Journal of Theoretical and Applied Information Technology
20th January 2016. Vol.83. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

EDWARD SNOWDEN DISCLOSURES TURN THE FEARS OF SURVEILLANCE INTO REALITY: THE IMPACT AND TRANSFORMATION IN INFORMATION SECURITY

FATIMETOU ZAHRA MOHAMED MAHMOUD, AKRAM M ZEKI
Faculty of ICT, International Islamic University Malaysia (IIUM), Kuala Lumpur, Malaysia

E-mail: fatimetou1991@hotmail.com

ABSTRACT

More than two years passed since the biggest event on information security and privacy which is the disclosure of very sensitive documents on the National Security Agency in United States. Those disclosures had a lot of resonance and impact in term of discussions between people who supported the act and others who consider it as crime and breach of trust. The fact, is that the impact was huge not only regarding information technology but it has been extended to economy and politics. This paper provide a holistic view and analyse of the current situation of information technology security and privacy especially with the lack and limited researches that have been done to study the transformation in information security strategies, policies and law after Edward Snowden disclosures and how those transformation had affect the technology, business and politics in various countries. This paper describes in detail and explain how the disclosures done by Edward Snowden has happen, What is the most dangerous programs used by NSA to violate people privacy, The reaction of different countries such as USA and Canada toward this revelations and the change and transformation in policies, strategies and law regarding information security and privacy. Furthermore, how this revelations gave affect the relationship and make it more complicated between China and USA. In addition, many countries focus in developing law to protect their citizens' privacy and security from any foreign surveillance. Moreover, how this revelations has been a lessons to NSA to strengthen its inside protection, lessons to companies to not trust to any internet company to store their business data and how to improve their security systems.

Keywords: *Edward Snowden, NSA, Information security, PRISM, Business companies*

1. INTRODUCTION

In fact, we are living now in the Edward Snowden post era, this name has been attached since 2013 to the worst, larger and most influential data breach that has been caused a countless damage to the National Security of United states where approximately 1.7 million classified documents have been copied and removed from the NSA's infrastructure. Subsequently, Snowden started to communicate with journalists through encrypted emails to disclose details about many NSA classified programs, their spying on Americans, and their allies and enemies, the NSA coordination and agreements with Microsoft, Facebook. Google, Yahoo and others. As a matter of facts, a lot information and communication policies, strategies and laws have been changed after this disclosures of Edward Snowden not only in the USA but in the Whole world. [1][2][3]

2. LITERATURE REVIEW

2.1. NSA Spies and Edward Snowden Disclosures

Initially, the National Security Agency (NSA) is an American organisation which work under the department of defense (DOD). Actually, the united states spend a very high budget for this project that was created to protect the information system and communication of the USA government starting by collecting calls in America, spying and data translation, analysis, coding and decoding. Thus, the NSA has affect from various sides the information security which is the protection of data against any attack, theft or misuse by keeping it safe from any unauthorized access, that's what has been shown by the disclosures of Edward Snowden. [4][5][6]

Secondly, Whistleblowing is to blow the whistle to uncover to the public a wrong or illegal practice in an organization. The whistle-blower after informing the leaders and the responsible in

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

any organization or agency about wrong or illegal practices and they do not respond to him, he do the right thing by uncovering the act to the public to make the concerned parties do the legal right action. In fact, this make them affected by massive personal, social and economic costs. [7][8]

The whistle blower Edward Snowden the "genius among geniuses" and the one who "could do things nobody else could" as described by his colleagues in NSA was one of approximately 1000 NSA system administrators allowed to look at many parts of the network with full administrative prerogative and virtually unlimited access to NSA data and he has create a backup system for the NSA that was implemented to point out security bugs to the agency. [4][5][6]

Before doing the disclosures Edward has tried for many times to make the people in NSA to recognize that many of its activities were illegal but they did not respond to him. After the disclosures Edward have received many sanctions issued and declared by the USA but still not applied due to his presence outside the USA. Actually, the opinions toward Snowden was various some considered him as a hero, where others considered him as a traitor. Some of the documents uncovered by Snowden show that:

- The NSA spies on WikiLeaks
- The use of PRISM program
- Reports which include the NSA boundless informant, call database, and the court order which required secretly Verizon to give the NSA the America's daily phone records, also the surveillance of French citizen's phone and internet records, in addition to people from the business and politic world.
- Xkeyscore that collect everything on the internet.
- The use of Bullrun program
- The secret tapping from NSA to Yahoo and Google data centers to collect information from hundreds of millions of account holders worldwide.
- USA was spying on its allies such as Brazil, France, Mexico, Britain, China, Germany and Spain. [4][5][6]

Indeed, the disclosures of Edward Snowden was not a shock for the NSA and the USA government only, but it has more huge effect and impact in the whole world which reverberated still continuous until today. This disclosure has clarify and confirmed a lot of doubts toward the information security and personal privacy. The NSA use many programs to spy not only on American's but also to other people and countries.

2.2. PRISM

In fact, one of the important information security surveillance programs use by NSA is called PRISM which has a significant impact on the information security. PRISM use data mining to collect and detect data regarding the criminals, terrorists and suspects. It search and collect data on USA citizens and foreign also. Actually, the data is captured from companies such as Facebook, Apple, Microsoft, Yahoo, Skype, Google, and YouTube by having a direct access to those servers. Edward Snowden disclosures has shown that the NSA by the use of PRISM program does not collect data about the criminals or suspects only, although it collect private data which is a violation of the right of privacy for whole people.[6][9][10]

Actually, NSA programs collect two kinds of data. Firstly, metadata such as the phone records which uncover the participants, calls durations and the time. Secondly, the content collected by PRISM such as the content of chats, emails, and cloud stored files. Thus, PRISM program broke the confidentiality and the policies aimed to achieve by the information security in each organization. Furthermore, the risk is not only on the personal information but also to data and information related to business. Moreover, with the development of the ways of data storage such as the use of cloud computing, the businesses trusted to the technology companies because the promised to keep it secure. Thus, after the disclosures about the PRISM program this trust become uncertain, and this make business companies think how to protect the security of their data by the continuous update of strategies and policies, and reviewing their terms and conditions. Also, the technology will more concentrate on the encryption which will be a motivation for the encryption companies to promote their methods and create new strong algorithms. [6][9][10]

Indeed, The PRISM program was the prove of the violation of people privacy by the NSA which has create a lot of doubts and inquiry to the protection of personal and business data in companies. Thus, one of the impact of the disclosures is that companies are now giving more interest to develop ways and strategies to ensure the protection of the security of their data. In addition some steps and procedures can be applied to prevent any security threat from inside the organisation such as a the repair and restructuring of risk assessment and risk management programs,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

renovate security management programs, continuous training and monitoring for employees to well understand security and ethics minimizing the number of people who can access to classified and sensitive data.

2.3. USA, Canada, and China Reaction and Change in IT Policies and Law after the Disclosures

Indeed, the internet belong to all people in all countries, thus there is no specific government, organization or even individual which controls its rules and mechanisms. In fact, Edward Snowden exposures had an effect in the relation between USA and other countries and also on the private and business sector. Actually, there is many business companies in USA which are afraid that their data privacy is not sufficiently protected. For this, and in the other hand the worries to lose the consumer trust have led to many surveys that has been conducted and studied by the European Union and USA to see how much people and organizations still trust to work with USA based cloud service providers. Thus, one of the impact of Edward Snowden disclosures is that the USA government start to place greater value on privacy rights and develop ways to make surveillance more transparent and they are working with their allies to strengthen privacy protection. Furthermore, many plans are executed by government, a huge budget has been specified on secure communication, the anti-censorship technology, and technology training. Moreover, the USA sponsored the Human right council resolution which reconfirm that the same rights that people have offline comprising freedom of expression must be protected online also.[11][12]

In order to restore the people and countries trust and confidence, USA is trying to move one step toward developing strategies to protect privacy and they are supporting and collaborating with Human right council to confirm their goodwill and sincerity to people around the world.

In fact, the main focus of Snowden disclosures was on the USA, but the huge number of revealed documents has clarify the significant role of allies surveillance agencies comprising the CSE(communications security establishment) the Canada's signals intelligence agency. Thus, the disclosures linked to Canada was concerning the surveillance on millions of internet downloads, spying on the Brazilian government, and airport wireless networks. The Canadian's government thereafter was forced to increase its attention to protect the privacy provided to the personal information of people in Canada that will lead to various changes in law implementation and execution practices which has been successfully done by approves the Canada access law legislation.[13][14][15]

Actually, the Edward Snowden disclosures have make the relation between the USA and China more complicated. China deem USA cyber security strategy as an insincere and menacing to the Chinese interests. Furthermore, Chinese analysts show that the USA use its network and information technology to intervene in the other countries affairs and its dominance and control in the network domain menace China's network, political, military and cultural security. One of the consequences of the disclosures is that in 2014 the U.S department has accused 5 PLA officers for economic espionage, and over the time until nowadays many other cases have been published by the USA as an objection to the Chinese attacks to USA. In the other hand especially after the Edward disclosures China consider itself as a victim to cyber-attacks and turn blame toward the USA. Thus, each country expect and wait the other to stop its espionage and change in its approaches which make the corporation between those two countries more difficult. Moreover, China has 3 major reasons to resist this change. Firstly, pursuing a cooperative and transparent relationship can interfere with the Chinese government's priorities. Secondly, China has realized that the U.S stay eager to cooperate and share information about its cyber strategy without ensuring that it will apply the same step. Thirdly, the U.S lost important moral high ground after the Snowden intelligence disclosures, which gave China more chance to refuse any requests to change its behavior in cyberspace and cultivating its own network security infrastructure in addition to the study of other countries information security strategies. **[16]**

2.4. Major Changes after the Disclosures in Various Countries

As a matter of fact, many changes in law had taken place in various countries after the revelations of Edward Snowden, but there is one point that must of the countries have focused in as we see below for instance:

- Australia: in section 77 of the personally controlled electronic health records act forbid the transfer of HER outside the country and the reason is protecting the users privacy and security.[17]

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

- China: prohibition of financial institutions to store or process the personal information such as the info related to the account, identity, credit and financial transactions outside the state in order to protect the users privacy and security. Furthermore this law are not restricted to the financial data only but for all the exchanges of personal information's of users have to be internally in the country. [17]
- Brazil: some requirement from the internet providers to store and distribute the data in a local structure and the reason was to protect the privacy and security of users and the foreign surveillance. [17]
- Canada: Requirement that the personal information maintained by public institutions have to be stored and accessible only in the state due to the foreign surveillance. [17]
- Germany: many laws and decision have been suggested and supported by the government such as to ensure that the transfer of data is approved and safe from any external violation and that the data between Germans have to be routed inside the country networks in order to protect the privacy and security of users. [17]
- Malaysia: the personal data protection act prevent the transfer of personal data abroad unless specified by the minister or exposed to some exceptions comprise the consent and emergency requirements.[17]

Thus, due to the revelations of Edward Snowden the main focus in law change in the countries mentioned above and others is to protect the user's privacy and security in addition to the prevention of foreign surveillance.

2.5. Committee On Legal Affairs And Human Rights Resolutions

In fact, the protection of the human rights become increasingly challenging and crucial especially with the violations of human rights in some countries such USA where they apply illegal practices which threat online privacy and grow the risks to freedom of expression. Actually, in those countries and their allies the change and the limitation of surveillance is not easy. Thus, after the Snowden uncovers some countries such as France, Pakistan and Egypt are working to develop and improve their communications surveillance capabilities. Furthermore, in the individual levels people around the world have started to take steps to protect their online privacy.[18][19]

As a matter of fact, in order to protect the privacy and the freedom of expression some actions are required such as the usage of strong encryption and anonymity tools, the respect of international standards, the full protection and safety for the whistle-blowers who uncover public interest information and any violations of human rights, and a reform in the policies and laws. In addition, the reality has proved that the mass surveillance is not an efficient tool to prevent, limit and fight against terrorism, criminals and suspects. Finally, the national security and the protection of privacy are not two contradictory things in contrast both are wanted to ensure the people safety. [18][19]

3. LITERATURE FINDINGS

Firstly, those great and significant exposures of Edward Snowden was done by using a simple crawler software. Thus he used a very simple and low technology to make the attack from inside and there was no system to detect this breach. Actually, this has shown and have been a lesson to the NSA agency because they have a very strong system to prevent and block any attack from outside but their protection from inside attacks was very weak and primitive.

Secondly, the use of programs such as PRISM has open doors that will be difficult to close not only for NSA and USA but also for the internet companies which was collaborating with them such as Google, Facebook and Microsoft. Furthermore, this had create crisis of confidence between users as individuals or as business companies toward the companies providing internet services and data storage.

Thirdly, USA has lose the trust and confidence and it became difficult for it be back as a leader to defend the internet freedom. Thus, to overcome this crisis and the loss of reputation and credibility the USA and Canada has start to develop new policies, laws and strategies to protect the people privacy in order to get back the people and other countries trust especially with the continuous claim from the Human right council to protect people privacy which is not contradictory with maintaining the national security in addition they demand to have clear laws which protect the whistle blowers.

Finally, the reality is that even with big investments in plans and strategies the human elements proved to be the weakest and the most vulnerable and crucial one. Furthermore, technically in the information security there will

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

more challenges and difficulties in the management and cyber security professionals. Moreover, there will be more demand to have high-skilled, high-trained and credible cyber security professionals in the organisations. Also, some of the implication of the disclosures will be in the information security professionals in their work in the organisations by being more accurate with them, checking their background, doing more surveillance, and control of their access to data.

From all the points discussed, explained and described in this paper we can shape and formalize a view of the advantages and disadvantages of the Edward Snowden disclosures as shown in the table below:

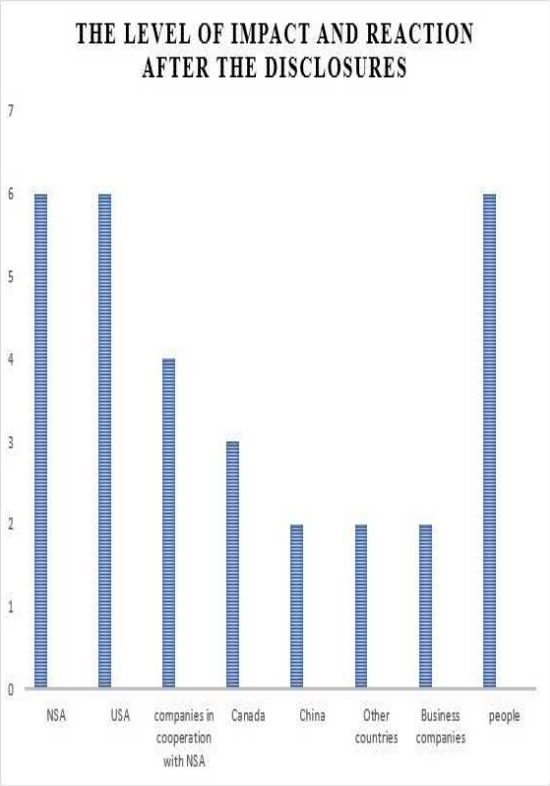
Table I: Advantages And Disadvantages

ADVANTAGES	DISADVANTAGES
The revelation of illegal acts of NSA with the support and cooperation of the USA government regarding the information security and privacy	Making governments more clever to hide their ways of spying and make it more secure and advanced
Informing and explaining to people worldwide the spying programs used and their purpose.	The creation of new problems and conflicts among countries
Contribute in the spread of awareness among people regarding the information security privacy and security.	The dissemination of a situation of no trust among people organisations and governments
Uncover the reality and truth of government especially those who claim protecting user's right and privacy in front of their nations.	
Reveal the implication of companies such as Facebook and Google and others in spying and collecting users data in cooperation with NSA	
Raising the business companies awareness toward the choose of the right company to store their data and also the necessity to develop their information security systems	
It show that even with the highest protection from outside hackers the insiders attacks can be more dangerous and fatal	
Whistle blowers are more courage in telling the truth and they are more protected than before	
Change in many countries laws, strategies and policies to protect their users privacy and security from the foreign surveillance	
Making countries working on balancing between the security and privacy	

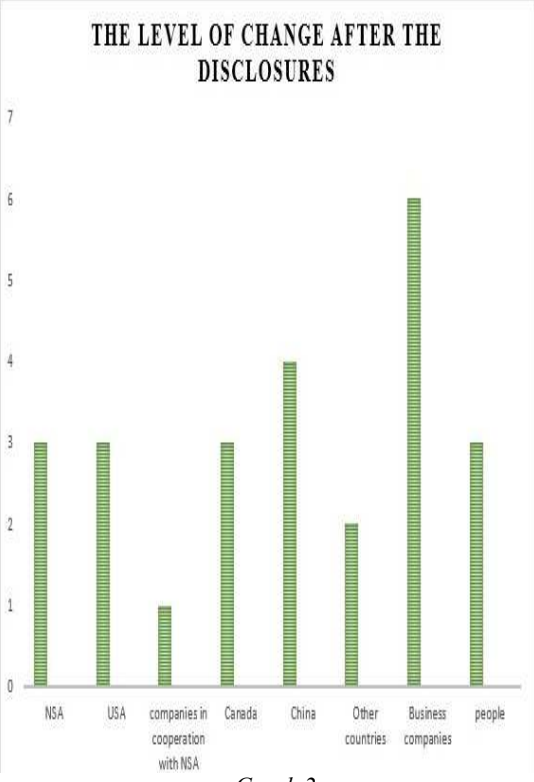
Thus, from the table if we are measuring and balancing the advantages and disadvantages we will see that the advantages part in the scale is more charged and dominating where in the other side the disadvantages we find a few considerable ones.

In the two graphs below we can see from the information's mentioned in this paper the variation between the impact and reaction toward the revelations of Edward Snowden (Graph 1) and the change that have been taken place after the reaction (Graph 2). For instance, in USA and NSA the impact and reaction was very high but their change was very low. Furthermore, the companies that are collaborating with NSA does not show a significant change to users in their policies and strategies. Also, the reaction was diverse between countries but China and Canada was among countries that was directly affected positively and negatively by those disclosures. Moreover, this disclosures have cause a dramatic change in business companies to promote their information security systems and protect their data. In addition, for the normal people worldwide the reaction was great and their fears was turned into reality by this disclosures that they are monitored and observed in every little small data that they share in internet.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195



Graph1



Graph 2

4. CONCLUSION

In fact, the act of the whistle blower Edward Snowden has cause many changes in strategies and policies regarding the Information technology security and privacy worldwide. Actually, regardless the sincerity and veracity of the NSA and the USA government to really apply new policies to protect people privacy that can may be just a cover to conceal their Spying programs and human and privacy rights violation by making it more secretly hidden and difficult to uncover. Moreover, Edward has given a lesson to all workers and employees around the world in all sectors especially IT, to never remain silent and accept wrong and illegal practices in their organisations. They have to be the voice of true to rectify all the illegal practices from the smallest to the bigger one in the organisations and agencies.

Actually, there is a shortage in studies that analyse and handle the Edward Snowden disclosures which is a point of transformation in our modern IT security history that had an impact in various countries, organisations and people. For this reason, this research has been done to cover this disclosure from a holistic view of the security strategy, policy, and law and analyse the level of privacy that people have today especially with the use of programs such as PRISM which break all the privacy rights. Moreover, it highlight the significant role of whistle-blowers in all organisations that must be the voice of reason that lead change and enforce organisations and countries to act right and legally. The potential for future work can involve extending and supporting this research work by an empirical study and analyses including business companies, IT professionals, whistle-blowers, and people from various background to evaluate the impact of disclosures and change and testing their level of awareness on their privacy and security rights especially after the facts demonstrated by Edward disclosures.

REFRENCES:

[1] Mark D. Young. "National Insecurity: The Impacts of Illegal Disclosures of Classified Information". 3 October 2013.

[2] Susan Landau." Highlights from Making Sense of Snowden, Part II: What's Significant in the NSA Revelations". January/February 2014. Published by the IEEE Computer and Reliability Societies.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[3] Jeff Stein.” The End of National Security Reporting?”. July/August 2013. Published by the IEEE Computer and Reliability Societies.

[4] Sharon D. Nelson, Esq. and John W.Simek.” Edward Snowden: How will NSA revelations change the profession of law”. 2014 sensei enterprises, Inc

[5] Hal Berghel. University of Nevada, Las Vegas” The Intimidation Factor: How a Surveillance State Can Affect What You Read in Professional Publications”. Issue No.12 - Dec. (2013 vol.46)

[6] Hal Berghel. ”Through the PRISM Darkly”. Institute of Electrical and Electronics Engineers. Computer.Vol 46, pp. 86-90, July 2013.

[7] Peter Yeoh.” Whistleblowing: motivations, corporate self-regulation, and the law”. International Journal of Law and Management. Vol. 56 No. 6, 2014. Emerald Group Publishing Limited.

[8]. R.D. Francis, A.F. Armstrong, I. Foxley.” Whistleblowing: a three part View”. Journal of Financial Crime Vol. 22 No. 2, 2015 pp. 208-218. Emerald Group Publishing Limited

[9] Keir Giles, Kim Hartmann.” Socio-Political Effects of Active Cyber Defence Measures”. 2014 6th International Conference on Cyber Conflict P.Brangetto, M.Maybaum, J.Stinissen (Eds.) 2014 © NATO CCD COE Publications, Tallinn

[10] Aiesha Y. Khudayer, Rasha M. Abdulsalam, Suha M.Alshaibani, Jamaludin Bin Ibrahim.” Impact of NSA-PRISM to National Information Security Strategy & Policy”. Volume 4 No. 1, January 2014. International Journal of Information and Communication Technology Research.

[11] Susan Ariel Aaronson and Rob Maxim.” Data Protection and Digital Trade in the Wake of the NSA Revelations”. Intereconomics 2013.

[12] Richard Fontaine.” Bringing Liberty Online Reenergizing the Internet Freedom Agenda in a Post-Snowden Era”. September 2014. Center for a New American Security.

[13] Michael Geist.” Law, Privacy and Surveillance in Canada in the
Post-Snowden Era”. University of Ottawa Press 2015.

[14] Andrew Clement and Jonathan A. Obar.” Canadian Internet “Boomerang” Traffic and Mass NSA Surveillance: Responding to Privacy and Network Sovereignty Challenges”.

[15] Association for Progressive Communications (APC), Humanist Institute for Cooperation with Developing Countries. Communications surveillance in the digital age.” Global Information Society Watch 2014”.

[16] Amy Chang.” Warring state: China’s cyber security strategy”. December 2014.Center for a new American security

[17] Anupam Chander .Data Nationalism. [Vol. 64:677]. Emory Law Journal. 2015

[18] Ben Emmerson.” Two years after Snowden: protecting human rights in an age of mass surveillance”. 2015

[19] Mr Pieter Omtzigt.” Committee on Legal Affairs and Human Rights Mass surveillance”. AS/Jur (2015)