintentional***	***Level***
Googling name	Passive	Unintentional	3
	Active	Intentional	1
Public Internet Connection	Passive	Unintentional	3
		Intentional	2
	Active	Intentional	1
Identity Theft	Passive	Intentional	2
	Active	Intentional	1
Accessing Employee Databases	Passive	Unintentional	3
		Intentional	2
	Active	Intentional	1
Online Wire Tapping	Passive	Unintentional	3
	Active	Intentional	1

Legend:
Active-Privacy Breach
Passive-Publicly Available
Intentional- Bad intentions
Unintentional- Good Intentions

Levels
1-Highly Intrusive
2-Intrusive
3-Acceptable

V. References

[1] J. Bort, (2012, March) "How Many Web Sites Are There?", Internet: http://www.businessinsider.com/how-many-web-sites-are-are-there-2012-3 [February 26, 2016]

[2] C.O. Avendano, (2013, January) "87% of Filipino Internet users have been victims of cybercrimes–DOJ ". Internet: http://technology.inquirer.net/21557/87-of-filipino-internet-users-have-been-victims-of-cybercrimes-doj [February 26, 2016]

[3] "The USA PATRIOT Act: Preserving Life and Liberty " Internet: https://www.justice.gov/archive/ll/highlights.htm [February 25, 2016]

[4] M.Rouse, "USA Patriot Act" Internet: http://searchdatamanagement.techtarget.com/definition/Patriot-Act [February 25, 2016]

[5] C. Fuchs. "New Media, Web 2.0 and Surveillance", 2011 http://fuchs.uti.at/wp-content/uploads/Web20Surveillance.pdf [February 26, 2016]

[6] P. Ohm, "Parallel-Effect Statutes and E-Mail "Warrants": Reframing the Internet Surveillance Debate", 2004 http://siliconflatirons.com/documents/publications/faculty/OhmParallelEffectStatutes.pdf [February 26, 2016]

[7] No Author. "Surveillance Techniques: How Your Data Becomes Our Data". Internet:

https://nsa.gov1.info/surveillance/ [February 27, 2016]

[8] No Author. Controlling dual-use exports", 2011. Internet: http://www.europarl.europa.eu/news/en/news-room/20110927IPR27586/Controlling-dual-use-exports [February 27, 2016]

[9] K. Macnish. "Surveillance Ethics". Internet: http://www.iep.utm.edu/surv-eth/#H2 [February 27, 2016]

[10] "Timeline of NSA Domestic Spying". Internet: https://www.eff.org/nsa-spying/timeline [February 27, 2016]

[11] Human Rights Watch. "They Know Everything We Do: Telecom and Internet Surveillance in Ethiopia", 2014. Internet: https://www.hrw.org/report/2014/03/25/they-know-everything-we-do/telecom-and-internet-surveillance-ethiopia [February 28, 2016]

[12] N. LaBauve. "Former Department of Commerce Agent Indicted for Making a False Statement and Exceeding Authorized Access to a Government Database", 2007. Internet:

https://www.justice.gov/archive/criminal/cybercrime/press-releases/2007/robinsonIndict.htm [February 28, 2016]

[13] T. Wu, J. Chung, J. Yamat, J. Richman. "The ethics (or not) of massive government surveillance". Internet:

http://cs.stanford.edu/people/eroberts/cs181/projects/ethics-of-surveillance/interview1.html [February 28, 2016]