Colby Goettel

Reed

English 312

25 February 2014

NSA Snooping and Counter-terrorism

The US government has been spying on its citizens since at least the 1950s. Recent revelations from whistleblowers like Bradley Manning and Edward Snowden have brought many of these programs to light. The full extent of the NSA and other divisions of government is still unknown, but what is known is startling and terrifying. It presents a clear and present danger to the people of the United States by infringing on their right to privacy. Furthermore, there is no justification in these programs, meant to stymie terrorism, because they have only stopped one terrorist plot, which was simply wiring $8,500 to a Somali militant group.

In 2001, the US government legalized domestic and foreign spying with the Patriot Act. In 2007, they extended the reach of their spying with a secret NSA program called PRISM. Prism is a mass, metadata collection program launched in participation with the British spy agency, the Government Communications Headquarters (GCHQ), and large, American corporations like Google and Apple. The requests to these companies are made under §702 of the FISA Amendments Act of 2008 which allows the Attorney General and the Director of National Intelligence to target non-US citizens who are not currently in the United States. Under FISA, the Foreign Intelligence Surveillance Court, which operates in secret, (Schneier 2013) was set up to hear cases under Prism and other secret programs.

The government has been eavesdropping on American citizens since the 1950s under a program called Project Shamrock. Once computers got to the point where they could be used for

mass data analysis, computerized programs such as HARVEST were used for eavesdropping. In 1978, the Foreign Intelligence Surveillance Act was put in place with allowed for metadata collection (both hard and soft) of foreign powers and US citizens suspected of spying or terrorism. When the order was issued, it only applied within the United States. Since the FISA Amendments Act of 2008, this power has extended to foreign entities. This Amendments Act also makes previous warrantless wiretapping done by the NSA through AT&T illegal.

Prism, with a confidence interval of only 51% that the target is not a US citizen, can perform “extensive, in-depth surveillance on live communications and stored information” (Greenwald and MacAskill 2013) such as a “phone call, e-mail or chat” (PRISM slide 2) from Microsoft, Yahoo, Google, Facebook, PalTalk, YouTube, Skype, AOL, and Apple (PRISM slide 5w and Upstream slide).

Unless there is a backdoor present in the system, it is impossible for anyone to gain access to secure information. However, if the information is not stored securely then there is no promise of protection. All information sent over the Internet needs to be encrypted using the most up-to-date encryption standards. Old standards, such as MD5, have been compromised and are no longer considered secure. The computing world is constantly changing and evolving and the onus is on users and corporations to ensure that all information is properly protected.

The computing overhead to encrypt and decrypt information used to be enormous. For that reason, the standard was to only encrypt sensitive data and transmit everything else as plain text. Since computers have evolved exponentially in the past few decades this is no longer needed. In 2010, Gmail switched all of their e-mail to HTTPS and experienced an increased CPU load of only 1% (Langley).

The First and Fourth Amendments protect Americans' right to free speech, practice, and privacy. Without a warrant, personal information is theoretically always safe. Without a warrant, except in specific circumstances, law enforcement personnel are not allowed to enter houses. How is data any different?

Bruce Schneier, a security expert, talks at length about how NSA has overstepped its bounds and shown a clear disregard to people's right to privacy with no intentions of stopping:

> We are long past the point where simple legal interventions can help. The bill in Congress to limit NSA surveillance won't actually do much to limit NSA surveillance. Maybe the NSA will figure out an interpretation of the law that will allow it to do what it wants anyway. Maybe it'll do it another way, using another justification. Maybe the FBI will do it and give it a copy. And when asked, it'll lie about it (Schneier 2014).

Since the revelations last year from Snowden, the NSA has shown no backing off, making it clear that they have no intentions of stopping this unethical and possibly unconstitutional behavior.

The main justification for this breach of trust is to stop terrorism. Terrorism is a huge concern in Americans' minds, especially since the events of 9/11. However, in 2011 only seventeen "US citizens worldwide [were] killed as a result of incidents of terrorism" (US State Department). In fact, it is more likely that people will be killed by a toddler or lightning than by a terrorist, not to mention the probability of being killed by a drunk driver. Terrorism is no longer the threat, it's simply the cover story.

Unfortunately, many people hold onto the false notion that they have nothing to hide and therefore don't need security. Everyone has something to hide because everyone makes mistakes.

Crimes can always be found and proven, all someone needs to do is look hard enough. But the main concern is the lack of government transparency. The people do not know how the information that the NSA and others are collecting is being used. They don't even know if the information is being used for or against them. More transparency would go a long way towards solving this problem, but there still exists the overreach of the government into people's personal lives. Another common argument is that anything collected by the NSA is inadmissible in court. This matters less when the NSA and others are using recognized, secret courts and executing their own citizens in drone strikes (ACLU).

Referring to the NSA's lack of stopping terrorism, Schneier said:

> We have no evidence that any of this surveillance makes us safer. NSA Director General Keith Alexander responded to these stories in June by claiming that he disrupted 54 terrorist plots. In October, he revised that number downward to 13, and then to "one or two." At this point, the only "plot" prevented was that of a San Diego man sending $8,500 to support a Somali militant group. We have been repeatedly told that these surveillance programs would have been able to stop 9/11, yet the NSA didn't detect the Boston bombings — even though one of the two terrorists was on the watch list and the other had a sloppy social media trail (Schneier).

Schneier thus concludes that "[b]ulk collection of data and metadata is an ineffective counterterrorism tool."

The NSA has gone to an extreme extent to stop terrorism, an extent wildly out of their hands, and have proven fruitless in their labors. They do not possess the ability to stop another

9/11 from happening, nor did they possess the ability to stop the Boston marathon bombings. Their surveillance programs, widely regarded as unconstitutional (and under legal fire from the EFF, ACLU, and others), have not been able to stop terrorist plots against the United States and need to be stopped.

Works Cited

"ACLU & CCR Lawsuit: American Boy Killed By U.S. Drone Strike." *ACLU*. N.p., n.d. Web. 20 Feb. 2014.

Benkler, Yochai. "In secret, Fisa court contradicted US supreme court on constitutional rights." The Guardian. The Guardian, 22 Sep 2013. Web. 18 Feb 2014.

Boyd, Danah. "Apophenia." *Danah Boyd Apophenia RSS*. N.p., 10 June 2013. Web. 05 Mar. 2014.

Greenwald, Glenn, and Ewen MacAskill. "NSA Prism program taps in to user data of Apple, Google and others". The Guardian, 06 Jun 2013. Web. 25 Feb 2014.

Langley, Adam. "ImperialViolet." *Atom*. N.p., 25 June 2010. Web. 05 Mar. 2014.

Prism slide 5w. 2013. Graphic. Wikimedia. Web. 18 Feb 2014.

Schneier, Bruce. "How the NSA Threatens National Security." Schneier on Security. N.p., 13 Jan 2014. Web. 18 Feb 2014.

Ibid. "How the FISA Court Undermines Trust". Schneier on Security. N.p., 23 Jul 2013. Web. 25 Feb 2014.

Solove, Daniel J. "The Chronicle Review." *The Chronicle of Higher Education*. N.p., 15 May 2011. Web. 05 Mar. 2014.

"Terrorism Deaths, Injuries, Kidnappings of Private U.S. Citizens, 2011." US Department of State, Diplomacy in Action. Office of the Coordinator for Counterterrorism, 31 Jul 2012. Web. 18 Feb 2014.

Upstream slide of the PRISM presentation. 2013. Graphic. Wikimedia. Web. 18 Feb 2014.