ASA

Annie Searle & Associates LLC

Research Note

The Big Bad NSA: A Risk Based Analysis of Domestic Spying Practices

Jared Williams

April 2016

Keywords: National Security; Domestic Surveillance; Spying; Government Surveillance; National Security Agency.

Abstract: This paper discusses the major risks around government domestic surveillance programs, particularly the U.S. National Security Agency (NSA). While domestic surveillance is not a new practice by governments, technological innovations have changed the game. The paper discusses the issues, both from the perspective of the risks to governments and the risks to citizens under domestic surveillance.

Part I: The State of Things and Significance

Though we often imagine domestic spying to be a new concept, governments have been keeping tabs on their people forever. In the time of Caesar, politicians had spies to keep note of rivals, and indeed Caesar himself had a network to watch for possible threats in the domestic realm.[1] As a more recent example, many of us know of the Watergate scandal, in which the Nixon administration was found to have bugged, watched and kept record of the private conversations and actions of rivals and those they found suspicious.[2] This trend of governmental leaders spying on their people has only worsened with time and the advancement of technology. With each advancement in communication technology, it becomes easier for governments to watch larger numbers of the populace, more often and with greater efficacy. With smart phones, social networks, cameras and national paranoia a government may watch every step you take. Knowing this, we can analyze the major risks and failures in domestic spying, in order to develop a strategy to treat and terminate the problems they create. By dissecting the National Security Agency (NSA) and other current governmental spying actions both within and outside the U.S., I hope to highlight the risks and errors of domestic surveillance. These issues will be examined on both the side of risk to the governments in question and the risk to citizens within and affected by these nations.

We know that a government spying on its citizens is not a new concept, nor is it exclusively an

American issue. From Caesar in ancient Rome, to the Catholic Church through the fourteenth century,[3] to the United Kingdom's Government Communications Headquarters (GCHQ) today, domestic surveillance has been a standing practice for centuries. In its earlier forms, this spying was meant to either give political candidates and leaders the upper hand over their competition, or to protect them against plots against their wellbeing. In the U.S., domestic spying has been used as far back as 1861 when Pinkerton's National Detective Agency unearthed a plot against the life of Abraham Lincoln, which was then prevented.[4] By 1919, the U.S. had its first federal intelligence agency that worked during peacetime, known as the Cipher Bureau. Before this, federally sanctioned spying was a matter of war. Though those in power may have had their own spy networks (generally focused internally, on rivals), until 1919 there had never been an American peacetime spy agency. At this time the surveillance focus was on political action in other countries.[5] Not until the 1960's did domestic surveillance become a commonality. From the early 60's to today, the UK government has been building a Closed Circuit Television Network (CCTV) that watches the actions of those within cities – primarily London - to ensure safety.[6] The government-owned CCTV system in the UK marks the first large scale domestic surveillance system, and it has been questioned and criticized by privacy advocates since its inception. But why does it matter?

From the standpoint of a government, domestic spying has great significance. Through watching people within their borders, a government can theoretically profile dangerous inhabitants and stockpile information on actions, conversations, and other communications between people. This information may help identify trends or outliers in actions that can help lead a government to preventing crises. The NSA has been known to do this with conversations and specific key words, watching the use of words over time and deducing potential threats based on this data.[7] Meanwhile European CCTV systems allow for real-time tracking of crimes - seeing everything at once means the government can know what is going on in any given moment. Ultimately, from a government's perspective, domestic spying provides a feeling of greater security.

At the same time, however, this gathered information comes with great risk. Most openly, there is huge reputational risk for the government and the agency in charge of surveillance. For them the risk is two sided; in the event that a crisis occurs, a government will be asked "why did you let this happen" and they fear losing the confidence of the people in their ability to provide security. At the same time, while a government agency works to give this security, they may take too many liberties. In this case they again see reputational risk, if the people learn of the overstepping organization they are likely to lose trust in the governments ability to provide an acceptably free environment. With the great reputational risk a government also takes on significant internal risk. The risk internally manifests in two main forms, people and process. People are a risk to the government because people are unpredictable, and within spying agencies the people are also highly skilled. All too often we ignore the human element within agencies as a risk,[8] but in cases such as these where the people are highly skilled and poorly regulated they have a large chance to create crisis. This means that when a person dislikes what the organization is doing, or decides to

act maliciously, they have the skills to steal information or out the organization, as we saw with Edward Snowden. The processes are a risk to the government on a number of levels. Firstly the vast majority of spying occurs on the internet where there are dangerous actors that would like nothing more than to break into the agencies systems and tear everything down, or worse yet, steal information. This is the second danger, an agency that keeps watch of so many people has an immense amount of data, and this data is a huge target for both other nations, and individual hackers. In fact, the NSA created a map[i] that showed, over a five year period, over six hundred successful attacks on corporate, private and government systems.[9] A further risk in process, is the vetting process for agents within government surveillance organizations. It is extremely hard to ensure your employees are reliable and trust worthy, an agency must know everything about a person and measure risk on many scales. However, we saw within the American government, after Snowden, that vetting processes are far from water tight and tended to favor time and odds over data, leading the government to sue the external organization responsible for background checking their candidates.[10] As for the significance to persons within such governments, the risks and benefits are quite similar. In terms of benefit, the obvious gain is security, as this is what the government is working to provide. However, through these security gains the citizens are losing privacy, and without the work of an inside man such as Snowden, may never know to what extent there security is lost. Further, when unacceptable are found out, the citizens are likely to feel less secure, and thus distrust their government. However, this distrust of government is not the only issue with exposure of government surveillance. In order to get a better idea of the fallout of exposure, let us compare the NSA debacle with the state of CCTV.

When Snowden released information on the NSA and its practices public opinion changed quickly, and international conversation began to focus on privacy. It became clear that the government had taken on massive surveillance projects, and was overstepping the bounds of what was acceptable, through examining phone metadata, internet usage and many other private data. Knowing this, the NSA took a large hit in reputation and the government was forced to respond. At the same time, this opened up a global conversation and inspection of surveillance in many other nations. Recently, it has been in the news that Australia's surveillance has begun to overstep bounds in metadata collection.[11] This story comes based on statements and data from Snowden, and has created a conversation about Australia across the western world. Clearly, the effect of the NSA exposure was not a confined matter, and has spread across nations. I believe this effect is only seen due to the fact that the NSA chose secrecy in their invasion of privacy. At the same time, CCTV has been gradually increasing its coverage and people have been raising questions about invasion of privacy. However, this has led to a much smaller outcry, and little international coverage. This I believe is due to the fact that the governments using CCTV, has been surprisingly open with the use and rules of the network. This may be that people have been slowly losing their privacy and simply grew accustomed to it, but it is clear that government

[i] This is an NSA file explaining some of their visualization methods and how words are tracked.

transparency on the matter has ensured little fallout.

Part II: Summary, Solutions and Suggestions

Until recently, technology has only allowed for small scale surveillance. A government wishing to spy domestically needed a specific target with a specific danger in mind. That is to say, if Caesar wanted to protect against being murdered, he would have to hire a spy to watch the politicians he feared would overthrow him. Now, with technology like CCTV and smart phones, the game has changed. We now have the ability to spy on a vast group for a wide variety of fears. That is to say, the NSA may collect millions of people's cellphone data and check it all for everything from the word "bomb" to conversation about attacks. But why does this surveillance lead to lost privacy? Where does it break down? Before a nation begins domestic surveillance, there will be a reason, something both the government and the people fear. This fear may be violence, treason, or terrorism. Once a nation fears something, the people will look to the government for security. In response, we have seen that the government will likely give an agency, such as the NSA, an excess of power. I do not believe that, at least in the case of the NSA, this is done in an attempt to harm the people, though the loss of privacy has shown to be a direct byproduct. When an agency like this is handed too much power, and there is a poor oversight and regulation system in there processes, there is bound to be an internal failure. Be it an employee leaking information, like Snowden, or some other failure, when masses of information and poor process are involved something will eventually give. Once this happens, there is a public unrest that leads to governmental distrust and a feeling of security lost. Still, this does not have to be the case.

Disaster in domestic spying need not always follow this model. Recently, in response to the Snowden leaks and the following public response, the U.S. government has acted to reform their system. With a re-examination of the background check process, and punishment of the parties responsible[12] we can hope that new employees responsible for surveillance will be reliable and trustworthy. At the same time, the U.S has chosen to limit the expansion of the NSA, thus ensuring that increased domestic surveillance cannot occur. Not only will this help prevent further failures due to unmanageable amounts of information, but will allow for easier regulation and oversight of the organization. With this, the government has chosen to create greater oversight systems, to ensure that everything occurring within domestic spying agencies is within the confines of the law. Finally, the American government has acted to roll back and remove programs that were unacceptable and unlawful, with policy to make court orders necessary in order to retrieve private metadata.[13] This focus on a warrant based system means that when an agency sees a place where invasion of privacy may have a genuine value, they must first prove that there is valid reasoning. This ensures that all surveillance done is clear and the reputation of the agency is no longer based on secrets that may be lost but rather on a system of checks and balances. These actions have great potential to prevent further loss of privacy and represent steps all governments working toward a sustainable and acceptable domestic surveillance policy should consider. Alongside this, the American people have taken steps to ensure their own security. In general, conversation has erupted nationwide. With people questioning in place

policy and voicing what they desire on the fronts of security and privacy, the government has been given a clear indication of what must be done. This is perhaps one of the most important results of the American domestic surveillance issue. From the massive surprise came a massive voice, and the people were able to force change. This is not the case in Europe, where surveillance has been a slow burn, and in kind the conversation about privacy has been far from loud. All together, the changes made in the U.S. policy, are a significant step in the right direction, but they have not created a foolproof system, and may still allow for continued breakdown.

In order to prevent failure and overstepping of domestic surveillance systems around the world, governments should prevent the over-expansion of spying agencies, introduce significant oversight, limit agency power, remove unlawful programs, and introduce warrant dependent systems. Additionally, they should also act in a number of other ways as well. First and foremost, a government spying agency should build, or in the case of the NSA rebuild, a culture against the use of widespread domestic spying. It should not be the default of the organization to surveil people within their borders. This means an agency should not only prevent mass surveillance whenever possible, but also work to increase the privacy of citizens. Prior to the events of 9/11 the NSA had worked to ensure widespread domestic spying did not occur, in fact, before these events, policy was passed on multiple occasions to prevent domestic spying.[14] With this, when a government finds a true need for domestic spying, the spying should be specific and targeted. Surveillance should not be of a large group or population. In order to spy domestically a government agency should have evidence against a specific person or cell and should act only on these persons. At the same time, the agency should have a specified surveillance plan built for these targets, ensuring that any spying done is efficient and within the confines of both the law and the power of the agency.

Furthermore, agencies should significantly reform vetting processes for new agents. It should never be the case that money or time out prioritizes real data and trustworthiness when placing highly skilled people in charge of the privacy and security of citizens. Agencies should not only carry out background checks with one party, but should indeed receive checks from multiple reliable agencies. These agencies should also have some form of government oversight to ensure the checking process is proper. This change in vetting will ensure that hired agents are reliable and will prevent situations where the failure is with internal employees. With these reforms to vetting, it should also be that contractors are avoided whenever possible. Not only is it much harder for contractors to be vetted, but if a contractor finds a failure somewhere within the agency, it is much harder for them to get this fixed or to whistleblow. Knowing this, there should also be a much more robust whistleblower policy within the government. As was seen in the wake of Snowden, the government saw whistleblowers as "villains who compromised what the government classifies as some of its most secret, crucial and successful initiatives."[15] It was seen that when employees tried to follow the proper channels to prevent unlawful spying, they were shut down. The government should change this culture, and ensure that when a whistleblower surfaces, they are given routes to inform those in power of what they have found. This needs to

be a matter handled outside the surveillance agency, by a government bureau or agency that has reliance or relation with it. This will help ensure that matters are looked at with an unbiased eye and may be handled accordingly. With all of these recommendations taken into account, a government can be far more confident in the fact that its handling of domestic spying will be lawful, watched, safe internally and externally, and when something does go wrong, the proper process will be in place to bring the failure to light.

Understanding the history, reasoning, and process of domestic surveillance is the key to creating a system in which a government can assure security for their citizens while also allowing privacy to remain in society. From the age of Caesar domestic surveillance has existed and evolved with the world and what technology allowed; recently this evolution led to failure in systems and distrust of government in citizens. With agencies given excessive power with little oversight, and spying practices being hidden from citizens, it became a guarantee that the system would eventually fail on some level. This, however, need not remain the case; through examination of major risks, and treatment or termination thereof, national spying agencies can create a sustainable system. Through a culture against invading privacy and a tightening of regulation and process within organizations, crisis within and caused by domestic spying agencies will be removed. That is not to say that the suggestions presented in this paper will ensure a secure and private society forever. Indeed, as this issue continues to develop, and as our system becomes more adequate, new risks will arise that must be met with equal thought. Still, by examining domestic spying through the eyes of risk and on both the side of security and privacy, we will be capable of working toward a more perfect system. The process will take time; however, through determination on both the side of the people and that of the government we can create strong regulation and build a secure, private society.

---

1 Zucher, Anthony. "Roman Empire to the NSA: A World History of Government Spying." BBC News. 1 Nov. 2013. Accessed Dec. 2015 <www.bbc.com>.

2 Woodward, Bob. "FBI Finds Nixon Aides Sabotaged Democrats." The Washington Post. 10 Oct. 1972. Accessed Nov. 2015 <www.washingtonpost.com>.

[3] Zucher.

4 Prince, Sam. "A History of Domestic Espionage in the United States." Heavy.com. 10 June 2013. Accessed Nov. 2015 <www.heavy.com>.

5 "The Evolution of the U.S. Intelligence Community-An Historical Overview." Federation of American Scientists. 23 Feb. 1996. Accessed Dec. 2015 <www.fas.org>.

6 "The History Of CCTV In The UK by Camtrak Ltd." SRMTi. 12 Apr. 2012. Accessed Nov. 2015 <www.srmti.com>.

7 "An Information Visualization Primer and Field Trip." The Next Wave: Vol. 17 No. 2 2008. The National Security Agency. Accessed Nov. 2015 <www.nsa.gov>.

8 Fischhoff, Baruch, and John David Kadvany. Risk a Very Short Introduction. Oxford: OUP Oxford, 2011.

9 Windrem, Robert. "Exclusive: Secret NSA Map Shows China Cyber Attacks on U.S. Targets." NBC News.30 July

2015. Accessed Dec. 2015 <www.nbcnews.com>.

10 Schneider, Joe. "Security Firm Sued by U.S. Over Bad Background Checks." Bloomberg. 24 Jan. 2014. Accessed Dec. 2015 <www.bloomberg.com>.

11 Milman, Oliver. "Edward Snowden Says Australia's New Data Retention Laws Are 'Dangerous'" The Guardian. 8 May 2015. Accessed Dec. 2015 <www.theguardian.com>.

12 Schneider.

13 Strohm, Chris. Talev, Margaret. "Obama Unveiling NSA Changes in Response to Snowden Leaks." *Bloomberg*, 16 Jan. 2014. Accessed Dec. 2015 <www.bloomberg.com>.

14 "Timeline of NSA Domestic Spying." Electronic Frontier Foundation. 30 Nov. 2012. Accesssed Dec. 2015. <www.eff.org>.

15 Peter, Eisler. Page, Susan. "3 NSA Veterans Speak out on Whistle-blower: We Told You so." *USA Today*. 16 June 2013. Accessed Dec. 2015 <www.usatoday.com>.