Laura Donovan

13 December 2017

Surveillance State Blues:

Government Invasion of Digital Privacy in the 21st Century

I. Abstract

This paper will discuss the relationship between human rights abuses and mass surveillance in the digital age. It will describe what surveillance-assisted human rights abuse looks like, in countries such as Russia, Saudi Arabia, and Mexico. Then, it will look at mass surveillance in the United States and look at the tradeoff between national security and individual liberty, and whether or not the path this nation is on may upset the balance between the two that makes for a democratic society. Above all, it will ask: do you know what mass surveillance really entails? And what can you do about it?

II. Introduction

As anyone who has watched a spy movie knows, *surveillance* is the act of watching a person or a place, especially a person believed to be involved with criminal activity or a place where criminals gather. So, too, are people familiar with the concept of traditional surveillance. The concept conjures to mind images of hard-boiled private eyes and CCTV cameras and walls with ears. Almost everyone is familiar with traditional surveillance, in two senses: they are *knowledgeable* of it, since it has been around for decades, and they are *comfortable* with it, since (due to the technological limitations of the twentieth century and the logistics of deploying such surveillance) they have little reason to expect ever having to face such surveillance in real life. But the technological advances of the past few decades have given rise to a new form of surveillance with which people are less familiar in the first sense but not the second: digital

surveillance. By that, I mean few are *knowledgeable* as to the extent of modern-day digital surveillance in the United States – the scale at which it is implemented, the technology behind it, its targets, anything beside a cursory understanding of the NSA's activities. At the same time, few are *comfortable* with digital surveillance, because what little they do understand is that the advances in technology allow anyone – and thus, potentially everyone – to be a target.

In the past decade or so, the National Security Agency and other U.S. governmental agencies have begun enacting mass surveillance of the American populace using new technologies in the name of protecting national security. However, owing to the increasingly invasive nature of these surveillance methods and the lack of evidence that these methods have prevented a significant number of terrorist attacks on American soil, it becomes more and more evident that we are not striking an even balance between the interests of national security and of individual liberty. After all, surveillance by definition has an element of suspicion. By enacting this warrantless surveillance on thousands of Americans who have done nothing to prove they are anything but innocent, let alone guilty, the U.S. government is treating citizens and green card holders like potential threats to the state instead of the people whose rights they are beholden to protect. When coupled with the worrying implications of mass data-collection on the American citizenry in a time where human rights abuses, technological advances, and lack of governmental oversight go hand-in-hand(-in-hand), it becomes evident that reevaluation of the current surveillance methods and security objectives is necessary, and until such time as that is possible, it is in the best interest of every American to inform themselves of the dangers of mass surveillance, speak up to their representatives at the state and federal level, and above all, avoid becoming complacent.

III. To the Community

"But wait," you may be thinking, "I have nothing to hide. So long as the interests of national security are being served, I am okay with the government going through my information, if it comes to that." First of all, is that really true? Many Americans have not committed any offense more serious than jaywalking, so from a legal sense, the hypothetical commenter may be right. However, everyone has their dignity, and in a mass surveillance culture such as this, the little embarrassments and secrets that one would keep to oneself or share only with those they can trust are also accessible to strangers hundreds of miles away. After all, "the government" is not the one reading your email to your friend from abroad, or listening in on your phone call to your deployed spouse – instead, it is (statistically speaking) a young man aged 18-22, freshly recruited from college. It must be remembered that the analysts employed at the NSA are subjective humans in positions of power with little oversight – but more on that later. It must also be remembered that, due to the mass data collection and storage, you might not have any information that would be incriminating *now* – but if this lack of oversight continues and the government, one day, makes a decision criminalizing a previously accepted behavior, you can retroactively be penalized for your past, previously legal behavior. That would be especially something to worry about if they have other reasons to target you, because, as subjective human beings, these NSA analysts and the people giving them orders have biases. And you do not want the biased people who make secret decisions about who will be wiretapped and potentially arrested to lack oversight.

Most importantly, even if the presence of mass surveillance does not affect *you* personally – and it probably affects someone you know, or even, just, you know, other American citizens, try having a little *empathy* – if this level of secrecy and mass surveillance continues, it can foster a culture of compliance and helplessness. After all, if you do not know what the NSA

considers target behavior, you will either live in fear as you continue to express yourself or – and this is the more likely option – you will begin to self-police your own behavior, silencing your dissent with the political or social situation and removing yourself from the democracy – if such a society could even still be called a democracy.

So, it's important that every citizen pays attention to mass surveillance, especially as it pertains to their most basic rights – freedom of expression, freedom from undue search and seizure, freedom of press – both at home and abroad. After all, while the most personally relevant news will concern the NSA as the legality of and media response to their tactics continues to evolve, one can and should look abroad to countries with questionable human rights records for a warning of what could happen to the United States if we do not agitate for change.

IV. Surveillance Technology Abroad

One way to begin examining the relationship between mass surveillance and human rights abuse is to look at mass surveillance practices around the globe, focusing on countries whose human rights track records are less than outstanding.

Russia has come into trouble with the United Nations, Human Rights Watch, and other entities for its laws stifling political dissent and online expression. Some recently adopted laws, for example, allow for unchecked government surveillance on virtually all online communications in Russia, violating the privacy of its citizenry. In addition, the government interprets dissidence or political/religious/military criticism as "extremism," and in so doing, invokes older laws that allow them to prosecute Russian citizens for dissident online speech, including "social media posts, online videos, media articles, and interviews," according to the Human Rights Watch. 216 Russian citizens were convicted of and punished for extremism-related crimes in 2015, approximately a 700% increase from 2010. The Human Rights Watch

article chillingly reports: “Today, many Russians are increasingly unsure about what is acceptable speech and what could land them a large fine or prison term” (Human Rights Watch, 2017). This example makes clear that the implementation of laws curtailing online privacy and lack of oversight for reinterpretation of old laws allows the Russian government to stifle freedom of expression and actively silence criticism.

Saudi Arabia is another example of a country that curtails its citizens privacy, especially in cases of protest or dissent. In 2014, Canadian-based Citizen Lab analyzed a sample of “lawful interception” malware, a malicious Android app downloaded by thousands that imitated the legitimate “Qatif Today” news application. Lawful interception malware is sold to governments for law enforcement purposes – but due to the lack of oversight for use of such technology, it can be misused and has been, especially against political dissidents. Features of this particular spyware app include obfuscated source code, key-logging, audio and video recording, screenshot-taking, accessing third-party communication apps, and location services. In addition, it grabs data about the user’s social media activity. Since the Qatif region has a history of protest against the Saudi government, which itself has a history of threatening and pressuring journalists, dissenters, and human rights activists, Citizen Lab proposes that the fake news app, which contains Hacking Team code, was likely introduced by the government to target protestors who use such local news sources and social media in order to organize protests (Marquis-Boire, Scott-Railton, Guarnieri, & Kleemola 2014). This surveillance could not only be used to track and arrest networks of protestors, but if word spread about the presence of such spyware, it would have the undemocratic effect of intimidating those who would otherwise be critical of the government into silence.

Another example of government spyware – known as "Pegasus" – has been found on the phones of several prominent Mexican lawyers, journalists, and activists which inundates the target with texts containing attention-grabbing titles and links which, if followed, will infect the target's mobile phone. Once infected, the phone will begin recording every aspect of the user's digital activity, including calls, texts, email, and audio/visual recording via the microphone and camera. Like the Qatif Today app, this spyware is sold to governments for the purpose of investigating criminal activity, but clearly is misused by the government against dissenters and their families due to lack of guidelines and oversight once purchased. As is standard for Mexican intelligence, the government must have gone against Mexican law to launch this spyware attack against its own citizens, since it is unlikely that they gained the necessary judicial to hack the phones. The New York Times details the experiences of anti-corruption actors who have dealt with this app: Juan Pardinas, a supporter of anti-corruption laws, says, "We are the new enemies of the state," having been inundated with these malicious links via text message. "Ours is a society where democracy has been eroded" (Ahmed & Perlroth 2017).

SUMMARY – These three examples of government surveillance using modern technology have been selected from a pool of many. They exemplify the fact that a country with a poor human rights record may take advantage of modern ways of organizing protests or merely expressing oneself to suppress dissidence and maintain control of an unhappy citizenry, thus illustrating how unchecked use of surveillance technology can be used to stifle the declared rights of the citizen. Just as the surveillance technology is used to suppress human rights, people attempting to exercise their rights becomes grounds for further deployment of surveillance technology. Good thing we don't need to worry about surveillance technology in the United States, though, right?

V. Surveillance Technology in the United States

The modern NSA surveillance program began in 2001, relatively traditionally. It originally was known as the “President’s Security Program,” as George W. Bush, secretly and without public consent, authorized the warrantless wiretapping program that searched for terrorists by monitoring calls between one person inside of and one person outside of the United States. It had relatively limited scope at first. Analysts eavesdropped and analyzed metadata: where each caller was, how long the call lasted, etc. Even this analysis would ordinarily require a warrant, and once two reporters broke the story in 2005, the legality went to the courts (Lichtblau & Risen 2005). The NSA continued with their operations, with some changes.

Ever since those auspicious beginnings, the NSA has cooperated with telecommunications companies who granted them backdoor access to caller data and their companies – without a warrant, still. Telecommunications companies like AT&T, MCI, and Sprint handed over calling records to the government, including personally identifiable information like names and street addresses, in an effort to create "to create a database of every call ever made" in the United States. The NSA was also allowed to install surveillance equipment at their facilities, granting them real-time access to the data, which they could store and then data-mine using keywords. The Electronic Frontier Foundation describes the process as follows:

> When you send an email or otherwise use the internet, the data travels from your computer, through telecommunication companies' wires and fiber optics networks, to your intended recipient. To intercept these communications, the government installed devices known as “fiber-optic splitters” in many of the main telecommunication junction points in the United States (like the AT&T facility in San Francisco). These splitters make exact copies of the data passing through them: then, one stream is directed to the government, while the other stream is

> directed to the intended recipients. ("How the NSA's Domestic Spying Program Works" 2014)

The NSA also has tools that allow for deep packet inspection, like the Narus Semantic Traffic Analyzer, which allowed them (in a less high-tech time) to analyze 10 gigabits of IP packets per second and reconstruct the interaction.

AT&T has had a special relationship with the NSA, in particular. It installed NSA surveillance equipment at more facilities than Verizon and other telecommunications companies. Between 2003 and 2013, AT&T helped the NSA carry out the secret wiretap order by grating access to billions of emails that passed through its domestic servers – some containing foreign correspondents, but many doubtlessly not (Angwin, et al. 2015). This furnishes further proof that the NSA is in cooperation with ISPs. This means that the NSA has access to even more sensitive information than is thought, since ISPs could use your browsing history to decode your political views, sexual orientation, and other extremely personal information (Brodkin, 2017). In addition, it is known that the NSA has access to the servers of companies like Google and Facebook and "extracting audio and video chats, photographs, e-mails, documents, and connection logs that enable analysts to track foreign targets" (Gellman & Poitras 2013). While these details may enable them to do just that, they also mean that everything one might upload to the internet has a substantial chance of ending up in a NSA database.

The above factors might even be fine and dandy if the government could be trusted without question to act in the best interest of the people – but past NSA behavior (like eavesdropping on protestors of the Vietnam War) and present NSA culture, and the fact that humans are curious, self-serving people, casts doubt on the possibility of a safe, non-invasive NSA database (if such a thing is even possible). The interviews with NSA whistleblower Edward Snowden reveal not only the profound lack of oversight but also several uninspiring details of

the workplace culture. According to Snowden, nude photos were not only intercepted but routinely passed around and remarked upon playfully:

> They turn around in their chair and they show a co-worker. And their co-worker says: "Oh, hey, that's great. Send that to Bill down the way." And then Bill sends it to George, George sends it to Tom and sooner or later this person's whole life has been seen by all of these other people. Anything goes, more or less. (Rusbridger & MacAskill 2014).

The government, first of all, can glean no national security information from one's intimate pictures. This huge invasion of privacy has no merit, and as such it reflects incredibly poorly on the institution that allows it to happen through lack of oversight. Many such incidents are never reported, or if they are, are self-reported. The NSA only answers to a secret council, the FISC, but even so they are mostly self-policed, which means that there are no consequences for such actions. Not only is that repulsive in the moment, it can only become more dangerous as time goes on and there continue to be no consequences.

This is especially galling, as in the sixteen years the program has been in effect, there have been negligible results that are attributable to mass surveillance instead of traditional surveillance. Snowden remarks:

> The White House investigated those programs [which allowed mass surveillance] on two separate occasions and on both occasions found that they had no value at all, and yet, while those panels recommended that they be terminated, when it actually came to the White House suggesting action to legislators, the legislators said: "Well, let's not end these programs. Even though they've operated for 10 years and never stopped any imminent terrorist attacks, let's keep them going." (Rusbridger & MacAskill 2014).

This is especially galling, considering the invasion of privacy thousands of Americans have experienced at the hands of the NSA: In 2012, there were 2,776 incidents "of unauthorized collection, storage, access to or distribution of legally protected communications" (Gellman 2013), but many more were uncounted. For what reason, then, do we continue to have our most

private moments glanced into and stored for posterity by strangers with security clearances? Without tangible results from such a program, the negatives become so much clearer: for example, that it consumes a huge amount of time and money; that the backdoors the government builds into our telecommunications systems, just like any backdoors, can be found and exploited by malicious actors; and that as these records are held onto and more are collected, the more danger we are in of becoming compliant and not holding the government accountable.

VI. Action Items

Use secure protocols and only send sensitive information over an encrypted connection! That means use HTTPS instead of HTTP whenever possible. Your Internet Service Provider cannot see any information you send over HTTPS; therefore, they cannot provide that information to the government. A handy browser extension is HTTPS Everywhere, which tries to force encryption on every site you visit.

Use mobile applications that protect your information, like DuckDuckGo (a search engine) and Signal (for texting and calling).

Use an ad-blocker, since websites do not always vet ads that run scripts. As a result, even a legitimate website can host malware hidden within advertisements.

Pick smart, unique passwords or use a password manager to keep track of many complicated passwords. Mix up your security questions, so if someone figures one of them out then they will not have free access to the rest of your accounts.

If you are worried about the government (or other malicious actor) accessing your files, encrypt your hard drive with a difficult-to-guess phrase and *remember that phrase* (McCarthy, 2015). In addition, use two-factor authentication so someone without access to, say, your cell phone cannot log in even if they do have access to your computer.

Use a VPN (Virtual Private Network) – you would have to shop around a bit for this one to find a provider you trust. If you pay for a VPN, your browsing will be encrypted, so other would not be able to trace you back to your IP address. They are usually more respectful of your privacy than your ISP, although they will also see your browsing history.

To preserve even more privacy than a VPN, you could find sensitive information using the Tor network, which routes your online traffic through several relays across the globe without letting others trace you back to your IP address (Brodkin, 2017). Be careful – using the Tor browser can be a cause of suspicion for the NSA.

Do not rely on private browsing/incognito mode – while it will prevent your own computer from saving your browsing history, it will not prevent your ISP from seeing your browsing history.

Stay informed on developments in mass surveillance and human rights at home and abroad, and if you feel that your freedom of expression is being infringed, reach out to your local, state, and federal representatives.

VII. Conclusion

Mass surveillance is a technologically enabled boon to national security, in theory. But in practice, at its worst, it looks more like redefining the definition of "extremism" or inundation your opponents with spyware to prevent political discourse and maintain the current governing body. In America, it is not at that point yet – but it is at the point of waste and pointlessly storing data on the American populace for what appears to be no good reason. It is at the point of pointless invasion into everyone's privacy. Is that liberty? It seems more like petty use of power. And we cannot let this level of surveillance continue unchecked, for fear that the pettiness may

morph into something more dangerous in the face of our complacence. As Edward Snowden says, “No system of mass surveillance has existed in any society that we know of to this point that has not been abused” (Rusbridger & MacAskill 2014). Citizens should not have to fear their government in any capacity, whether that means fear of needless invasion or embarrassment or fear of expressing oneself. It is time we take a good, long look at the NSA and at the rest of the world and take actual limiting measures so that it has to make good on its promise of benefit, or butt out.

VIII. References

"How the NSA's Domestic Spying Program Works." *Electronic Frontier Foundation*, 9 Aug. 2014, www.eff.org/nsa-spying/how-it-works.

"Online and On All Fronts | Russia's Assault on Freedom of Expression." *Human Rights Watch*, 18 July 2017, www.hrw.org/report/2017/07/18/online-and-all-fronts/russias-assault-freedom-expression.

Ahmed, Azam, and Nicole Perlroth. "Using Texts as Lures, Government Spyware Targets Mexican Journalists and Their Families." *The New York Times*, The New York Times, 19 June 2017, www.nytimes.com/2017/06/19/world/americas/mexico-spyware-anticrime.html.

Angwin, Julia, et al. "AT&T Helped U.S. Spy on Internet on a Vast Scale." *The New York Times*, The New York Times, 15 Aug. 2015, www.nytimes.com/2015/08/16/us/politics/att-helped-nsa-spy-on-an-array-of-internet-traffic.html.

Brodkin, Jon. "How ISPs can sell your Web history—and how to stop them." *Ars Technica*, 24 Mar. 2017, arstechnica.com/information-technology/2017/03/how-isps-can-sell-your-web-history-and-how-to-stop-them/.

Gellman, Barton, and Laura Poitras. "U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program." *The Washington Post*, WP Company, 7 June 2013, www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html.

Gellman, Barton. "NSA broke privacy rules thousands of times per year, audit finds." *The Washington Post*, WP Company, 15 Aug. 2013, 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?tid=a_inl&utm_term=.1b2affdfa6e2.

Lichtblau, Eric, and James Risen. “Bush Lets U.S. Spy on Callers Without Courts.” *The New York Times*, The New York Times, 16 Dec. 2005, www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html.

Marquis-Boire, Morgan, et al. “Hacking Team’s Government Surveillance Malware.” *The Citizen Lab*, 24 June 2014, citizenlab.ca/2014/06/backdoor-hacking-teams-tradecraft-android-implant/.

McCarthy, Kieren. “The Edward Snowden guide to practical privacy.” *The Register*, 12 Nov. 2015, www.theregister.co.uk/2015/11/12/snowden_guide_to_practical_privacy/.

Rusbridger, Alan, and Ewen MacAskill. “Edward Snowden interview - the edited transcript.” *The Guardian*, Guardian News and Media, 18 July 2014, www.theguardian.com/world/2014/jul/18/-sp-edward-snowden-nsa-whistleblower-interview-transcript.