# Internet surveillance
# Are you being watched or not?

Paolo George Q. Mayo
Asia Pacific College
Team ZAFT
Makati,Philippines
pqmayo406@gmail.com

Marc Alexander G. Alo
Asia Pacific College
Team ZAFT
Makati,Philippines
mgalo@apc.edu.ph

Jacky L. Chan
Asia Pacific College
Team ZAFT
Makati,Philippines
jlchan@apc.edu.ph

Keith John F. Mantupar
Asia Pacific College
Team ZAFT
Makati,Philippines
kitmantupar@yahoo.com

Bryan Anthony M. Aclan
Asia Pacific College
Team ZAFT
Makati,Philippines
bmaclan@apc.edu.ph

***Abstract* - In recent news, there has been a scandal with National Security Agency (NSA) and Robert Snowden, a former employee of NSA where-in he disclosed information that NSA has been watching and recording everyone's communication activities. It is possible that the government or maybe other organizations are pulling of the same activities.**

**This paper aims to discuss internet surveillance on how agencies do this activity. Moreover, it aims to investigate what positive values might be able to acquire from such actions. It also investigates how we can be able to protect ourselves from it. Finally, the paper discusses if surveillance should be acceptable or not due to ethical issues.**

***Index Terms*—**
***Surveillance* -** *close observation, esp. of a suspected spy or criminal.*
***Wire-tap*** *– method of surveillance done through mounting a device that records or transmits the same message as the one being relayed to the original receiver.*
***Network traffic*** *– Is the amount of data being sent and received via the internet.*
***Privacy safeguards****- are laws, policies or systems that strengthen privacy.*
***Blackmail*** *– act of threatening someone by giving out harmful information.*
***Unconstitutional****- means that it is not acceptable by law because it tramples other existing laws.*
***Network*** *- A group of systems.*
***Upstream of data*** *– data going out of a system*

## I. Introduction

Current innovations in technology has enabled numerous advancements and capabilities for man to use, one of which is a method called tap and trace which is done by connecting into a phone-line or network. The U.S. government has recently signed a law (The USA PATRIOT Acts [1] which allows the utilization of such advancements even the method stated above to enforce safety from terror threats. Advantages of this law is that it will strengthen homeland defense from terror threats and crime schemes by enabling law enforcement faster and more accurate response to possible encounters [2].

Disadvantages are that it is subject to human error like when an old woman was suspected to be a terrorist [3] and is also subject to human rights violations on privacy. The said law allows the unsolicited tapping of phone line- and networks which violate the right to privacy stated by the U.N. Commission on Human rights [4].

On one case NSA installed Real Time Access to Phone and Internet Traffic to secret rooms at key telecommunications facilities around the country. This equipment gave the NSA unfettered access to large streams of domestic and international communications in real time—what amounted to at least 1.7 billion emails a day [5].

## II. Problem Statement

The purpose of Internet surveillance is to prevent terror threats by monitoring every citizen through the use of tapping and tracing of phone lines or network. The implementation of Internet surveillance has brought a huge impact in other countries. Most organizations like governments, corporations, criminal organizations, etc. take use of Internet surveillance to track necessary data or information for personal purposes or intent.

But, like any other surveillance protocols, Internet surveillance has its own disadvantages and limitations (e.g. human error, being unconstitutional, etc.).

## III. Results and Discussion

The researchers believe that the problem lies on the idea of the Patriot Act itself, due to the fact that it is quite vague and unfair to the societal end of the state. The research team believes that a ratification of the said law or an upgrade of it being quite specific on how the government would pass this mechanism should be quite visible in this and thus promoting social inequality to all citizens.

According to results found in our discussions the NSA surveillance program violates the human rights act to privacy according to the UN Declaration of Human Rights because it is unconstitutional to tap record or trace any unsolicited private transactions. The proposed solution to this case is for the Dept. of Computer Crime & Intellectual Property Sections to impose a Warrant or some documented agreement that the Government will have to tap and trace a certain suspect network.

News reports in December 2005 first revealed that the NSA has been intercepting Americans' phone calls and Internet communications. Those news reports, combined with a USA Today story in May 2006 and the statements of several members of Congress, revealed that the NSA is also receiving wholesale copies of Americans' telephone and other communications records. All of these surveillance activities are in violation of the privacy safeguards established by Congress and the US Constitution.

Another example is the controversy regarding the wrongful imprisonment of Brandon Mayfield because of the "sneak and peek" search under the USA PATRIOT Act. FBI Agents bugged his home and office to collect evidence and Brandon Mayfield was wrongfully jailed for two weeks on suspicion of involvement in the Madrid train bombings [6].

Blackmail is an act, often a crime; of threatening to tell secret information about someone unless the person being threatened gives you money or does what you want if the demand is met. There are various forms of blackmailing including (1) extortion - Illegal use of one's official position or powers to obtain property. (2) Coercion - the practice of persuading someone to do something by using force or threats. (3) Commercial pressure - revealing business practices that could damage the business' reputation [7].

An example of blackmailing act case in Michigan involves a man who was charged with Internet extortion and cyber-stalking [8].

Internet surveillance needs to be resolved because our right as a human being is being violated and that is our privacy. Privacy is violated because someone might be tampering or getting information about you without your consent. After obtaining information of a certain individual or organization, attacks might occur on the person targeted because the attacker knows what to use based on the information they got from you.

If a simple person is able to perform such an act, simply imagine the magnitude an organization would be able to do.

Focusing in internet surveillance, this various forms of blackmailing can be used. They can obtain confidential information about that individual or organizations by just threatening them or forcing them to say it. Statistics founds that about 20 percent of teens and 5 percent of adults were blackmailed. Many people were devastated because of the harsh things that other people do to them and causing problem for them that they didn't deserve for it.

In June 2013, the media, led by the Guardian and Washington Post started publishing a series of articles, along with full government documents, that have confirmed much of what was reported in 2005 and 2006 and then some. The reports showed and the government later admitted that the government is mass collecting phone metadata of all US customers under the guise of the PATRIOT Act. Moreover, the media reports confirm that the government is collecting and analyzing the content of communications of foreigners talking to persons inside the United States, as well as collecting much more, without a probable cause warrant. Finally, the media reports confirm the "upstream" collection off of the fiber optics cables that Mr. Klein first revealed in 2006.

## IV. Conclusions and Recommendations

The researchers have concluded that the NSA surveillance system may be a huge asset for US Law enforcement in strengthening home land security it also may be a way to abuse the right to privacy the citizens have. The researchers recommend that until the ratifications have been made to NSA and all existing laws (ex: Patriot act) the public should be careful in transactions they make in daily life.

## V. References

[1] "The USA PATRIOT Act: Preserving Life and Liberty", Internet: http://www.justice.gov/archive/ll/highlights.htm [Feb. 19, 2014]

[2] "Internet Crime Schemes", Internet: http://www.ic3.gov/crimeschemes.aspx [Feb. 19, 2014]

[3] T. Brown, "Grandma Held As Terrorist While Buying Car", Internet: http://freedomoutpost.com/2012/07/grandma-held-as-terrorist-while-buying-car, July 18, 2012 [Feb, 19, 2014]

[4] "PRIVACY AND HUMAN RIGHTS An International Survey of Privacy Laws and Practice", Internet: http://gilc.org/privacy/survey/intro.html, [Feb. 19, 2014]

[5] "How the NSA's Domestic Spying Program Works", Internet: https://www.eff.org/nsa-spying/how-it-works, [Feb. 19, 2014]

[6] B. Denson, "Federal Court Rules Oregon attorney Brandon Mayfield can't challenge Patriot Act", Internet: http://www.oregonlive.com/portland/index.ssf/2009/12/portland_attorney_brandon_mayf.html, Dec. 10, 2009, [Feb. 19, 2014]

[7] F. J. Tipton, J. Allen, "What Are The Different Types of Blackmail?", Internet: http://www.wisegeek.org/what-are-the-different-types-of-blackmail.htm, Feb. 14, 2014, [Feb. 19, 2014]

[8] "New York Man Charged with Internet Extortion and Cyber Stalking", Internet: http://www.fbi.gov/detroit/press-releases/2013/new-york-man-charged-with-internet-extortion-and-cyber-stalking, [Feb. 19, 2014]