Colby Goettel

Reed

English 312

19 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).

Expand: Talk about NSA building at Point of the Mountain, GPUs, password cracking, potential of SHA1 having been hacked. Programs being used by other branches of government including local law enforcement.

Expand: All data should be encrypted. HTTPS everywhere. The computational power is no longer a problem.

Expand: The First and Fourth Amendments protect Americans' right to privacy. Without a warrant, personal information should always be safe. Without a warrant, except in very certain circumstances, law enforcement personnel are not allowed to enter houses. How is data any different?

Bruce Schneier, a security guru, talking about how to solve this problem said, "Fixing this problem is going to be hard. 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).

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" (State Department 2012). Terrorism is no longer a large threat. In fact, it is more likely that you will be killed by a toddler or lightning than by a terrorist, not to mention the probability of being killed by a drunk driver. We are fighting the wrong battle.

The line of thinking that "I have nothing to hide" is wrong. Numerous arguments against (to be summarized): -http://chronicle.com/article/Why-Privacy-Matters-Even-if/127461/

-http://www.zephoria.org/thoughts/archives/2013/06/10/nothing-to-hide.html

-https://papers.ssrn.com/sol3/papers.cfm?abstract_id=998565

-http://www.wired.com/opinion/2013/06/why-i-have-nothing-to-hide-is-the-wrong-way-to-think-about-surveillance/

-http://www.wired.com/politics/security/commentary/securitymatters/2006/05/70886

Another argument is that "anything collected by the NSA is inadmissible in court" which doesn't matter much when you're being tried by a secret court or you're dead because of a drone strike. For instance,

https://www.aclu.org/national-security/aclu-ccr-lawsuit-american-boy-killed-us-drone-strike

Ukraine is currently going through a revolution. Last month, thousands of protesters simultaneously received the following text message: "Dear subscriber, you are registered as a participant in a mass disturbance." This is just the tip of the iceberg for what the NSA is capable of doing, and this was done by a foreign power!

Again from Schneier, “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. Bulk collection of data and metadata is an ineffective counterterrorism tool” (Schneier 2014).

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

PRISM slide on companies used

http://upload.wikimedia.org/wikipedia/commons/5/5a/Prism_slide_5w.png PRISM upstream slide

http://upload.wikimedia.org/wikipedia/commons/a/a1/Upstream_slide_of_the_PRISM_presentation.jpg

http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data Glenn Greenwalk and Ewen MacAskill, 6 June 2013 ”NSA Prism program taps in to user data of Apple, Google and others”

https://www.schneier.com/blog/archives/2013/07/how_the_fisa_co.html Bruce Schneier, 23 July 2013, ”How the FISA Court Undermines Trust”

http://www.theguardian.com/commentisfree/2013/sep/22/secret-fisa-court-constitutional-rights Yochai Benkler 22 September 2013 ”In secret, Fisa court contradicted US supreme court on constitutional rights”

https://www.schneier.com/blog/archives/2014/01/how_the_nsa_thr.html Bruce Schneier ”How the NSA Threatens National Security” 13 January 2014

http://www.state.gov/j/ct/rls/crt/2011/195556.htm State Department report 31 July 2012