Domestic Surveillance and Government's Loss of Legitimacy

Chris Inks

Angelo State University

Abstract

The terrorist attacks against the United States on the morning of September 11, 2001 created an environment ripe for the abuse of power. With a fearful nation clamoring for greater protection against future attacks, the National Security Administration (NSA) took the opportunity to create and implement a secret domestic spying and data mining program, the size of which had never before been imagined. Because information is the ultimate form of power in today's world, unmitigated access to so much personal data has the potential to aggregate power into this one agency, leaving the rest of government and the populace unable to defend themselves against those who would use it to advance their own agendas. Once obtained, there is no way to check this power. Since government is only as legitimate as the populace believes it to be, such aggregations of power are likely to increase dissent among the citizenry and ultimately result in a belief that it has become illegitimate. Such a government is ineffective and puts the entirety of the populace in harm's way, not only from terrorists outside its borders, but from potential domestic abuses of this power. In the rush to protect the country against terrorism, one must be careful the actions he or she takes do not inadvertently create a homeland security threat from within.

The rapid rise in technology and subsequent connectivity throughout the world over the course of the past 20 years has given rise to a bigger, stronger, and more intrusive National Security Administration (NSA). While the agency defends its domestic surveillance on the basis that it is securing the nation against foreign enemies, its actions as of late unfortunately also give rise to the potential for domestic ones. As a matter of fact, the very idea that the less private an individual is allowed to keep his or her life the more secure a nation is, remains antithetical to the very notion of freedom the NSA argues it is securing. Justice Powell (United States, 1972), writing for the majority in a Supreme Court decision mandating that warrants are required for domestic intelligence surveillance, reminded the nation that "The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power. Nor must the fear of unauthorized official eavesdropping deter vigorous citizen dissent and discussion of Government action in private conversation. For private dissent, no less than open public discourse, is essential to our free society."

The well-understood fear of domestic enemies is so great that such protection against it is enshrined within the United States armed forces Oath of Enlistment which specifically holds that the individual enlisting in the U.S. military "will support and defend the Constitution of the United States against all enemies, foreign and domestic" (Government Printing Office, 2010). What constitutes a domestic enemy need not be argued or even defined at this point. All that is required is the realization that access to the daily habits, beliefs, concerns, and actions of the individuals that make up a specific populace places those people and, by extension, the nation whose borders they reside within, in harm's way. Unfortunately, many people do not understand how an agency, such as the NSA, having access to real-time data about the most intimate areas of their lives can result in its supporting of domestic enemies. To make sense of this, one need

only look at the recent explosion of companies attempting to data mine the information they have collected about the individuals that use their services.

Companies like Facebook and Google, through the utilization of their massive analytical resources, have access to the viewing, shopping, and connectivity/interaction habits of billions of people worldwide. They use this information to deliver more relevant advertising and help individuals discover people and information on the Internet that they may not ever discover on their own. At the same time, these companies are able to increase their revenue by selling access to the information in the form of product placement. While, on the surface, many people may welcome such tailored and potentially relevant advertising, at what cost is this being pursued? As a recent Op/Ed in Forbes, penned by the Chairman of the Board of Accion along with the company's President and CEO, points out, big data has the "capacity to better understand individual behavior" (Taylor & Schlein, 2014). Although this understanding is value-neutral, there is great potential for such understanding and information to be used negatively in order to further the political agendas and personal beliefs of those in the upper echelons of government or those who lobby such individuals.

The U.S. was founded on the belief that people should be allowed to think and say what they feel without fear of repercussion from their government. Because such a government is composed of many different people, all with differing thoughts and views about the world around them, it is imperative that the populace not be afraid to think or feel differently than that government. Unfortunately, this is easier said than done, as society often ostracizes those who do not believe as the consensus does. Therefore, many people tend to keep their nonconforming thoughts and beliefs undercover and only share them with other like-minded individuals. To these people, privacy is not just a convenience but it is practically a necessity. What happens

when these individuals' shopping habits, thoughts and beliefs, and participation in groups online and in real life are stored in giant databases? These people become nothing more than a snapshot in time.

The problem with being identified as only a snapshot in time is that individuals change as they are exposed to differing beliefs, opinions, cultures, increased education, and life experiences. As such, they may not be the same person five years from now that they once were. The way data mining works, however, is that a question is asked or a hypothesis is formed first, then the data is combed for patterns that answer the question or support the hypothesis. The patterns found may not be indicative of wrong-doing, just non-conformity. At this point, the individual is perceived as a threat and becomes a target of government agencies. For all intents and purposes, he or she is seen as guilty until the individual is proven innocent. The harm as a result of this is three-fold: 1) the individual is treated as a criminal though he or she is not one, 2) the agency wastes time and resources tracking this individual and building a case on false beliefs about him or her, and 3) the government loses legitimacy as it attempts to prosecute innocent individuals because they do not conform with mainstream society. If this were the only harm suffered as a result of the NSA's domestic surveillance program it would be enough, but there is more to worry about.

Another very real fear results from the fact that so much information is held in databases making any individual available for scrutiny at any point in time. The NSA is not immune to hackers as any information connected to the Internet is only a few keystrokes away from being accessed by someone else down the street or on the other side of the planet. The only Internet security that is 100% effective is unplugging the computer from the Internet. However, this does not disconnect the Internet from the information the individual has already placed there. As such,

not only do the American people have to worry about their information being misused by those who have legal access to their information (Alexander, 2013) but also by those who illegally access the information. This leaves the American people vulnerable to identity theft, harassment, and, even worse, persecution by those in government who do not share the individual's thoughts and beliefs. This latter assertion is significant because without dissenting thought real truth can never be known and government can be set in a specific direction without worry that its actions will be challenged by the populace. Such unrestrained information access leads to political power that is dangerous to the citizenry and the inherent U.S. ideals of what constitutes freedom. To understand just how likely such an abuse of power is, take a look at the past four decades.

Prior to the technological advances and widespread adoption of connectivity devices today, the Church Committee in 1975 had uncovered illegal domestic spying on anti-war protestors, civil rights activists, and political opponents by the NSA and other intelligence agencies. As a result, Senator Church pointed out "[The] capability at any time could be turned around on the American people, and no American would have any privacy left, such is the capability to monitor everything: telephone conversations, telegrams, it doesn't matter. There would be no place to hide" (Bamford, 2005). During the 1980s the Federal Bureau of Investigation (FBI) spied on domestic pacifists and religious groups who opposed American foreign policy in Central America (Gelbspan, 1991) and, again, in the 1990s when the agency "placed antiglobalization protests under its terrorist rubric even though no acts of violence were linked to the movement apart from select petty street vandalism" (Greenberg, 2011). In 2002, the NSA's data mining project, Total Information Awareness (TIA), was constructed to "assemble a massive database consisting of financial, educational, health, and other information on U.S. citizens, which would later be analyzed to single out people matching a terrorist profile" as

described by Admiral John Poindexter (Solove, 2008, p. 343). However, a significant problem with surveillance such as this is that "suspicious behavior is often unusual behavior" and these judgments "are necessarily hunches about abnormality, regularity, and conformity" (Jon, 2013). An action is not criminal in nature just because it does not conform. While TIA was ultimately never funded due to public backlash, the idea was implemented in various other projects and, according to a government report, as of 2004 there were already 200 different government data mining projects being used or developed (Solove, 2008, p. 344).

Unfortunately, laws and oversight do not keep people from committing crimes and this holds true for those in government as well. "From 2006 to 2009, the NSA was found by its judicial regulators in the Foreign Intelligence Surveillance Court (FISC) to be illegally surveilling thousands of phone numbers both inside and outside the United States without reasonable suspicion" (Greenberg, 2013). An internal NSA audit from 2012 noted that the agency violated the "rules or court orders for surveillance of Americans or foreign targets in the United States" 2,776 different times from April 2011 through March 2012 (Gellman, 2013). One NSA surveillance program collected 56,000 emails and other communications of Americans without terrorism connections annually over the course of three years (Aljazeera America, 2013). In addition, the NSA has made information, including email addresses and telephone numbers, available to the Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI), and National Counterterrorism Center (NCTC) in violation of a court order (Levy, 2013).

In terms of catching potential terrorists, this appears to be exactly what proponents of the NSA's domestic spying program want. However, it leaves the rest of the law-abiding populace vulnerable to abuse. Much like using a drift net results in catching all manner of fish, the outcome of the NSA's blanket spying program is that many innocent people are caught up with

those few who are guilty. White House counselor, John Podesta, noted that a recent 90 day review ordered by President Obama found that "potential for discrimination is an issue that warrants a closer look" (Sullivan, 2014). What does this mean for a political system originally designed to better the lives of the people who live under it? The ease and availability of such abuses of power can inadvertently bring about the rise of a tyrannical movement within the government thereby negatively affecting the very people that government was created to protect.

Because the United States' 218 year old form of government is democratic in that the populace votes for those in power who they entrust to create and pass legislation that is conducive to their own long-term plans and beliefs or, if nothing else, those least opposed to their own position, it is of the utmost importance that people remember at the end of the day even the most principled individuals are still nothing more than fallible human beings prone to making self-serving and/or bad decisions. At best, such decisions can result from personal financial or medical issues, strong positive or negative beliefs about specific groups of people, religious beliefs, or even the lust for fame, fortune, and/or power, and do not necessarily have positive results for their constituents. At worst, these decisions can result from an individual's blatant disregard for Constitutional limitations on his or her power, as witnessed by President George W. Bush's "secret authorization of domestic electronic surveillance by the National Security Agency (NSA) without judicial warrants" (Twight, 2008, p. 496) or the extraordinary rendition program (Natalie, 2012). Individuals do not gain morality or ethics as a result of being elected into office and that is precisely why the U.S. system of government was designed as it was, so that aggregation of power into a single area would be avoided to the greatest degree possible.

It must always be remembered that a government's legitimization is a double-edged sword that is achieved only through the populace's belief that the government is, in fact, legitimate. As such, a government does not remain legitimate because it exists; rather, it continues to exist only because it is perceived as legitimate or establishes itself as a tyranny. In a political system such as that instituted in the U.S., any point at which the populace believes the government is not working as they think it should leads to a growing perception of illegitimacy (Jaycox, 2014). This necessarily results in increased dissidence throughout the country and explains the current criticism and hostility being levied by the U.S. populace against the NSA's domestic spying program. However, such discontent by the people does not mean that elected officials will necessarily listen. In March 2014, the secret Foreign Intelligence Surveillance Court refused a request by the Obama administration to allow classified NSA telephone surveillance data to be stored beyond the current limit of five years (Mears, 2014). While Judge Walton may have decided in favor of personal liberty that day, there is no guarantee that future attempts to subvert privacy will be denied or that his decision will not be overturned by a higher court upon appeal. What is important to note is that the attempt was even made in the first place in the midst of such popular backlash against it.

Power is an aphrodisiac that corrupts those who would most-readily abuse it, all-pervasive gathering of information being the ultimate form of power in the technologically-advanced and interconnected world of today. As technology continues to evolve and global connectivity becomes increasingly widespread, information becomes more readily available and the ability to abuse it increases, especially by agencies such as the NSA. Power also tends to be corrupting to those who would normally not act in such a manner, as proven by the Stanford Prison Experiment (Haney, Banks, & Zimbardo, 1973). Allowing the NSA to continue operating

as it has been will only succeed in an aggregation of power into this one agency which will cause dissent among the populace. This will result in the loss of legitimacy for the government. Once a government is seen as illegitimate by its own citizenry, it can no longer count on the populace following its policies and legislation thus forcing the government to turn its power against the citizenry in an attempt to maintain its very existence. All those who disagree with the government policies and legislation will be perceived as threats to the status quo - i.e. home grown terrorists. Therefore, it is in the best interest of the government to reign in the excessive domestic surveillance of the American populace or it will face a homeland security threat from within far greater than that posed by any externality.

References

Alexander, H. (2013). *NSA employees spied on their lovers using eavesdropping programme*. The Telegraph. Retrieved from http://www.telegraph.co.uk/news/worldnews/northamerica/usa/10263880/NSA-employees-spied-on-their-lovers-using-eavesdropping-programme.html

Aljazeera America. (2013). *NSA illegally collected thousands of US emails annually*. Retrieved from http://america.aljazeera.com/articles/2013/8/21/nsa-collected-tensofthousandsofuscommunications.html

Bamford, J. (2005). *The agency that could be Big Brother*. The New York Times. Retrieved from http://www.nytimes.com/2005/12/25/weekinreview/25bamford.html?pagewanted=all

Gelbspan, R. (1991*). Break-ins, death threats, and the FBI: The covert war against the Central America movement.* Boston: South End Press.

Gellman, B. (2013). *NSA broke privacy rules thousands of times per year, audit finds*. The Washington Post. Retrieved from http://www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_story.html

Greenberg, A. (2013). *NSA secretly admitted illegally tracking thousands of "alert list" phone numbers for years*. Forbes. Retrieved from http://www.forbes.com/sites/andygreenberg/2013/09/10/nsa-secretly-admitted-illegally-tracking-thousands-of-alert-list-phone-numbers-for-years/

Greenberg, I. (2011). The FBI and the making of the terrorist threat. *Radical History Review*, (111), 35-50. doi:10.1215/01636545-1268686

Government Printing Office. (2010). *§502. Enlistment oath: Who may administer*. Retrieved from http://www.gpo.gov/fdsys/pkg/USCODE-2010-title10/html/USCODE-2010-title10-subtitleA-partII-chap31-sec502.htm

Haney, C., Banks, C., & Zimbardo, P. (1973). Interpersonal dynamics in a simulated prison. *International Journal of Criminology and Penology*, *1*, 69-97.

Jaycox, M. (2014). *Update: Polls continue to show majority of Americans against NSA spying*. Electronic Frontier Foundation. Retrieved from https://www.eff.org/deeplinks/2013/10/polls-continue-show-majority-americans-against-nsa-spying

Joh, E. E. (2013). Privacy protests: Surveillance evasion and fourth amendment suspicion. *Arizona Law Review, 55*(4), 997-1029.

Levy, P. (2013). *NSA FISA surveillance: NSA shared Americans' info from phone data program with CIA, FBI*. International Business Times. Retrieved from http://www.ibtimes.com/nsa-fisa-surveillance-nsa-shared-americans-info-phone-data-program-cia-fbi-1404303

Mears, B. (2014). *Government can't hold NSA surveillance data longer*. CNN. Retrieved from http://www.cnn.com/2014/03/07/politics/nsa-surveillance-extend/

Natalie, D. (2012). No long secret: Overcoming the State Secrets Doctrine to explore meaningful remedies for victims of extraordinary rendition. *Case Western Reserve Law Review, 62*(4), 1237-1283.

Solove, D. J. (2008). Data Mining and the Security-Liberty Debate. *University Of Chicago Law Review, 75*(1), 343-362.

Sullivan, E. (2014). *Discrimination potential seen in "Big Data" use.* ABC News. Retrieved from http://abcnews.go.com/Technology/wireStory/white-house-discrimination-potential-data-23481770

Taylor, D., & Schlein, M. (2014). How big data can expand financial opportunities for the world's poor. Forbes. Retrieved from http://www.forbes.com/sites/realspin/2014/04/25/

how-big-data-can-expand-financial-opportunities-for-the-worlds-poor/

Twight, C. (2008). Sovereign Impunity. *Independent Review, 12*(4), 485-517.

United States v. United States District Court 407 U.S. 297. (1972). Retrieved from LexisNexis Academic Database.