Edward Snowden: A Legal and Ethical Review of the NSA Leaks from 2013

Jared R. Andraszek

Department of Computer Science, Charleston Southern University

CSCI 405: Principles of Cybersecurity

Mr. Patrick Hill

Abstract

The collection of personal data and privacy concerns associated with said data are massive concerns in today's growing dependence on technology. One of the most significant privacy data leaks was from Edward Snowden, a former NSA contractor, who leaked 50,000 top-secret documents to a news journalist to spark conversations surrounding data confidentiality and privacy ethics. However, in doing so, he was charged with two counts of the Espionage Act of 1917 and stealing government property. The NSA's collection methods originated from the September 11 terrorist attacks and the introduction of the US PATRIOT Act. They used their new capabilities to collect user data from Verizon, Google, Facebook, and other large internet service providers (ISPs). The NSA could have implemented some improvements, both technical and personal, to prevent the data leak and ensure that the NSA heard all voices and concerns. Actions such as introducing a liaison or allowing no repercussions for speaking out would have allowed change or more room for fixes. The NSA could also have implemented better access controls and stricter rules on what a network administrator can access. While what Snowden did was illegal, he fully believed that the NSA was in the wrong by making warrantless searches through the collected data.

Keywords: Edward Snowden, NSA, data confidentiality, Espionage Act of 1917, US PATRIOT Act, internet service provider, ethics

Edward Snowden: A Legal and Ethical Review of the NSA Leaks from June 2013

"I can show you proof that the lack of this really failed. And when you lose 3000 people, that proof is pretty compelling" (Macaskill & Dance, 2013). Stewart Baker, a former United States National Security Agency (NSA) general counsel member, gave this quote in response to the information gathering system used after the September 11th attacks and allegedly 50,000 to 1.7 million NSA documents Edward Snowden leaked to The Guardian on June 5, 2013. Edward Snowden, a systems administrator of the information contractor Booz Allen Hamilton hired by the NSA, revealed how much data the NSA collected and how they collected it. However, other options were available to share the information instead of releasing top-secret files to the public. This paper examines the Edward Snowden incident, focusing on the situation leading up to the leaks, what information Snowden leaked, the legal and ethical ramifications, and potential strategies the NSA could have implemented to avoid this incident.

The September 11th attacks from al-Qaeda sparked a realization that terrorist attacks can occur from any group or nation-state and that the US needed to change how they perceived threats. So, the US government "authorized the NSA to expand its efforts to gather vast amounts of electronic data to identify and stop future terrorist assaults" (Boehme, 2017, p. 14) by authorizing the USA PATRIOT act, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism. This act granted the "authority to intercept wire, oral, and electronic communications relating to terrorism" and "…computer fraud and abuse offenses" ("USA PATRIOT ACT," 2001). With these new extensions, the NSA decided to "collect everything it could, then develop the means to search the data afterward to find patterns of suspicious activity" (Boehme, 2017, p. 16). From there, the massive collection of

personal metadata, data about electronic communications data (time, size, and who was communicating), started to form.

Edward Snowden started his career in the United States by enlisting in the Army in 2003; however, he would leave the armed forces after breaking his legs in a training exercise. He then signed up to work with the NSA in 2005, quickly moving up the ranks to a position at the Central Intelligence Agency (CIA). While working for the CIA, Snowden's views on the US espionage programs began to change as he witnessed CIA agents "persuade" a Swiss banker to become an informant by getting the man to drink and drive and then bailing him out of prison. Snowden left the CIA in 2009 to work for Dell to advise and assist the American and Japanese military on cyber defense against Chinese attackers. Finally, Snowden went to work for Booz Allen Hamilton in 2012, where he accessed the NSA documents about their surveillance systems and the data they collected on the American people (Greenwald et al., 2013).

On May 30, 2013, Edward Snowden flew to Hong Kong with 1.7 million top-secret NSA documents. He acquired these documents via Booz Allen Hamilton and his position as a network administrator. He created a spider or web scrapper and downloaded any file he could to a removable USB drive. These files contained a wide variety of information. Some of the leaked documents are about collecting millions of users' Verizon telephone records, targets for overseas cyberattacks, the UK's intelligence agency taking an active role in data collection, warrantless wiretaps, the ability to access user data from cellphones, and spying on anyone and everyone (Szoldra, 2016).

However, Snowden did not directly release the documents to the public. Instead, Snowden handed the documents over to trusted journalists, where Snowden had strict rules on what could and could not be published. These rules required that the items published or mentioned did not

reveal or damage national security but instead created discussions about privacy and the wrongdoings of the NSA. He also "did not download information about rosters of employees, assignments, or locations, and he did not provide any information on people working for the NSA or any other agency for fear of exposing them to danger" (Boehme, 2017, p. 36).

However, even though Snowden prompted discussions and pushed for more restrictions for the NSA and data collection agencies, he still leaked highly classified top-secret government information. Because of the leaks, Snowden was charged with two counts of the Espionage Act and theft of government property, each lasting a sentence of ten years. The Espionage Act of 1917 originates from when the US entered World War I, where any attempts to attain government information "with the intent to harm the United States or acquire code and signal books, photographs, blueprints, and other such documents with the intention of passing them to America's enemies" (Office of the Director of National Intelligence) would be a violation. This act was used multiple times from 1917 to today, primarily arresting dedicated spies or foreign informants. However, Snowden did not give any information to America's enemies, unless the US considered the public or journalists as enemies, or likely intended to harm the United States. Snowden did not sell the data to other countries; he selectively chose which data should and should not be made public, and he publicly stated, "I didn't cooperate with the Russian intelligence services — I haven't and I won't… I destroyed my access to the archive. ... I had no material with me before I left Hong Kong" (Davies, 2019). However, Snowden did steal government property. Since Snowden was a contractor with the NSA, he did not own the data he took to Hong Kong.

However, from an ethical viewpoint, both sides are fighting for a just cause. The NSA wants to collect the data to prevent future attacks and have a greater sense of awareness of both

the American population and the foreign governments. The idea is that if they have the whole haystack, it allows the NSA to have all the needles. However, according to Dahl, “of the 109 failed plots within the United States since 9/11, more than 75 percent were foiled at least in part because of traditional law enforcement methods, and not - from what we can gather - from NSA surveillance” and “These NSA programs do appear to be important for preventing terrorist attacks, and they make sense from an intelligence perspective. But their greatest value concerns threats overseas” (2013). The collection of data seems to help prevent terrorism plots that originate overseas but does not seem to help when it comes to domestic attacks.

On the other hand, Edward Snowden fully believed that what the United States was doing was wrong and unconstitutional due to warrantless searches. However, it exposed and showed weakness in the US’s most secretive agency and, if not done correctly, could have damaged national security. However, there were other options Snowden could have taken that were not as drastic, such as reporting his concerns to his chain of command or enacting the Whistleblower Act, which allows government employees and contractors to report concerns to the US Office of the Inspector General. However, there are valid concerns that he might have lost his clearance, the NSA could have demoted or fired him, or the NSA would not change or alter its methods. The NSA did an inside investigation and claimed that Snowden did not report his concerns. However, Snowden refutes that claim.

Ten years later, Snowden is a permanent resident in Russia, wanted in the United States, and the NSA has more restrictions on collecting data and thousands of documents lost to the public, with data privacy concerns still active. However, there were options and methods the NSA could have implemented to avoid this issue. Edward Snowden was not the cause of the problem but the byproduct of an ongoing issue. First, they could not have collected and amassed

an extensive database of personal data, but that would defeat the purpose of the counter-terrorism efforts. However, other people at the NSA or contracted with them likely had concerns with the data collection. So, it is likely that the NSA did not listen to workers' complaints or ideas when making the decisions. One fix is to have dedicated liaisons or have time set aside for the subordinates to raise concerns or issues. Another fix would be to have a separation of duties and multiple system administrators who only have access to some network areas. That way, one person does not know or have access to everything. There should have been no reason that Snowden had access to 1.7 million documents, where he may only need access to 10,000. So, stricter access control and better confidentiality would have limited the amount of data anyone had access to. Finally, disabling USB and removable media devices would have stopped or slowed the leaks. If Snowden had not used a removable media device, he could not have transferred the documents to the journalists without giving his laptop to them. The NSA would revoke his permissions, and he would have lost his access.

All-in-all, Edward Snowden caused an uproar concerning data privacy and the US government collecting and accessing personal information by leaking 50,000 documents to journalists in Hong Kong. While it was illegal and broke the rules and regulations in place, he was ethically just. Many users of devices and internet service providers believe that their data is private and secure, so the revelation that the NSA, one of the most secretive agencies, has full access to all their documents would be enough to raise concerns. However, there were some ways that the NSA could have prevented this situation from arising, and proper implementations of these methods would have either slowed or hindered Snowden in his efforts.

References

Bamford, J. (2020, January 8). *Edward Snowden: The untold story*. Wired. https://www.wired.com/2014/08/edward-snowden/

Boehme. (2017). Edward Snowden: Heroic Whistleblower or Traitorous Spy? Cavendish Square Publishing LLC.

Dahl, E. (2013, July 25). Discussion point: It's not big data, but little data, that prevents terrorist attacks. Discussion Point: It's not Big Data, but Little Data, that Prevents Terrorist Attacks. https://www.start.umd.edu/news/discussion-point-its-not-big-data-little-data-prevents-terrorist-attacks

Edgar, T. H. (2017). Beyond snowden : Privacy, mass surveillance, and the struggle to reform the nsa. Brookings Institution Press.

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

Greenwald, G. (2013, June 22). *On the Espionage Act charges against Edward Snowden*. The Guardian. https://www.theguardian.com/commentisfree/2013/jun/22/snowden-espionage-charges

Greenwald, G., MacAskill, E., & Poitras, L. (2013, June 11). *Edward Snowden: The whistleblower behind the NSA surveillance revelations*. The Guardian. https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance

Higgins, M. (2016). Edward snowden : Nsa whistle-blower. ABDO Publishing Company

MacAskill, E., & Dance, G. (2013, November 1). *NSA files decoded: Edward Snowden's surveillance revelations explained*. The Guardian. https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. No. 107-56 (2001), https://www.govinfo.gov/app/details/PLAW-107publ56.

Office of the Director of National Intelligence. (n.d.). *The Espionage Act of 1917*. Intelligence. https://www.intelligence.gov/evolution-of-espionage/world-war-1/america-declares-war/espionage-act

Office of the Insepector General. (n.d.). *Whistleblower protection*. Federal Trade Commission. https://www.ftc.gov/office-inspector-general/whistleblower-protection