The Case of Edward Snowden Data Mining Leaks

Miles Young

General Instructions

1. For each page, synthesize the reading and research by writing in complete sentences in essay format.
   a. Use the green instructions in the notes below each page to focus your research and writing.
   b. Write about each question, prompt, or process provided in those notes.
   c. Write a full page of text with lots of detail (about 250 words).
      i. Don’t generalize so much that your writing is devoid of detail.
      ii. Don’t repeat yourself.
   d. Cite each source by adding a hyperlink in the Title of the Article or law.
   e. Do not change the template:
      i. Text must be 14 point Lato left-justified type.
      ii. Refrain from adding extra margins or double spacing.
      iii. Do not bullet the paragraphs. Write in essay format only.
   f. Add additional pages if you need more room.

2. Add all sources to the Bibliography page.
   a. Include author, year, title, publisher, and URL.
   b. Number or bullet them using the list button.
The 2013 article *Prism’s Legal Basis* by Margot Kaminski contains the precursors to the laws that allowed data collection on US citizens. In 1978, Congress authorized collecting data on foreigners, and in 2001 with the PATRIOT act allowed the collection of business records which included location data and timestamps (*Kaminski 2013*).

The first evidence of large scale data collection was reported in the article *NSA collecting phone records of millions of Verizon customers daily* (2013) by Glenn Greenwald, which was the first article about FISA, PRISM, and how the NSA collected data. Greenwald reported on the the millions of records Verizon was giving to the NSA daily using a single FISA court order, which included location data, time, duration of calls, and identifiers, but not the audio of the calls (*Greenwald 2013*).

The 2018 article *NSA surveillance programs live on* by Laura Hautala reports that US lawmakers reauthorized PRISM and Upstream without changes like requiring warrants, and some lawmakers argue that it is important to fight “foreign terrorism.” The overall response from US citizens has been minimal due to a lack of interest, but some groups like the ACLU are still fighting for privacy protections (*Hautala 2018*).

In 2008, amendments to the 1978 “Foreign Intelligence Surveillance Act (FISA)” allowed the US government to use “single court order” in order to monitor people who live outside of the US (*Kaminski 2013*). Kaminski further states that this allowed the accidental collection of data of people who lived in the US, as the law required only a “reasonable belief” of the location due to the potential for communicating with people outside the US. The types of data was expanded to include “email, search history,” and other personal data (*Kaminski 2013*).

The 2013 article *Edward Snowden and the NSA files* by Mirren Gidda contains information about how Snowden was able to avoid arrest. On June 9th, Snowden first revealed himself as the leaker and then went directly to Hong Kong (*Gidda 2013*). Gidda then reports he went to Russia on June 23rd, and then on July 12th Snowden reports that he was requesting temporary asylum in Russia before potentially going elsewhere. The article also reports during this time more leaks were occurring about the information Snowden had.
The main problem that Edward Snowden revealed was about the amount of data the NSA was secretly collecting about US citizens. The 2013 article *U.S., British intelligence mining data* by Barton Gellman and Laura Poitras reports on the amount of data the NSA’s PRISM is able to collect, along with the sources that it gets data from. The article reports that Facebook, Google, Yahoo, and others were forced to give information to the NSA through broad court orders from secret courts. As much as “1 in 7 intelligence reports” used the data, and that companies needed to build backdoors or be hacked in order to allow the NSA to collect that amount of data (Gellman 2013). The 2014 report *Edward Snowden: Leaks that exposed US spy programme* from the BBC contains the many scandals that Snowden’s information had including tapping internet cables, placing bugs in EU offices, wiretapping German Chancellor Angela Merkel’s phone, and spying on allies. How this problem was created was due to sections of the 2008 FISA Authorization Act which allowed more data to be collected with single warrants and allowed data from US citizens to also be collected (Kaminski 2013).

Why massive data collection is a problem is that it reduces privacy on the internet, and allows the NSA to track more people at the same time. The 2018 ACLU blog post *The NSA Continues to Violate Americans' Internet Privacy Rights* by Patrick Toomey argues that US citizens do not know what data was collected about them due to the fact that warrants are not required for the NSA when collecting this sort of data. Toomey includes an example of when emails were used as evidence, but the US government did not use a warrant to get the information thus making it potentially unconstitutional.
Consequences and Laws

Since the NSA was using the FISA and other laws correctly, there were not many regulations that were broken as a result (Kaminski 2013).

The actions some government agencies have taken as a result of these revelations could be due to more public scrutiny. The 2016 article Snowden disclosures helped reduce use of Patriot Act provision by Spencer Ackerman reports on the FBI has shifted away from using FISA court orders to collect large amounts of data due to different legal interpretations. However, the 2018 EFF post Newly Released Surveillance Orders Show That Even with Individualized Court Oversight, Spying Powers Are Misused by Aaron Mackey and Andrew Crocker show that the US court system has been limiting how US government agencies can collect data. Mackey examines court documents that indicate US judges have been ordering data that was improperly collected destroyed or limiting the amount of surveillance even before Snowden released information about the NSA’s activities.

The article Here’s everything we know about PRISM to date (2013) by Timothy B. Lee details how companies like “Microsoft, Yahoo, Google, Facebook and [others]” responded to the revelations that the NSA was monitoring their communication by firmly denying that they were passing information to the NSA. Since it is hard to prevent secret court orders with collecting data, it is difficult for many companies to prevent this from happening again. The 2015 article Europe’s highest court strikes down Safe Harbor data sharing between EU, US by Sebastian Anthony reports that one way countries in the EU will prevent this is by requiring EU data about citizens be kept in the EU, which would then limit data the NSA could collect as it would be in different countries.
The 2013 video The NSA and surveillance ... made simple from The Guardian illustrates the types of data the NSA collects on people, and what types of data is kept. This video contains an example of while the actual data the NSA collects is deleted in 3 days, it keeps metadata of the receiver and sender of the data for up to a year to be able to build profiles of where people are and who they communicate with.

© 2013 The Guardian
Ethical Analysis of the Major Player(s)

One of the only major human players in this case would be Edward Snowden who released information to journalists about the NSA’s data collection. The article [US expects fallout from Snowden leaks for years to come](https://www.latimes.com/world/la-na-snowden-nsa-data-20180907-story.html) (2018) by Deb Riechmann illustrates the power that Snowden briefly held over the NSA in regards to their secret processes they were using for data collection. However, when Snowden gave the documents to journalists he gave up that power and gave some of it to journalists who could then publish information about illegal activities ([Riechmann 2018](https://www.latimes.com/world/la-na-snowden-nsa-data-20180907-story.html)).

One theory that could be used to analyze Snowden’s actions would be utilitarianism. The 2016 video [Utilitarianism](https://www.youtube.com/watch?v=Qv6SvTa4dZc) by Hank Green defines utilitarianism as using the action that would “produce the greatest good for the greatest number” of people. Therefore, when Snowden recognized the dangers of the NSA collecting private data, releasing that information would allow more people to know about it, and even take steps to prevent it. One example of this is Snowden and the journalists who had the files instead of releasing them in bulk, they only released information about illegal activities that the NSA did ([Riechmann 2018](https://www.latimes.com/world/la-na-snowden-nsa-data-20180907-story.html)). Another example is in the 2013 interview [Snowden Says He Took No Secret Files to Russia](https://www.nytimes.com/2013/06/06/us/snowden-says-he-took-no-secret-files-to-russia.html) by James Risen, where Snowden stated that he made sure not to pass any information to China or Russia that could compromise what the NSA was doing. Risen also reports that Snowden stated that if people knew about the programs it would be different that when people did not know as then they could not make educated decisions about what data sent over the internet. Therefore using utilitarianism Snowden was morally justified as more people were able to learn about what data was being collected along with providing the greatest good to the public to be informed about the illegal programs like PRISM the government used.


Acknowledgements


