From High School Drop Out to International Man of Mystery

Matthew Gaudrault

Charleston Southern University

Principles of Cybersecurity CSCI 405

Patrick Hill

1/31/24

In the 1990s as the internet was just starting to become available to general public, I remember the loud screeching of the modem which let me know that I was about to be connected to my America Online account. Once I was connected, my friends list would populate and let me know who else was at the computer on their account or could go to an online chat room and message with anyone else in there. The internet was so new to most of us that we did not know really what we were doing or what data we were creating on the web. There were not many guidelines and our parents were encountering this new area of the web as well. No one was thinking about how the glamorous new world wide web would grow to be such an integral piece in our day to day lives. With all the access we experience now though, it increases how susceptible we are to the criminals and bad actors that are around the world. To protect us from this new threat, there has been great steps in the world of cybersecurity. According to IBM, "cybersecurity is any technology, measure, or practice for preventing cyberattacks … [which] have the power to disrupt, damage or destroy businesses" (IBM). What is at the heart of the protection of cybersecurity is data. Data is being created with everything you do and access while online and most people do not even understand how much data they are creating on a daily basis. On the internet someone could go back and pull up transcripts of what I said in that AOL chat room over 20 years ago as a pre-teen boy. As I am now a parent, I start to think about how much data will be accumulated on her before she is 18. The world has a surplus of data and is collecting every click of the mouse and every letter typed, but this leads to the question of who is collecting this data? The different applications you download on your phone or computer have end user agreements that have you agree to allowing them to collect your data most of the time, but are they the only ones? This is where Edward Snowden comes into the picture in 2013. In this paper I will go over who is Edward Snowden and what he did, what his leak meant to the government and any legal issues it caused, and the ethics of his actions as well as if there could have been steps taken to styme the leak.

Who is Edward Snowden

From high school drop out to international man of mystery, who is Edward Snowden? Born in North Carolina, he grew up to be a computer whiz who did not complete high school and went straight into working with computer systems of varying levels. Even though he only had his GED he was able to end up working for the likes of the Central Intelligence Agency (CIA) and the National Security Agency (NSA). While working as an American intelligence contractor with top secret clearance, he started to notice how much data was being collected on Americans that were not part of any investigation. He raised his concern to his supervisors but was ignored per an article in the Bill of Rights in Action (BRIA)(Jennings). After he felt that this was ignored by superiors, he felt he needed to get this information out to the American public and be a whistleblower on the NSA for what he considered an overstep of data collection. In 2013, Snowden traveled to Hong Kong and met with multiple reporters and shared what he had discovered. Both The Guardian and The Washington Post released articles about what Snowden had shared but did not revealing their source. Snowden eventually came forward and left Hong Kong planning to find asylum in South America, but did not make it past Russia as USA had suspended his passport. After being stuck in the international airport section in Moscow, he was eventually allowed to stay in Russia after applying for asylum in about 20 countries. He is still in Russia to this day.

Legal and Ethical Issues

Since Snowden was working with the NSA, he had to sign a non-disclosure agreement about his statement of work. With this signed he was not allowed to share anything that he worked on or talk to anyone about his work. This is probably the biggest legal hurtle to try and fix. It is pretty cut and dry that he was not allowed to talk much less record and make copies of his findings, and then share with reporters what he had discovered. Snowden has also labeled a traitor and could be charged in violation of the Espionage Act per NPR.org. This second point of being a traitor or spy is where it becomes harder to proof one way or the other but there tend to be two ways of thought for this, he is true patriot for

sharing what was unethically being completed, or that he hurt the USA with what he did and he is a traitor. In Snowden's interview with NPR he states, "I realize we have been violating, in secret, the Fourth Amendment of that Constitution for the better part of a decade, the rate of violation is increasing, the scope of the violation is increasing with every day, that we are committing felonies in the United States under a direct mandate from the White House billions of times a day" (Davies). From the statement, as long as he is being truthful, it shows that Snowden was trying to make up for the unethical practices he encountered. He was witness to the US government recording all of citizen's data including their emails, phone calls, google searches, and phone movement. This was part of the idea of the NSA to go ahead and collect as much data as possible and then if needed they could go back and follow the digital trail of each and every person involved. Working in the cybersecurity field myself, such a massive store of data worries me not only because of the means of how it was gathered, but how safe is while it is being stored? Snowden mentions in his interview with NPR that his work started with him investigating China and seeing what data collection techniques were being used there. This is just one example of governments hacking into other governments to see what they have and seeing what can be accessed. What would happen if another country was able to break into that NSA database and get access to the mass treasure trove of data on US citizens? Many nefarious actions could be planned off of that data, even the phone movement alone would be able to be used for patterning of US citizens. This is where ethics need to be evaluated more closely within cybersecurity. Snowden feels resolved in his ethics and has stated that he will come back to the US and stand trial if he can "be able to tell the jury why I did what I did, and the jury has to decide: Was this justified or unjustified." (Davies). This would give the power to his peers and let them decide if he did the correct ethical decision.

As this was in the past, one deciding factor on if Snowden was justified is to look at what changes were made because of his release of NSA data collecting tactics. There are both examples of good that has come from the leak as well as some most likely unintended side effects from it. You could

argue that Snowden was justified in his release of data as it did change government policy with the collection and surveillance of citizens with the USA Freedom Act. Since a change at the highest level was made, it would be a fair conclusion that Snowden could have been correct in his concerns and he was valid in pushing the need for change. The other face of the coin on the situation though is all the trouble he caused internationally for the USA. One big issue was the timing of the leak, the night before the Obama-Xi summit. This summit was put in place to give the USA a chance to discuss cybersecurity with China as they had been very brazen with many of their cyber-attacks. Since the paper came out the night before summit, it gave China an easy way out where they just stated “We don’t do hacking. You do it a lot more than we do." (Kaplan). This is just one example where Snowden set back international relations with having his story be front page news. International governments were all trying to test each other’s cybersecurity efforts and the USA just had theirs shared for the whole world to see. This really increased distrust in the US government as Obama’s director of national intelligence was on record stating “No, sir … not wittingly” when asked if the NSA collects data on the millions of Americans (Kaplan). This was before the leaks were released so after Snowden’s reports were shared showing that NSA has been collecting all this data it made people trust the US government even less as they have been on record denying what they were doing.

How could it have been stopped?

Many of the correct steps for protecting data were followed like the requirement of a NDA and background checks before access was granted, but as Snowden did not have any previous issues and had been performing this work for years it was understandable for his superiors to be caught unprepared. One big red flag that was mentioned in the BRIA article was that Snowden persuaded coworkers into letting him borrow their passwords. This is a big issue in cybersecurity as people can sometimes be the weakest links in IT infrastructure. I’m sure his team did not think much of it as Snowden had been doing the work for so long, but this goes to prove the issue an insider threat can cause. Another step that

could have been used to make sure that the data was not leaked is a requirement of data tracking software, so that the watcher can be watched. Since the data was being downloaded on to local laptop hard drives, it could have sent up a flag as that would not have been the typical storage device while performing that kind of work. The last way that I see to have stopped the leak, is to have paid more attention to Snowden's initial concern. We he went to his management and raised his concern about the data collection processes, if there would have been some communication showing that management heard him and was working on escalating his concern or working on a way to mitigate his concern, then he most likely would not have felt the need to share that information with the journalists. If the journalists weren't involved then majority of the US citizens would have remained blissfully un aware of the data being collected off of them.

Conclusion

So now that we have discussed who Edward Snowden is, what he did, the legal and government issues, the ethical issues, and what could have been done to stop his sharing of leaked data, what are your thoughts on his guilt or innocence? No matter which way you lean on that decision, it should open you eyes to how much data is all around us. Snowden leaked the NSA's PRISM program which "collected the content of emails, photos, and other media from the servers of nine Internet service companies (Microsoft, Google, Apple, Yahoo, AOL, Facebook, YouTube, Skype, and Paltalk)." (Jennings). If data is being stored whenever you do any of the above listed things on the web, and you use the web from your phone throughout the day, how much data do you think you create each day? Now multiply that by 365 and your age. This is why I am curious as to what kind of world my daughter will grow up in as the amount of change, I have noticed with the internet in my life so far as been unimaginable. Personally, I feel that Snowden had good intentions but not the best execution of those intentions. I do not know what the correct path forward should have been but the steps he took definitely changed the cybersecurity world forever.

References

Davies, D. (2019, September 19). *Edward Snowden speaks out: "I haven't and I won't" cooperate with Russia*. NPR. https://www.npr.org/2019/09/19/761918152/exiled-nsa-contractor-edward-snowden-i-haven-t-and-i-won-t-cooperate-with-russia

IBM. (2020, November). *What is cybersecurity?*. IBM. https://www.ibm.com/topics/cybersecurity

Jennings, P., & Martz, C. (2016). *Edward Snowden, the NSA, and mass surveillance*. Political Conflict, Spring 2016 (31:3). https://www.crf-usa.org/images/pdf/gates/snowden_nsa.pdf

Kaplan, F. M. (2017). *Dark territory: The secret history of cyber war*. Simon & Schuster Paperbacks.

Ray, M. (2024, January 11). *Edward Snowden*. Encyclopædia Britannica. https://www.britannica.com/biography/Edward-Snowden