Political, Economical and Social Impacts of Snowden Breach

Hasan T. Arslan & Joyren Quarcoo

Abstract

This exploratory research takes a look into the effects of Edward Snowden's Surveillance disclosures on political, economic and social fronts and examines the source of the surveillance issue. The political ramifications include four ways in which American politics and policy have been damaged by the reports. The paper illustrates the economic damage to two major contributors to the U.S and global economy. It also explores the existence of the social debate between privacy and security. Finally, the paper seeks an answer to the question what must Americans draw the government's attention to, to really affect change?

Keywords: Snowden, PRISM, privacy, security, surveillance, NSA

Introduction

Edward Joseph Snowden is a former Central Intelligence Agency (CIA) employee and National Security Agency (NSA) contractor, who became the center of attention and a liability for the United States government in 2013 for leaking classified documents revealing operational methods about National Security Agency (NSA) global surveillance programs. British newspaper, *the Guardian*, announced the existence of a leak of classified NSA documents on June 5, 2013; and the next day, the exposure became worldwide via the front pages of the Guardian and the Washington Post. The Snowden documents disclosed confidential information about the NSA surveillance program codenamed *PRISM*. For the purpose of this research, this momentous modern day leakage will be referred to as "Snowden Breach" and its outlined effects will be referred to as "Snowden Impact".

The issues in question in this exploratory research are whether metadata should be protected by the 4th Amendment and whether an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. Legally, the Third Party Doctrine established by *Katz v. United States* (1967) set the precedent that absolves an individual's reasonable expectation of privacy when they voluntarily disclose information to a third party in an area

accessible to the public. Therefore, the Snowden impact is analyzed in three different spheres, more particularly targeting the homeland: Political, Economic and Social orders. In terms of impacting the political sphere, the release stimulated protocol changes to government surveillance, rendered foreign relations between the U.S. and her allies unsympathetic, and hindered American counter-intelligence and counter-terrorism operational methods. The exposure has also been economically damaging to the U.S. government, which needs to adopt and adjust new policies and train new employees. Final damage of the impact can be observed in the social sphere where these revelations have struck a chord with parts of an American audience who feel like their privacy has been violated. This has sparked an ongoing debate between privacy and security zealots.

NSA Surveillance Program: PRISM

PRISM is a clandestine government surveillance and data-mining program initiated by the NSA in 2007. "The program, code named PRISM, has enabled national security officials to collect e-mail, videos, documents and other material from at least nine U.S. companies over six years, including Google, Microsoft and Apple" (O'HarrowJr,Nakashima, and Gellman, 2013, June 8).Under Section 215 of the U.S.A PATRIOT Act, the Foreign Intelligence Surveillance Court (FISC) may grant the government authorization to collect and store metadata. Therefore, PRISM created a means by which the government collects and stores mass amounts of Internet and telecommunications data and metadata. Prior to the Patriot Act, Congress had already enacted the Communications Assistance for Law Enforcement Act (CALEA), which requires third party companies to make their information systems and data accessible to the government. In situations involving the Third Party Doctrine and CALEA, information freely given to the government does not require a warrant and it is in the interest of third party companies to cooperate with the government. Also legal is the warrantless collection and storage of metadata. Simply, the PRISM program is completely legal under the Foreign Intelligence Surveillance Act(FISA), because "the program is court-approved and does not require individual warrants" (Gellman and Poitras, 2013, June 7). Furthermore, if any individual who knowingly exposes information to a third party they will no longer have a reasonable expectation of privacy over that information. Therefore, there is no violation of 4th amendment rights should that information be searched and or seized by the

government. This is where many Americans may consider criticizing their justice system.

Furthermore, in Justice Sonya Sotomayor's sole concurring opinion for the majority in *United States v. Jones* 132 S. Ct. 945, 565 U.S. (2012), in which the Higher Court provided an answer for the constitutionality of the warrantless use of a tracking device on the defendant's vehicle to monitor its movements on public streets. Justice Sotomayor asserted a need of change for the *Katz decision* by stating "*it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties*."This statement itself supports the core argument of this paper while the justice system continues to litigate cases involving privacy vs. security paradigms. In the following sections, a brief analysis of the Snowden Impact is discussed.

Political Impact

This refers to imminent consequences of Snowden Breach on American politics, which stimulated protocol changes to the government surveillance program. However, in order to influence a change in terms of policy and legislature in the wake of the Snowden Impact, the difference between data and metadata must be examined. "Metadata is the data that defines the structure of data records in files and databases" (Bloor, 2014).Thus, the NSA collects all phones and email records but not their content. Based on the government's actions, legislatively FISA technically characterizes pen register data or metadata as a sort of subset of data. Indeed, under FISA Title 50 U.S. Code § 1842:

> "Pen registers and trap and trace devices for foreign intelligence and international terrorism investigations, a court order or subpoena is sufficient authorization needed for the government to collect pen register information or metadata. No warrant and probable cause are needed."

Basically, government has the right to know who is calling whom but no right to access the content of that conversation. During the NSA warrantless surveillance controversy between 2001 and 2007, the spying agency was authorized by executive order to monitor the phone calls, web activity, text

messaging and etc. of any party believed by the NSA to be outside the country, even if the other end of the communication originated in the U.S. This was all done in the name of the 'war on terrorism' effort. When it was discovered, the Bush administration defended itself with the pretense that they had lowered the standards that are required to establish probable cause for judges to issue to warrants (Sanger and O'Neil, 2006, January 23). Prior to this scandal, the government had to show probable cause that a particular 'target' and 'facility' as required by the 4th amendment were both connected to terrorism or espionage. Following this, the federal FISC judges were forced to issue orders, which remain classified that the government had reasonable procedures in place to minimize collection of "U.S. persons data without a warrant" (Gellman and Poitras,2013, June 7).

What many Americans should be more concerned about are the policies and legal framework in place that legalizes the government's actions. The Snowden Breach, in a way, revealed a certain segment of the political apparatus of the U.S. government particularly dealing with the security issues. "This spying is a signpost of democracy lost, or at least in profound crisis. To reclaim ourselves from this situation will require an organization or movement capable of challenging intertwining state-corporate incursions" (Grabiner, 2013, p.124). The Breach caused a pressure on the White House and finally, on January 17, 2014, President Obama spoke about changes and plans to modify protocols to the government surveillance apparatus (Keller,Parlapiano, Sanger and Savage, 2014, January 17)some of which are depicted in Table 1 below:

Table 1: Changes to Surveillance Protocols

	What Snowden Reveled	**U.S. Govt. Changes to Government Surveillance**	**Detrimental effects**
Phone Records	The NSA systematically collects logs of every American's phone calls and stores the data for 5 years with a blanket FISA court order. Agency analysts were able to	Will require court permission for each search of collected phone metadata based on reasonable, articulable suspicion, and restrict the number of people whose records can be examined to two linkages.	This dramatically lowers the scope of US intelligence gathering capabilities. This puts pressure on the private sector to dramatically expand their

	examine the call records of people three linkages removed from any person under investigation of ties to terrorism.	FederalGovernmentwill not be collecting and storing data and instead have storage responsibility to the private sector.	storage capabilities while the public sector already has these capabilities. To require individual court permission puts an unneeded burden on the legal system as the information is classified and can only be heard by federal FISC judges.
Emails and Phone Calls	The NSA based on FISA may access databases that contain information about emails and phone calls of Americans.	President Obama asks the attorney general and the director of national intelligence to come up with ideas for additional restrictions on the government's ability to use information collected in a warrantless capacity.	This will affect intelligence gathering as it calls into question an issue already outlined and taken care of by FISA.
Federal Intelligence Surveillance Court Structure	There was no form of advocacy present in FISC proceedings to argue against the Justice Department in secret proceedings.	President Obama created a panel of advocates to represent privacy concerns in significant cases.	Since the panel would not have the authority to monitor the court's case load and independently decide when a case warrants its presence decisions are still in the hands of the court and makes this position kind of pointless.

In terms of foreign relations and the strategic interests of the U.S., the federal government must have a realistic policy when dealing with the threat of danger. In the Machiavellian mind frame, this might be the safest approach for the U.S. government. Therefore, as a sound precaution, given the resources at the government's disposal surveillance on the leaders and nationals of foreign countries is conventional. Whether these leaders are allies should not determine if they are surveyed. Thus, from an intelligence gathering perspective the U.S. government's actions are expected; however, what has rendered foreign relations between America and her allies, such as Germany and France, unsympathetic is the overt semblance of an idealist policy which could not withstand exposure.

According to NSA, 1.7 million documents were copied and Snowden shared up to 200, 000 documents with reporters (Gjelten and Block, 2013, December 17). This security breach majorly impacted the U.S. intelligence apparatus; indeed, the Snowden Breach has led to revelations that have hindered U.S. counter-intelligence and counter-terrorism operational methods. There is an undeniable operational effect of informing adversaries of American intelligence tactics, techniques and procedures. Snowden did not only disclose the "what" and "who" of intelligence sources but also the "how" of American intelligence collection(Sabatini, 2013).An official assessment of the damage caused by reports of the Snowden leak about government surveillance programs established by the NSA suggests that terrorist groups are altering their communication methods in order to avoid detection by the NSA. On the terrorist circuit NSA officials say, "foreign individuals or groups targeted for surveillance may now switch to more secure communication methods" (Gjelten, 2013). The disclosures have given these terrorists the opportunity to take action and close their vulnerability. So while these threats may take longer to come to fruition they at the same time become more difficult to track, control and thwart. In tactical terms, denying the NSA the ability to see and stop foreign intelligence threats is not practical and pragmatic for the best interest of the U.S.As the result of initial effects of the Snowden Breach, the chain reaction prompted NSA leaders to "divert agency resources from intelligence missions to security reforms and the investigation" (Gjelten,

2013). This devotion of countless employees has caused one of the world's leading foreign intelligence gathering agencies to be "off task" for the extended period of time the investigation takes. This is a confounding waste of resources. Apparently, Snowden Breach also changed direction of the stream against security in favor of privacy.

Economic Impact

This refers to damages caused by Snowden Impact both forcing intelligence community to make expedited security reforms as part of an effort to prevent future leaks and making private sector to spend millions of dollars to invest in new technologies. While there is not exact information about amounts that the U.S. government has had to spend cleaning up Snowden's mess, probably due to the fact that the process is ongoing, damage to the U.S. government's economy can be deduced. In reality, this total expedited reform process has caused the NSA to spend money that it did not intend to. "We've had to do things that we had planned to do over the next three or four years and move them dramatically to the left…[without] additional resources" says Lonny Anderson NSA chief information officer (Gjelten, 2013).

The revelations of Snowden have impelled U.S. policy changes that have the potential to be very expensive for the U.S. government. With new policies in place, new employees will have to be hired and trained. Thus, Congress must approve a new exponential budget, which brings additional financial burden on taxpayers. The leaks have driven "75% of U.S. defense contractor executives" to change information assurance protocols, "mostly by increasing employee training" (Sternstein, 2014). While training is important, resources spent on the intelligence community's mission would be of more value. In the meantime, many American technology companies must also follow the footsteps of their government and retrain personnel while at the same time losing many customers.

Not only has the U.S. economy been dramatically affected by the revelations of Snowden but the American technology industry has also taken quite a severe hit."The European Parliament has already approved new regulations to curb the transfer of user data to U.S. corporations. If these rules enter into law,

it could have a serious impact on both the operations of companies like Google and Facebook and how the U.S. collects intelligence data" (Keating, 2013).Tech companies in countries in Europe and South America "say that they are gaining customers [who] are shunning United States providers" and both abroad and in the United States, businesses"[are questioning] the trustworthiness of American technology products" (Miller, 2014, March 21).It is not even just the major tech companies, Daniel Castro, a senior analyst at the Information Technology and Innovation Center says that it is "clear to every single tech company that this is affecting their bottom line" and Castro also predicts that the "U.S cloud computing industry could lose up to $35 billion by 2016"(Van Susteren, 2014, March 21). According to Forrester Research, a technology research company, the worst-case scenarios could include net losses as high as $180 billion for the global economy by 2016 as a result of the PRISM disclosures (Staten, 2013, August 14).

Furthermore, it is undisputable that the Snowden Breach has also caused distrust between the American government and its citizens as well as between American technology companies and their customers. Trust is essential for trade and commerce; its absence causes the removal of hundreds of billions from the global economy (Francis, 2013, July 2).

Social Impact

One of the revelations of Snowden is the NSA's spying on Americans. In fact, Snowden Breach questioned the constitutionality and morality (Toxen, 2014) of this secret surveillance. One key question that should be asked is "What does the future hold for the American people?" The changes made to government surveillance in the Snowden Impact could lead to unfavorable scenarios involving the Internet and who controls access and content. Evidently, cyber space is a neutral zone where people from all races, religions and genders meet and interact using different modes of communication. The "Net Neutrality Principle" requires all Internet service providers and governments to treat all data on the Internet equally, not discriminating or charging differentially by user, content, sight, platform, application, type of attached equipment, and modes of communication (Pizzi and Elliott, n.d.). In the U.S., the issue of net neutrality has been an issue of regulatory and judicial disputation among network users and access providers. The following made a

brief examination of net neutrality principle in terms of the interest of the consumer, and the interest of the Internet Service Providers (ISPs).

In the interest of consumers in the net neutrality debate, the government is trying to prevent ISPs from interfering with the consumer's Internet speed when the consumers are trying to use their Internet in such a way that ISPs do not find ideal. On the side of ISPs who are not in favor of net neutrality; is that the "neutral net" principle is a "threat to innovation because it inhibits network providers who believe that the capital raised by charging for 'tiered service' would enable major improvements in broadband infrastructure" (Atkinson and Weiser, 2014). This would make it very difficult of the private citizen consumer who can only afford to pay so much for Internet service. Big corporations would be the only players on the higher tiered Internet service packages. This would affect the fact that the Internet is a human right by making it seem like a privilege.

The kind of Internet that ISPs have sought and are close to gaining would require an innovator to pay extra fees, and ask permission in order to exercise their right to not only explore the Internet but to contribute to its wealth of information. Not only will this stifle peoples' right to the Internet but it will encroach upon the constitutional rights of free speech. People will begin to censor themselves because of surveillance and the incentive to be an innovator will be lost. It would be very dangerous to set a legal precedent that would lead to a world with constraints on original and innovative ideas.

In the light of the Snowden Impact, the future of the Internet lies in the hands of the same policy makers who are restructuring the surveillance apparatus. We are on the cusp of basically losing the free Internet, as we know more drastic measures will most likely follow. As a great influencer and world power America must set the example. Like the government, the Internet was created by the people for the people and should remain this way. This fundamental principle cannot be trampled over for the sake of the proverbial financial bottom line. Creativity must not be stifled and in turn sacrificed for absolute security that is unattainable. It should be kept in mind that "privacy or security is not a zero sum game" (Clarke Jr, 2013).

Forces that pull the Internet away from the quadrant are concerns over loss of security, control of where revenue goes, and compromised personal

information. The first two issues would be of concern to the national or big company level. Unfortunately, for the people the player with the most power and influence at this point in time are the big companies and corporations. Based on their needs they lobby and get policy makers to see matters from their point of view. Thus, the policy makers enact rules and regulations that benefit the big players. The main personal fear on the Internet is the presence of malicious users who attempt to steal and use personal information and the fear of being under surveillance by the government. This leads us to the most likely scenario that the Internet will turn into in the future called the Boutique Networks Scenario, "which envisions a future in which political, regional, and large enterprise interests fail to optimize on the social and economic potential of a shared, global set of richly connected networks"(Jean-Malbuisson, 2009). It is a decentralized and distributed model with heavy regulation and closed standards. It imposes balkanization and no consensus and multiple roots or different Internets, which are not characteristic of the original Internet model. The world will not embrace the balkanized Internet model because it takes the power away from "we the people". Thus, it is important that we recognize socially what shifting policy on surveillance could lead to. A more moderate line should be drawn to be better suiting American people's constitutional interpretations of privacy.

Conclusion

The surveillance modifications that the U.S. government has put into motion are not only detrimental but will also not have the desired effect Americans want. This paper illustrates the detrimental effects of the Snowden Breach in the political, economic and social arenas. The subtle nuances and technicalities under which the U.S. government surveillance program PRISM operated legally, prior to the 2015 US circuit court of appeals holding that bulk data collection is actually not covered by the provisions in section 215Patriot Act, are also detailed. The public has tolerated the easy release of metadata for many years, being in a way wrongly conditioned to be more concerned with the 4th Amendment protection of their content. In addition, also explored and proposed is an avenue through which the surveillance legislative and policy changes that are sought after by the American people can be obtained while at the same time protecting the freedom of the Internet and other communication platforms and their users. As in all legal proceedings the problem cannot be addressed and solved until the issue is correctly defined. In this case the real

issues are whether metadata should be protected by the 4th Amendment and whether an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. Society should not want to turn their right to free communications and innovation platforms into a regulated fractured system. With this in mind, it is important to pay attention to what one is freely given up in terms of personal information and then blaming the government for accessing it.

Finally, one particular question, *what Americans must draw the government's attention to really affect change,* demands an answer, which seems to be hidden in the details of the third party doctrine. Policies and legislation to protect the information that people 'willingly' but truly are required to give up to private sector companies in order to use internet services must be created. The information should no longer be considered third party information where the law and the government are concerned and should instead be considered private information. As long as the private sector no longer has access to the metadata it could no longer bargain its turnover to the government. First Americans must become aware of the fact that the private sector has such intrusive access to their information. Next options like encryption can be used to secure this information allowing only the owner to access it. Lastly, enforceable rules and regulation must be put in place legislatively to ensure that people's privacy rights are respected. Tying these regulations to budgets and grants would be a great motivating factor. These steps would likely assuage the American public and ensure a move in the right direction.

References

50 U.S. Code § 1842 - Pen Registers and Trap and Trace Devices for Foreign Intelligence and International Terrorism Investigations. *LII / Legal Information Institute*. Cornell University Law School, n.d. Web. Sept.-Oct. 2013. Retrieved from on March 20, 2014 from http://www.law.cornell.edu/uscode/text/50/1842.

Atkinson, R. D.&Weiser, P. J. (Summer 2006). A Third Way on Network Neutrality - The New Atlantis. *The New Atlantis*,13, 47-60.Retrieved from March 20, 2014 from

http://www.thenewatlantis.com/publications/a-third-way-on-network-neutrality.

Bloor, R. (2014, June 30). Does Big Data Mean Big Metadata. Information Management. Retrieved on March 20, 2014 from http://www.information-management.com/news/does-big-data-mean-big-metadata-10025760-1.html

Clarke Jr., D. A. (September 2013).Making U.S. Security and Privacy Rights Compatible. Retrieved on March 25, 2014 from http://calhoun.nps.edu/bitstream/handle/10945/37603/13Sep_Clarke_David.pdf?sequence=1

Francis, D. (2013, July 2). How Edward Snowden Could Derail the Global Economy. *The Fiscal Times*.Retrievedon April 8, 2014 from http://www.thefiscaltimes.com/Articles/2013/07/02/How-Edward-Snowden-Could-Derail-the-Global-Economy

Future of The Internet: Boutique Networks [Video file]. Retrieved on February 19, 2014 from https://www.youtube.com/watch?v=YUd8dVVXmRQ.

Future of The Internet: Common Pool [Video file]. Retrieved on February 19, 2014 fromhttps://www.youtube.com/watch?v=rVp3hFJ7ooc

Gellman, B.&Poitras, L. (2013, June 7). U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program. *Washington Post*. Retrieved March 5, 2014 fromhttp://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-Internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html.

Gjelten, T. (2013, September 20). The Effects Of The Snowden Leaks Aren't What He Intended. *National Public Radio*. Retrieved on April 18, 2014 from http://www.npr.org/2013/09/20/224423159/the-effects-of-the-snowden-leaks-arent-what-he-intended.

Gjelten, T., Block, M. (2013, December 17). Snowden's document leaks shocked the NSA, and more may be on the way. *National Public Radio*. Retrieved on April 18, 2014 from http://www.npr.org/templates/story/story.php?storyId=252006951.

Grabiner, G. (2013). Commentary: Government and Market Surveillance, Emergence of Mass Political Society, and the Need for Progressive Social Change. *Social Justice*, *39*(4), 115-125.

Jean-Malbuisson, G. (2009). Internet Futures Scenarios. *Internet Society*. Retrieved on March 6, 2014 from https://www.internetsociety.org/sites/default/files/pdf/report-internetfutures-20091006-en.pdf

Katz v. United States. 389 U.S. 347 (1967).

Keating, J. (2013, October 24). Why the Snowden Leaks Will Have a Bigger Impact Than WikiLeaks. *Slate Magazine*. Retrieved on April 4, 2014 fromhttp://www.slate.com/blogs/the_world_/2013/10/24/reports_of_nsa_spying_on_france_and_germany_why_the_snowden_leaks_will_have.html.

Keller, J., Parlapiano, A., Sanger, D. E.&Savage, C. (2014, January 17). Obama's Changes to Government Surveillance. *The New York Times*. Retrieved on January 20, 2014 from http://www.nytimes.com/interactive/2014/01/17/us/nsa-changes-graphic.html?_r=0.

Miller, C. C. (2014, March 21). Revelations of N.S.A. Spying Cost U.S. Tech Companies. *The New York Times*. Retrieved on April 8, 2014 fromhttp://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html?hp

O'Harrow Jr., R., Nakashima, E.&Gellman, B. (2013, June 8). U.S., company officials: Internet surveillance does not indiscriminately mine data. *The Washington Post*. Retrieved on March 12, 2014 from http://www.washingtonpost.com/world/national-security/us-company-officials-internet-surveillance-does-not-indiscriminately-mine-data/2013/06/08/5b3bb234-d07d-11e2-9f1a-1a7cdee20287_story.html.

Pizzi, P. J. & Elliott, S. (n.d.) A Primer on Net Neutrality. Retrieved on April 8, 2014 from http://www.connellfoley.com/sites/default/files/pjp_net_neutrality_11-07_0.pdf.

Sabatini, C. (Interviewee) &Lee, B. (Interviewer) & (2013, July 16). *Will Snowden Come Between the U.S. and Latin America?* Retrieved on March 5, 2014 fromhttp://www.cfr.org/latin-america-and-the-caribbean/snowden-come-between-us-latin-america/p31109.

Sanger, D. E.& O'Neil, J. (2006, January 23). White House Begins New Effort to Defend Surveillance Program. *The New York Times*. Retrieved on April 5, 2014 from http://www.nytimes.com/2006/01/23/politics/23cnd-wiretap.html?_r=0.

Staten, J. (2013, August 14). The Cost of PRISM will be Larger than ITIF Projects (James Staten's Blog). Retrieved on March 18, 2014 from http://blogs.forrester.com/james_staten/13-08-14-the_cost_of_prism_will_be_larger_than_itif_projects.

Sternstein, A. (2014). 75 Percent of Pentagon Contractors Adjusted Security After Snowden Leaks. *Nextgov*. Retrieved on April 8, 2014 from http://www.nextgov.com/cybersecurity/2014/02/75-percent-pentagon-contractors-adjusted-security-after-snowden-leaks/78302/.

Toxen, B. (2014). The NSA and Snowden: Securing the All-Seeing Eye. *Communications Of The ACM*, *57*(5), 44-51. doi:10.1145/2594502

Van Susteren, E. (2014, March 21).U.S. tech companies lose business because of spying. *Silicon Valley Business Journal.* Retrieved on April 13, 2014 fromhttp://www.bizjournals.com/sanjose/news/2014/03/21/u-s-tech-companies-lose-business-because-of-tech.html.

United States v. Jones. 132 S. Ct. 945, 565 U.S. (2012).

About the Authors

The author Hasan T. Arslan, is a PhD Scholar at the Criminal Justice and Security Department, Pace University, USA. He can be reached at harslan@pace.edu

The author Joyren Quarcoo is an M.A. candidate at The Institute of World Politics, USA. He can be reached at joyren.quarcoo@iwp.edu