An Invasion of Privacy?:

A Look into NSA Domestic Surveillance Policies

Brenda C. Machuca

IT 103/012

Sajid Mahmood

October 3, 2014

"By placing this statement on my webpage, I certify that I have read and understand the GMU Honor Code on http://oai.gmu.edu/the-mason-honor-code/. I am fully aware of the following sections of the Honor Code: Understanding the Honor Code, Understanding the Consequences. In addition, I have received permission from the copyright holder for any copyrighted material that is displayed on my site. This includes quoting extensive amounts of text, any material copied directly from a web page and graphics/pictures that are copyrighted. This project or subject material has not been used in another class by me or any other student. Finally, I certify that this site is not for commercial purposes, which is a violation of the George Mason Responsible Use of Computing (RUC) Policy posted on http://copyright.gmu.edu/?page_id=301 web site."

Abstract

With the emergence of a government agency devoted to look into and do some surveillance amongst its own people, a technology must be in place to commit to these efforts. A look at to what extent these policies affect the public's data will also be undertaken. An emphasis on metadata will be placed in this paper due to its uses in the NSA, its potential misuse, and its controversy. A look into the benefits of having such an agency will be investigated. In addition a look at its security, legal, ethical, and social aspects will be undertaken. The theme of the paper will be that the use of the Surveillance capabilities is required in order to make for a safer environment. A stance that safety is more important than internet privacy will be approached. This relates to the IT world in that someone wrote the code necessary to make the technology available to allow this agency to handle such extensive data mining.

Keywords: Metadata, NSA Surveillance.

Word Count:167

An Invasion of Privacy?:
A Look into NSA Domestic Surveillance Policies

The National Security Agency having access to an enormous amount of personal data creates debate over privacy or the safety of the American public. With the whistle blowing efforts of one, Edward Snowden, the issue has only recently become widely known. In many ways, the information gathered by this agency may help track down terrorist, however, at the expense of the American public's privacy. The legality of this large database of information is up to public debate. Security is the main issue when it comes to the NSA's surveillance policies. The social implications of the NSA's surveillance cross over to the political calling for a more urgent approach to this issue. To what extent do these policies affect the American public's data? The purpose of this investigation is to determine whether or not safety is worth infringing upon people's internet and virtual privacy.

Background

Recently, the issue of online privacy has been controversial due to Edward Snowden's massive data breach on how the NSA conducts its information gathering. Meta data is information such as the time, date, sender and recipient information of a particular communication transaction such as a call, text message or e-mail. It must be noted that, according to The Guardian (2013), "the spy agencies do throw away most of the content they collect" after about three days but keep the Metadata for up to about a year. The NSA now has a database of information that it can use to fight terrorist. According to Price (2014), with the fast pace issuance of the Patriot Act post 9/11, the mining of Metadata has been considered a social norm when it comes to the loss of privacy to Internet and Telephone users. The technology the NSA uses has many positive aspects when it comes to safety and security of American Citizens.

Potential Benefits

Most importantly, the U.S. government cites security of its citizens as being the main reason domestic surveillance is required. According to Herman (2014), only after an analyst has acquired access by a supervisor through proof of a link to terrorist can he look up the Metadata. This shows that the information acquired is not used in an irresponsible way. A concern to some is that the analysts have a wide access to the data. In many ways, the reality of such measures is permissible because the Preamble of the Constitution states that the government must 'provide for the common defense' of its people. However, has this interpretation of the constitution gone too far? In the current state of warfare amongst the U.S. and it enemies, it only makes sense to monitor for possible communication between terrorist via the technology used today. Price (2014) says that within the last twenty years, the government and corporate surveillance programs have been compiling large amounts of Metadata. As an aside, another benefit of Metadata in the corporate realm could be companies getting better advertisement information to better it marketing techniques to a specific consumer. Going back to the issue at hand, according to Greenwald (2014), Obama is quoted as saying, "we don't have a domestic spying program. What we do have is some mechanisms that can track a phone number or an e-mail address that is connected to a terrorist attack" (p. 182). While people like Edward Snowden have created a state of panic between the people's sense of security and the NSA, Americans do need to realize that there is some information that should not be public domain. Therefore, the information leaked in the Snowden scandal may not be completely true. The main potential benefit of such a database is to protect American citizens and property from any form of threat directed at the U.S.

Legal and Ethical Issues

The legality of the NSA surveillance remains unclear. Claypool (2014) insists that the first two federal court cases in the District Court of the District of Colombia and the District Court for the Southern District of New York have made split rulings on the issue. The former ruling it was unconstitutional while the latter ruling it was not unconstitutional. The laws and ethics of this issue are seemingly complicated. In addition, according to Claypool (2014), Judge Richard J. Leon of the District Court of Columbia said that the data acquired without court monitoring goes against the Fourth Amendment of the Constitution, while, in contrast, Judge William Pauley said that the NSA had every right to acquire this data post 9/11 and goes further on to say that Americans do not really care about their own privacy. Already, the NSA has moral and ethical grounds to use this technology, because if they do not, and a disaster happens that could have been prevented, then the American public will blame the loss on the government. Ethically, the government does have the right to protect its citizens at all costs as it forms one of the basis of which the country was found. However, does it constitute the government to extend their abilities in the cyber realm and 'spy on its citizens'? The answer is a resounding yes because the lives of people are more important than their privacy.

Security Concerns

According to The Guardian (2013), the NSA uses their relationships with companies such as Facebook, Google and Microsoft to get things "like emails and messages straight from their servers." The security of people's information is uncertain in these aspects. In many ways, especially with the emergence of Facebook, a growing trend has been transparency. The web used to be a place where one could post anonymously, but now users are expected to have more accountability when it comes to what they say and do on the Internet. According to Greenwald, a

NSA analyst with X-KEY SCORE access, a data collecting program, can compile a massive list of all visits to a particular website and from which computers (p. 156). For many, just the concept of someone looking into their every online transaction and location is enough to raise suspicion. However, one must consider that there most likely is not anyone tracking down their every move. Users of any social media network must presume that the seemingly private messages, pictures and content can be hacked by the NSA. A function of the X-KEY SCORE is to look through social media someone's messages, chats and other private posts (p. 158). With this in mind, any message one puts on the internet is accessible and can be breeched, but in reality, the only information the NSA is looking for signs of terrorism.

Social Problems

There are certainly many social ripples that can happen as a result of the knowledge that the NSA has access to this surveillance type of technology. According to Greenwald, "Telephony Metadata can expose an extraordinary amount about our habits and our associations," including our civil and political affiliations (p. 134). A database like the one described can be alarming as it could lead to ostracizing a certain group of people much like the Nazis did to the Jews but in a more technologically advance method. The problem of domestic NSA surveillance comes down to whether or not we can trust elected official and the bureaucrats in charge of these information system technologies. Sagar (2013) concludes that the leaking of information, like that of the NSA, weakens democracy by causing distrust between its citizens and elected leaders (p. 204). While it is okay to never blindly trust the government completely, there must be a certain balance of trust and distrust between the American people and the people stockpiling these massive databases. Ironically, perhaps the data collected may be doing more harm than good with respect to Americans' trust of the government that created this agency for the intended purpose of protecting them.

Conclusion

To conclude, although privacy issues are being raised over these NSA allegations of mishandling private data, the American public must realize that there is a bigger issue at hand; Safety is the number one priority. At its most basic purpose, the NSA was created to protect its American Citizens from whatever forces may harm them. In this new technologically advanced world, regardless of privacy ethics, Safety will trump all other matters. In many ways, the Meta data collected will not harm individual citizens not involved in terrorist like activities. The information collected is used a precautionary protocol to identify possible threats. The American public needs to get past the privacy issue and look towards a new era of heightened security post 9/11 to prevent any future terrorist disasters.

Word Count: 1430

References

Claypoole, T. (2014). Constitutionality of NSA Cyber Surveillance: Early cases split between privacy and counterespionage. *Scitech Lawyer, 10*(2), 10-11,25. Retrieved from http://search.proquest.com/docview/1507825320?accountid=14541

This scholarly journal provides an informative view on how the Courts have taken into account the legality of using such information and whether or not it violates the constitution. This source is highly valuable to the investigation because the writer leads his firm's Privacy and Data Management Team. The credibility of the author is high because as a lawyer he has a great knowledge of the legality behind this IT issue. The information provided here will help to better understand the legality behind the NSA's surveillance policies.

Greenwald, G. (2014). *No Place to Hide.* New York, New York: Metropolitan Books Henry Holt and Company, LLC.

This source is relevant to my topic because it offers an orthodox view to the issue at hand. It offers a personal narrative over how the issue was portrayed in the media and how it affects everyday citizens including visuals, such as charts, images and graphs. A limitation of this source could be its conspiracy oriented message; however, the data used is reliable. In addition, the author is directly related to Edward Snowden, because Glen was the journalist who published the leaked information via *The Guardian.*

Herman, A., Yoo, J. (2014, April 7). A defense of bulk surveillance: the NSA programs enhance security without uniquely compromising privacy. *National Review*, *66*(6), 31. Retrieved

from http://ic.galegroup.com/ic/ovic/MagazinesDetailsPage/MagazinesDetailsWindow?failOverType=&query=&prodId=OVIC&windowstate=normal&contentModules=&display-query=&mode=view&displayGroupName=Magazines&limiter=&currPage=&disableHighlighting=false&displayGroups=&sortBy=&search_within_results=&p=OVIC&action=e&catId=&activityType=&scanId=&documentId=GALE%7CA364957036&source=Bookmark&u=viva_gmu&jsid=fb5dd8673cb4f454ad5d843c7f5740a7

This source offers a pro NSA stance on the subject and shows some inconsistencies of the opponents of the NSA surveillance. It offers a unique perspective from the other sources on this list and its timing offers a new approach of the information. This source gives the investigation a more realistic approach of the information and less of the over exaggerated reports

Price, D. H. (2014). The New Surveillance Normal: NSA and corporate surveillance in the age of global capitalism. *Monthly Review, 66*(3), 43-53. Retrieved from http://search.proquest.com/docview/1543483298?accountid=14541

This source offers other examples of other motivations behind NSA surveillance. Surprisingly it cites that one of its reasons is for economic advantages in the national and foreign markets. This source provides a comparative view at past examples of gathered intelligence for national and state markets and what it could mean for the future of privacy in the modern age. This source give the investigation possible motives for the government compiling such massive amounts of information

Sagar, R. (2013). *Secrets and Leak*. Princeton, New Jersey:Princeton University Press

This print source provides a critical view of the government's policies regarding NSA surveillance and goes on to point out that it limits democracy as a whole. It is useful or one of its chapters entitled "Should the Law Condone Unauthorized Disclosures?" , which could potentially be beneficial to the legality potion of this investigation. The book itself is extremely reliable as it offers a comprehensive documentation of its citations and references and offers it high credibility.

The Guardian. (2013, November 27). The NSA and surveillance ... made simple – animation [Video File]. Retrieved from https://www.youtube.com/watch?v=GoM4jIZbTtQ

This video created a simplistic view at what the NSA is doing with the technology and information available. It could be limited in that its original source is The Guardian as it was directly involved in the Snowden scandal and because it takes a conspiracy sort of angle to the information. However, nonetheless, it does provide good insight on how the agency works.

.

.