Constitutional Considerations of the National Security Agency's Domestic Wiretapping

Robert H. Wiltbank, III

Fort Hays State University

Abstract

In their efforts to gather intelligence and proactively assess threats to the United States, the National Security Agency engages in the bulk domestic collection of phone metadata through the use of pen registers. The information is analyzed and correlated to produce associations, profiles of behavior and locations of the individuals involved. These practices have implications against First and Fourth Amendment protections and, if left unmoderated, create a slippery slope down which the further erosion of constitutional protections lies. There is support for both sides of the data collection program in Congress and legislation has been proposed that will essentially codify the NSA's policy of gathering domestic information without proper legal documentation. However, United States Code requires the application for a court order to install the pen register must include a statement indicating that the pen register will likely yield information to aid in an ongoing criminal investigation, indicating that the practice is outside of the bounds of US Law and unconstitutional.

Table of Contents

Constitutional Considerations of the National Security Agency's Domestic Wiretapping

The Issue

The National Security Agency, estimated to be one of the largest intelligence agencies in the United States (Gellman & Miller, 2013) and operating under the jurisdiction of the Department of Defense, has been conducting domestic electronic surveillance since 2010 to "discover and track connections between intelligence targets and people in the United States" (Risen & Poitras, 2013).

According to Stray (2013), based off of the documents leaked by Edward Snowden, the NSA collects information on most telephone calls in the United States, emails, Facebook status updates, instant messages and massive amounts of raw network traffic from the Internet. Utilizing their available resources, analysts are able to piece together the parts of your online time to create a profile for a given user.

To further facilitate the discovery and association process, the NSA uses its information to develop complex graphs of the social connections between some Americans, allowing them to identify people with whom they commonly associate, the location of an individual at various times throughout the day and various other personal information (Risen & Poitras, 2013).

Context

On their website, nsa.gov, the National Security Agency explains that the information is collected and analyzed to pro-actively assess threats to the United States; furthermore, they

claim their operations and intelligence gathering efforts are essential to the continued security of our nation. Driving this point home, NSA chief General Keith Alexander spoke at a security conference in July of 2013 and indicated that, with the information collected by the NSA, "54 different terrorist-related activities" were thwarted (Black Hat, 2013). 25 in Europe, 13 in the United States, 11 in Asia and 5 in Africa; however, the NSA is unable to provide evidence supporting these claims.

Significance

The citizens of the United States are guaranteed to be free from unreasonable search and seizures and, in addition, no warrants shall be issued unless there is probable cause and a description of the location to be searched and items to be seized (U.S. Const. amend IV). The people are further guaranteed free exercise of speech without abridgement (U.S. Const. amend I).

While there are many different data collection behaviors in which the National Security Agency is engaging, each with their own case history to guide the precedence, the issue is distilled down to the NSA collecting mass amounts of information (seizure) for which some people have a reasonable expectation of privacy, and the analysis and the correlation of that data (search). In addition, now that the American people are aware that their every communication has the possibility of being recorded, their First Amendment right is tangentially infringed upon as they are now self-censoring to prevent the government from collecting even more information.

Left unfettered, the information collection practices of the NSA can have a chilling effect on speech in the United States. The American Civil Liberties Union has filed a lawsuit against the NSA on behalf of whistleblowers stating, "any person hoping to approach plaintiffs with proof [of government wrongdoing] would be understandably wary knowing that the government receives, almost in real-time, a record of every telephone call," further explaining that even the mere fact that phone calls took place could be "particularly sensitive or confidential" (McVeigh, 2013).

There has been some support in Congress for curbing the NSA's domestic activities. In a letter written by Senator Darrell Issa, the Republican stated, "Now that it has been publicly acknowledge that the communications of Americans were included in the NSA's data collection program, likely violating their Fourth Amendment rights, Congress must responds in a manner that both increases the transparency of the Agency's programs and reinforces the constitutional protections of our citizens" (Issa, 2013).

Since legislators are made to take an oath to defend and protect the Constitution of the United States upon taking office, the questionability of constitutional violations – made apparent by several outstanding political figures and civil liberty groups -- demands that it bear greater scrutiny by policymakers to ensure their primary responsibility.

In the event nothing is done to moderate the data collection program, the NSA would view this as a tacit approval of their efforts and would continue under the premise of supporting the United States' intelligence operations and infrastructure; however, the rights of

the country's citizens would certainly suffer and further the abridgement of other constitutionally protected freedoms.

Current Status

In a recent attempt to protect their anonymity, people have begun using services that are specifically designed to obscure the identity of its users. Tor, a free software service based on 2nd generation onion routing to allow anonymous communication, is primarily funded and promoted by the government of the United States (Ball, et al., 2013). However, in an article by James Ball et al. in The Guardian, the National Security Agency "has made repeated attempts to develop attacks against people using Tor" (2013). Though seemingly self-defeatist, this is done by deploying attacks against vulnerable software on a users' computer, similar to how a typical hacker operates.

Recent reports have also surfaced indicating that the NSA "tracked or considered tracking the cellphone location data of millions" of citizens in the United States (Sasso, 2013). Although a small group of lawmakers has proposed legislation to stop the collection of metadata, it appears as though Congress generally supports the efforts of the NSA, as Senate Intelligence Committee chair Dianne Feinstein introduced a bill that would "change, but preserve" the data collection program (Fung, 2013).

In an editorial in the Mercury News, a call was put out for the Silicone Valley private sector to push back to help protect privacy rights, saying that, "The NSA must not be allowed to

go on fishing expeditions through Internet users' information without showing cause" (2013). This call was heard by Google who began encrypting its traffic between data centers which, in effect, has halted the intelligence gathering operations of the NSA from Google sources – a move which Yahoo will be following by the first quarter of 2014 (Panzarino, 2013).

Question

Is the NSA's practice of collecting domestic electronic data and telecommunication information constitutional?

It is unknown what information the NSA collectively gathers. Though, in a very recent article, what is believed to be the original court document authorizing the data collection practices included three pages of redacted categories and indicated a secret email surveillance program authorized following the September 11th attacks on the United States (Nakashima & Miller, 2013).

Of primary concern is the collection of telephone metadata which allows the National Security Agency to record the phone number of callers and recipients, the duration of the call and the approximate location of the participants. Information collected in this manner is covered by pen registers, codified in 18 USC Chapter 206. 18 USC §3121(a) states that, "…no person may install or use a pen register or a trap and trace device without first obtaining a court order." Furthermore, while section (c) provides that, "A government agency authorized to install and use a pen register … shall use technology reasonably available to it that … does

not include the contents of any wire or electronic communications." Most importantly, §3122(b)(2) states that, in order to obtain the court order, the application must include a certification by the applicant stating that the "information likely to be obtained is relevant to an ongoing criminal investigation," which indicates that the NSA would need to obtain a court order for each pen register and show cause.

Based on the available information and the relevant legislation, it would appear to the layperson as unconstitutional. However, between executive orders, redacted court documents and the general secrecy under which the intelligence agency operates, the citizens of the United States, in addition to its elected officials, will never have a clear understanding of the agency's goings-on.

Position

In Katz v. U.S. (1967), the Supreme Court established that communications are protected from unreasonable search and seizure if the individual involved had a reasonable expectation of privacy; however, Smith v. Maryland (1979) clarified that the use of a pen register did not constitute a search because the person dialing "voluntarily" gave the number to have it connected. This decision does not consider the fact that the recipient of the call should still retain his or her reasonable expectation of privacy since they did not "convey numerical information." Furthermore, while the subscribers and customers of a service owned by a private entity may expect the telephone company to track calls made for the purposes of billing, it is not reasonable to expect the carrier to act as agents of the government by providing

information without proper documentation; however, the Smith decision effectively puts pen registers outside of constitutional protections.

Conclusion

As a liberty-loving citizen of The United States of America, the gut reaction is to halt the practice of unauthorized wiretapping and data collection. Just as a citizen has a right to walk down the road and be free from arrest without probably cause or detention absent reasonable articulable suspicion, one should similarly be able to navigate the Internet without fear of having one's information collected and analyzed unless authorized by a court after having been provided details sufficient to support the order.

Legislators must understand the constitutional implications of these devices and craft privacy policy to specifically guide the use of pen registers so that they are only utilized in instances where they will likely lead to information in an ongoing criminal investigation as opposed to using them for bulk collection of data.

However, the calls have been put out and legislators often believe that, if something is done in the name of safety, it must be right and it must be implemented. "If it saves just one life, it's worth it." Herein lays the debate that immediately ensues: how much freedom is one American citizen willing to give up in order to potentially save another life? Thankfully, we don't need to make that decision; the founding fathers crafted the guidelines upon which these

legal decisions were to be made. Trying to craft policy around the Constitution -- or avoiding it altogether -- goes against the very fibers with which our country was sewn together.

If one believes that a policy should be enacted and that policy doesn't fit within the bounds of the Constitution, there is a process to amend it.

References

Ball, J, et al. (2013, October 4). *NSA and GCHQ Target Tor Network that Protects Anonymity of Web Users*. The Guardian. Retrieved November 5th, 2013 from http://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption

Black Hat. (2013, July 31). *Black Hat USA 2013 Gen. Alexander Keynote* [Video file]. YouTube. Retrieved November 5th, 2013 from https://www.youtube.com/watch?v=xvVIZ4OyGnQ

Fung, B. (2013, September 26). *Sen. Feinstein Unveils Her Own Bill to Reform the NSA's Spying Practices*. Washington Post. Retrieved November 5th, 2013 from http://www.washingtonpost.com/blogs/the-switch/wp/2013/09/26/sen-feinstein-unveils-her-own-bill-to-reform-the-nsas-spying-practices/

Gellman, B. & Miller, G. August 29, 2013. *U.S. spy network's successes, failures and objectives detailed in 'black budget' summary*. The Washington Post. p. 3. Retrieved August 29, 2013 from http://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_story.html

Issa, D. (2013, September 10). Letter to Eric Cantor [Image]. Retrieved November 19th, 2013 from http://images.politico.com/global/2013/09/10/issa-cantor-nsa-amash.html

Katz v. United States 389 U.S. 347. (1967). Retrieved from LexisNexis Academic Database.

McVeigh, K. (2013, August 27). *NSA Surveillance Program Violates the Constitution, ACLU Says*. The Guardian. Retrieved November 5th 2013 from http://www.theguardian.com/world/2013/aug/27/nsa-surveillance-program-illegal-aclu-lawsuit

Nakashima, E. & Miller, G. (2013, November 18th). *Official Releasing What Appears to be Original Court File Authorizing NSA to Conduct Sweeps*. The Washington Post. Retrieved November 19th, 2013 from http://www.washingtonpost.com/world/national-security/official-releases-what-appears-to-be-original-court-file-authorizing-nsa-to-conduct-sweeps/2013/11/18/194522b6-50a7-11e3-9e2c-e1d01116fd98_story.html

Panzarino, M. (2013, November 18th). *Yahoo Will Follow Google In Encrypting Data Center Traffic, Customer Data Flow By Q1'14*. Tech Crunch. Retrieved November 19th, 2013 from http://techcrunch.com/2013/11/18/yahoo-will-follow-google-in-encrypting-data-center-traffic-all-traffic-between-company-and-customers-by-q1-14/

Crimes and Criminal Procedure, 18 USC §3121.

Risen, J. & Poitras, L. September 28, 2013. *N.S.A. Gathers Data on Social Connections of U.S. Citizens*. The New York Times. Retrieved November 5th, 2013 from http://www.nytimes.com/2013/09/29/us/nsa-examines-social-networks-of-us-citizens.html

Sasso, B. (2013, September 26). *Dem Senator Hints That NSA Tracked Locations for Millions of Cellphones*. The Hill. Retrieved November 5th, 2013 from http://thehill.com/blogs/hillicon-valley/technology/324967-senator-hints-nsa-tracked-locations-of-millions-of-cellphones

Smith v. Maryland 442 U.S. 735. (1979). Retrieved from LexisNexis Academic Database.

Silicone Valley Must Push Back on NSA to Protect Privacy Rights [Editorial]. (2013, October 5th). San Jose Mercury News.

Stray, J. August 5, 2013. *FAQ: What You Need to Know About the NSA's Surveillance Programs*. ProPublica. Retrieved November 19th, 2013 from http://www.propublica.org/article/nsa-data-collection-faq

U.S. Const. amend. I.

U.S. Const. amend. IV.