RESEARCH PAPER ON EDWARD SNOWDEN, DATA LEAKS AND CYBERSECURITY IN THE FACE ETHICS

Joshua T. Smith

Principles of Cybersecurity, CSCI 405

Charleston Southern University

September 11, 2021

Abstract

This paper delves into the Edward Snowden incident, WikiLeaks, and the complicated topic of whistleblowing. In this modern age enemies of the state are constantly looking to access critical data about how governmental agencies are operated. With the Snowden leak, the public was made aware of NSA activities of espionage, cyberattacks, and most notable surveillance. The legality of exposing confidential data, and the ethics of the act became a hot topic of debate. It also raises questions about how far we go to protect our governmental agencies when they violate their own citizen's rights, and how do we conduct ourselves based on individual morality? In addition, examines how we ensure protection from future events like this, and ways we can mitigate insider threats before they strike.

Keywords: cyberattacks, espionage, morality, legality, protection, insider threats

RESEARCH PAPER ON EDWARD SNOWDEN, DATA LEAKS AND CYBERSECURITY IN THE FACE ETHICS

Edward Snowden's situation reflects numerous questions about the ethics of cybersecurity and the potential cost of national security on its citizens. To understand Edward Snowden's actions we have to first consider some preliminary background information about his employment. Snowden was employed in 2009 to work under the NSA and during this time he collected classified information on broad surveillance programs carried out over US citizens (Ray, 2021). He observed how these programs had the potential to infringe on the natural rights of its citizens. This observation and data collection would last until May 2013 when Snowden fled the United States to Hong Kong to conduct interviews with the press (Ray, 2021). This would in nature expose several top-secret activities and in the process made him an enemy of the United States. After the interviews were conducted he looked for diplomatic protection to avoid extradition and this is where his partnership with WikiLeaks began.

To comprehend what this partnership entailed we have to observe the mission goal of WikiLeaks. In her book, Taylor aptly describes the company by stating, "WikiLeaks specializes in the analysis and publication of large datasets of censored or otherwise restricted official materials involving war, spying, and corruption"(Taylor, 2017). This ultimately means the WikiLeaks mission goal is to expose what governments do behind closed doors. Their goal is to provide a basis of where top-secret files can be accessed regardless of nation, or often national security. This lined up with Edward Snowden's case and so they offered up many resources to protect him. However, this was a departure from their normal interaction with whistleblowers, as in the past they only provided an unrestricted

platform to post information (Griffiths, 2013). However, due to the scope of information leaked they chose to respond to Snowden's call for protection. Ultimately they secretly moved him to Russia where he remains today (Ray, 2021).

Now that we have observed the groundwork and background information we can now move on to some of the data that was revealed. Considering the size of the NSA, the list compiled by the BBC is quite expansive. It even encompasses cyberattacks enacted on other countries in Europe, and Latin America. The BBC lists these as the major compromises: the U.S. collecting phone records, SMS messages collected and stored, tapping of UK fiber optics with data being shared with the NSA, over 61,000 hacking operations from the U.S. on China, numerous EU offices 'bugged', a multitude of embassies targeted by spy operations, and even a continent-wide surveillance program on Latin America (BBC, 2014). This data breach was a bombshell when released to the public, and raised several questions about what the U.S government conducts behind closed doors. Showing that even American citizen's data was at risk of being exploited by their own government when not regulated. However, at the same time several critical spy operations integral to the country were exposed to the world, and this includes its enemies. Potentially putting the lives of American spies at stake as they conduct espionage in foreign countries. This is what makes Snowden's case so difficult to evaluate legally and especially ethically when you can see him as either a criminal or a hero to the people.

Discussion

Legality

Considering the legality of Snowden's case, he did break the law by exploiting his position in the government to gather classified information to expose to the public. The New York Times states, "...by leaking information about the behavior rather than reporting it

through legal channels, Snowden chose to break the law"(Morrissey 2013). If Snowden would have raised his concerns through natural legal channels that exist he would not be guilty of a crime and instead be a normal whistleblower protected by the law. However, by taking this data to reporters he revealed data that could be exploited by the United States's enemies. This in essence is an act of treason, in addition fleeing the country means that any punishment he was guilty of could not be enforced. The legality of his actions could have been properly defended or exposed through a fair trial if he would have faced the consequences of his actions. Let it be known this is not defending the actions of the NSA, but a proper inquiry by Congress should have been the one examining the NSA and not Snowden strictly speaking legally.

Ethics

If we look at this from a different viewpoint Edward Snowden can be seen as a single man making a stand against a government that had crossed a moral line. He most likely would have been scared of the consequences of exposing the NSA, even legally, and may have not been given a fair trial. In a sense even leaving the country with this information can be seen as a just act, as his primary purpose was to inform the public of injustice being inflicted upon them. He had already lost trust in the system he previously was a part of and could not guarantee his personal safety.

Civil Disobedience

In essence, Edward Snowden's actions can be defined as civil disobedience in a broad sense. A judicial system acts as a way to ensure justice, but if that trust is lost in the government then it is morally justified to have the public presented with information directly affecting them. Brownlee sums up this idea by stating, "He was properly sensitive to the responsibility that public officials have to exercise first-order moral reasoning about the

programs they oversee"(Brownlee 2016). Snowden was aware that he would be alienated by his own country, and if extradited would face the very likely verdict of committing treason. However, he still decided to go against his own government through civil disobedience, and in the process forfeited the life he held previously to retain his moral responsibility.

Future Protection

Although nothing can be done about the past incident with Snowden, there are certain things we can learn from it to better protect whistleblowers and the information stored in critical agencies. The process of protecting whistleblowers can be broken down into several parts, but all need to work in tandem to maintain security assurance. In Governance Directions, it is stated that the "Key to supporting and protecting whistleblowers is having good policies and processes for ensuring early assessment and management of risks of detrimental conduct, active support provision, fair and strong investigation processes and high levels of interpersonal justice"(Lawrence & Brown 2019). All these portions can be summed up into two concepts: early preventance and responsibility. Higher-level managers needed to listen to employees and provide opportunities for investigations to be carried out without the risk of backfire. In addition, noticing potential violations of the constitution needs to happen before those practices are put into effect. Protecting the information can be ensured by protecting the people first.

Insider Threats

Recognizing the catastrophic impact Edward Snowden had on the perception of the NSA, it goes without saying that insider threats are one of the largest problems concerning the security of information. Nurul Mohd, & Zahri Yunos pointed out in the article that the five factors that increase the likelihood of insider threats are: "Foreign intelligence agencies, political or social involvement, personal financial issues, unsatisfied employees, fear of being

sacked"(2020). To protect data we have to consider both insider and outsider threats. Edward Snowden exemplifies what an unanswered risk of an insider threat produces. Politically Snowden did not agree with the surveillance of U.S. citizens, and on top of that feared backlash from releasing information against the NSA and his government. Eventually pushing him to leak the data rather than voice his opinions internally in a safe manner. More often than not agencies and corporations fail to realize that cybersecurity is not just made up of the technology, but the people as well.

Mitigating Insider Threats

Although never perfect, governmental agencies and corporations already implement several ways of data leak prevention, or DLP for short. The article by Nurul Mohd, & Zahri Yunos breaks up DLP into two phases that both need to be implemented to mitigate overall risk. The first phase is composed of three parts and is as follows: Installation by end-users, registration of portable storage devices, registration of portable printers (Nurul Mohd, & Zahri Yunos 2020). These three portions would prevent unauthorized devices from retrieving information and, as a result, it becomes harder to pull data without a record of the device being available. The second portion of DLP prevention would be the policy development stage, and it includes both data classification and policies to handle incidents when they do occur (Nurul Mohd, & Zahri Yunos 2020). In short, you first contain the information in phase one with recognized devices attached to registered users, and then have a structured way of dealing with incidents justly based on easily available policies. These two concepts are where the NSA was potentially lacking, and if they would have recognized the unauthorized data being extracted Snowden's situation could have been handled or mitigated in severity.

Conclusion

In conclusion, Edward Snowden's case needed to have been handled better and more protection for whistleblowers needed to be in place. Yes, Snowden did break the law in releasing his information to the public, but morally it's hard to say if he was in the right or not. On one hand, he did compromise NSA secrets, but he did reveal unconstitutional surveillance measures that were used on U.S. citizens. In a perfect world, the Snowden situation would go through proper legal channels with little to no risk to the whistleblower. Then another branch of the government could launch an investigation to judge the NSA without exposing confidential data to U.S. enemies. However, we have to realize that this is not a perfect world, and there is no telling if the outcry by Snowden would have been listened to without risking himself or his career. Snowden acted on the moral responsibility he held and chose to release the data to the public, and something so critical as constant surveillance needed to be recognized immediately.

Ultimately through his actions I believe he brought about a lot of change, and challenged the conventional means of whistleblowing. His acts of civil disobedience changed this country for the better, because the U.S. citizens learned that we can not always blindly trust our government to do the right thing with our data. Instead we have to actively apply our morals in order to make judgments about the actions of the government and make it more acceptable to speak out against injustice safely. Despite this, I hope an event like this does not happen again in the future, because if every whistleblower went straight to the public it could cause potential chaos that would do more harm than good. Regardless, we have to weigh morality against the protection of data and cybersecurity on a case-by-case basis. Confidential Data has enormous power in this digital age, and we have to put forth our best effort to preserve it, while also maintaining our morals as Americans.

References

BBC. (2014, January 17). *Edward Snowden: Leaks that exposed US spy programme*. BBC News. https://www.bbc.com/news/world-us-canada-23123964.

Brownlee, K. (2016). The civil disobedience of Edward Snowden: A reply to William Scheuerman. *Philosophy & Social Criticism*, *42*(10), 965–970. https://doi.org/10.1177/0191453716631167

Griffiths, P. (2013, August 23). *WikiLeaks defies U.S. to Help Edward Snowden*. HuffPost. https://www.huffpost.com/entry/wikileaks-edward-snowden_n_3487256.

Lawrence, S., & Brown, A. (2019). Protecting whistleblowers: Creating the optimal environment. *Governance Directions*, *71*(9), 486–490.

Morrissey , E. (2013, December 18). *A whistle-blower, a criminal or both*. The New York Times. https://www.nytimes.com/roomfordebate/2013/06/11/in-nsa-leak-case-a-whistle-blower-or-a-criminal/edward-snowden-broke-the-law-and-should-be-prosecuted.

Nurul Mohd, & Zahri Yunos. (2020). Mitigating Insider Threats: A Case Study of Data Leak Prevention. *European Conference on Cyber Warfare and Security*, 599–605. https://doi.org/10.34190/EWS.20.004

Ray, M. (2021, June 17). Edward Snowden. Encyclopedia Britannica. https://www.britannica.com/biography/Edward-Snowden

Taylor, C. A. (2017). *The Ethics of WikiLeaks.* Greenhaven Publishing LLC.