Glenn Findlay 11/2021

Edward Snowden: Hero or Traitor?

On May 20, 2013, NSA contractor Edward Snowden fled to Hong Kong with a vast quantity of highly classified documents he had downloaded from his workplace at an NSA facility in Hawaii. Over the coming weeks he would share thousands of these documents with journalists. They contained many revelations about the extent of the NSA's surveillance capabilities, which included secret programs that enabled them to defeat trusted security measures and collect data on a scale that few would have imagined.

The programs revealed by these documents ignited a debate about whistleblowing and government surveillance. Are such programs necessary to ensure the safety of Americans, or were they a dangerous and even illegal overreach by government intelligence? Should Snowden be applauded for having cast light on dubious government programs, or should he be arrested and prosecuted as a traitor who revealed some of his country's most closely guarded secrets?

In this essay I will work to address each of these issues in turn. First I will provide more detail into the nature of the programs revealed. Then I will cover important points in the relevant debates surrounding whistleblowing and government surveillance, and explore the ethics and laws involved.

Who is Edward Snowden?

Snowden was born into a family with a tradition of public service. His father and maternal father were both officers with the coast guard, and his mother was a chief deputy clerk at the U.S. District Court for the District of Maryland[1]. In 2003 he enlisted in the army because, in his words, "I felt like I had an obligation to help free people from oppression" [2] but he was discharged after breaking both legs in a training accident. Shortly after he began to work in IT security at CIA facilities, where he was quickly successful due to his understanding of the internet and his talent for programming.

According to *Ars Technica*, Snowden had been active on the site's online forums for many years under the pseudonym "TheTrueHOOHA" and had posted as recently as 2012. On many occasions TheTrueHOOHA showed strong support for U.S. security agencies, and in January 2009 criticised the

New York Times for publishing previously-secret details of U.S. attempts to sabotage Iranian nuclear infrastructure. Their anonymous sources should, he said, "be shot in the balls." [3]

As his career progressed, Snowden became disillusioned with U.S. security agencies and their impact on the world. In his words, "I realised I was a part of something that was doing far more harm than good."[1] At some point he became interested in internet freedom organizations such as the Electronic Frontier Foundation and the Tor project.

Investigators believe that Snowden began amassing documents describing government surveillance programs in April of 2012, [4] when he was at that time working as a contractor for the NSA. He continued to do so until May 2013, when he fled to Hong Kong and began to share his trove of top-secret documents with journalists. Just over a month later he boarded a flight to Moscow, and he has remained in Russia since. According to Snowden, he had destroyed or shared with journalists all the classified documents in his possession before leaving Hong Kong.[4] He also claims that he never intended to remain in Russia, but that he was left stranded there when the U.S. cancelled his passport.[4]

Snowden chose not to opt for anonymity because, in his words, "I have no intention of hiding who I am because I know I have done nothing wrong." [1] In public statements, intelligence officials have sought to minimize his work for the NSA by describing him as a low-level systems administrator. He pushed back vehemently against this characterization of his work, saying "I was trained as a spy in the traditional sense of the word in that I lived and worked undercover overseas – pretending to work in a job that I'm not – and even being assigned a name that was not mine… I developed sources and methods for keeping our information secure in the most hostile and dangerous environments in the world." [5]

What was revealed?

The documents that Snowden shared with journalists revealed a number of secret information-gathering programs of unprecedented ambition and scope. Some estimates have placed the number of documents he shared with journalists in the hundreds of thousands,[4] but here I will try to highlight some of the most outstanding revelations.

The NSA divides online surveillance into a couple of broad categories; 'upstream' and 'downstream.' Upstream surveillance generally involves the direct collection of internet traffic as it passes

through infrastructure such as fiber optic cables. ‘Downstream’ surveillance, on the other hand, describes the collection of data stored by companies such as Google, Facebook, Microsoft, and others.

Documents leaked by Snowden describe PRISM, a downstream surveillance program that allowed the NSA to directly reach into data housed by Google, Apple, and other cloud storage companies to extract emails, photos, contact lists and many other kinds of data. It also allowed for the agency to collect ‘huge quantities of raw internet traffic at major network exchange points’ by scanning in-transit internet packets for particular keywords. [6] The NSA had broad powers to obtain this data on communications between foreigners so long as they were deemed to be relevant to the broadly defined category of ‘foreign intelligence information.’ [7] Communications between foreigners and U.S. citizens could also be collected, meaning that potentially huge amounts of American communications and other sensitive data could also be swept up, without the need for a warrant.[7]

The documents revealed by Snowden also included a top secret court order issued by an intelligence court that required Verizon to provide the NSA with information on all the calls in their systems, updated on an ‘ongoing, daily basis’ over a 3-month period.[8] This data did not include the content of the calls themselves, but it did include certain ‘metadata’ including phone numbers, call time and duration, and location data. Members of congress later confirmed that similar orders had been issued every 3 months for years.[9]

The leaked documents also describe the ‘MUSCULAR’ program wherein the NSA would collect data by tapping directly into fiber optic cables owned by companies such as Google, Yahoo, and others. The PRISM program had some limitations in that much of the raw traffic collected was encrypted, and ‘PRISM requests are relatively limited in scope.’ [6] By tapping into data connections between data storage centers and within company security perimeters, the NSA could collect vast amounts of unencrypted traffic. The NSA took care to place these taps overseas, where the agency is subject to less restriction and oversight.[10] Legally, they are allowed to assume that all data collected outside the U.S. belongs to foreigners and collect data in a way that would be illegal in the U.S. itself. Happily for the NSA, many companies will backup their data across various data centers, replicating data for the purposes of backup and universal access. This means that the data of many Americans would be collected on these taps, even if they had never travelled overseas.[10]

The documents leaked by Snowden also detail ongoing efforts by the NSA to defeat or circumvent standards of encryption. Even with powerful supercomputers at their disposal, government intelligence agencies often struggle to circumvent modern encryption standards.[11] Their best option is often to go over, under, or around encryption - but rarely through it. In the words of cryptographer Adi Shamir, “Cryptography is typically bypassed, not penetrated.” [11] One approach used by the NSA was to collaborate with technology companies to intentionally insert weaknesses or ‘backdoors’ into commercial encryption software.[12] This program, which appears in leaked slides as “SIGINT [signals intelligence] enabling”, received $254.9 million in funding in 2013 alone.[24] In another case, the NSA succeeded in stealing encryption keys used by a SIM card manufacturer named “Gemalto” and based in the Netherlands, allowing them to decrypt communications on vast numbers of mobile phones around the world.[11]

It is difficult to know what happens internally at the NSA, but there are some signs that growing pains set in as the agency began to absorb previously unfathomable quantities of data. Databases became clogged with vast amounts of spam emails,[6] analysts complained of ‘drowning’ in data, and some NSA officials grumbled about the ballooning costs of ‘collect-it-all’ style programs.[13] In response, the NSA began to develop sophisticated tools to efficiently trawl through data collected. One such tool, ‘XKEYSCORE’, was described by *The Intercept* as a kind of ‘google for the world’s private communications.’ [14] Using this tool, an analyst could easily filter and study online activity. One leaked slide displays a search in which an analyst queries the system for “all individuals in Pakistan visiting specific German language message boards.” [14] XKEYSCORE also provides powerful tools for studying the online activity of individuals – an analyst can conduct sweeping searches simply entering a person’s email address, name, or telephone number ‘with just a few clicks.’ Apparently, this tool was used in hacking Gemalto’s network, by enabling spies to stalk the online activity of employees and uncover their usernames, passwords, and email. [14]

One recurrent issue in NSA offices was a tendency of analysts and officers to use their surveillance tools to spy on love interests, a practice referred to as "LOVEINT" by NSA employees. Documents leaked by Snowden reveal that internal audits found the NSA breaks its own privacy rules thousands of times a year. [25]

Were these programs legal?

In United States law the cornerstone of privacy is 4th amendment, which says that "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." This is to say, a person's privacy can only be violated after a warrant is issued, and the warrant must specifically detail the 'persons or things to be seized'. In 1986, the Electronic Communications Privacy Act (or ECPA) clarified that electronic communications and data are protected, and law enforcement will need a warrant to acquire them.[15] Certain kinds of metadata such as records about phone use have a lower level of protection, however, and can be obtained by law enforcement with a court order. In general court orders require a lower standard than a warrant and are easier to obtain.

Legally, the Fourth Amendment is understood to protect U.S. citizens and residents only. From a legal standpoint, it is very easy for the NSA to read the emails (for example) of foreigners provided they can in some way be obtained. In the case of the overseas tapping of fiber optic cables, the NSA is allowed to collect such data en masse by assuming that the targets will be foreigners.[10]

In 1978, the Foreign Intelligence Surveillance Act (FISA) was passed into law, with the intention of curtailing the NSA's capacity to spy on Americans. At that time, surveillance by the NSA of activists, civil rights leaders and others had caused a widespread backlash, and this law specified for the first time that the NSA was for the purpose of foreign surveillance.[16] If they believed that a foreign agent or spy was operating in the U.S. they would need to obtain a warrant from a Foriegn Intelligence Surveillance Court, or FISC, a secretive court where cases are presented behind closed doors and decisions are made away from the public view. As of 2008, the Fisa Amendments Act allowed for the warrantless collection of communications, in the case where at least one end of the exchange is outside of the U.S. It also clarifies that no warrant is needed for surveillance targeting a U.S. person overseas.[16] This further broadened the possibilities for the data of Americans to be swept up in foreign surveillance, and provided the legal basis for programs such as PRISM where vast amounts of communications between Americans and foreigners was collected.

According to the NSA, court orders such as the once compelling Verizon to share call metadata with the NSA were authorized under section 215 of the Patriot Act, which allows the government to order companies to collect “tangible things” that aid in a terrorism or espionage investigation. This interpretation of the law was accepted for years by FISC judges.[16] In 2015, however, a federal appeals court ruled in favor of the A.C.L.U and declared that these requests were illegal and used an interpretation of that language that was overly broad and beyond the scope of the law’s original purpose.[17]

A great deal of the NSA’s overseas surveillance activities are authorized by Executive Order 12333, signed in 1981 by President Raegan, which authorized the collection of any intelligence relevant to ‘national defense’ as long as it is not specifically prohibited by any other law.[16] In general, these activities are outside the scope of the FISC and receive very little congressional oversight. The NSA may be required to justify that the collection of data is relevant to defense, but the agency will only need to make this case to itself and individuals in the executive branch.[10]

By and large, the NSA did operate within the confines of existing laws. Loopholes were exploited creatively and aggressively, however. In particular, lax rules regarding the surveillance of foreign communications and the overseas collections of data allowed them tremendous leeway in collecting data on Americans in ways that would otherwise require a warrant. Some of the programs revealed required very little oversight from courts or from Congress. Many of their surveillance activities were approved by FISC judges. As to whether the laws under which the NSA operated were consistent with the 4th amendment is a broader question that I will return to later.

In 2015, the USA Freedom Act was passed. It banned the bulk collection of metadata via court orders and constrained requests for such data to be more specific.[18] It also allowed companies to disclose more information about FISA orders they receive, and moderately increased the amount of information about FISC court rulings that would be accessible to the public. [18]

Were these programs ethical?

While U.S. citizens and residents are protected by the Fourth Amendment, the rights of foreigners do not appear to be well defined. This raises an obvious ethical issue - foreign people obviously have rights - and also opens up enormous loopholes that have allowed the NSA to scoop up huge amounts of