Spring 4-13-2017

Surveillance Self-Defense: Privacy in the Post-9/11 Mass Surveillance State

Nathaniel D. Fortmeyer
Southern Illinois University Carbondale, fortn@siu.edu

SURVEILLANCE SELF-DEFENSE: PRIVACY IN THE POST-9/11 MASS SURVEILLANCE STATE

by

Nathaniel Dean Fortmeyer

B.A., Southern Illinois University, 2011
B.A., Southern Illinois University, 2013

A Research Paper
Submitted in Partial Fulfillment of the Requirements for the
Master of Science.

Department of Mass Communication and Media Arts
In the Graduate School
Southern Illinois University Carbondale
May 2017

RESEARCH PAPER APPROVAL

SURVEILLANCE SELF-DEFENSE: PRIVACY IN THE POST-9/11 MASS SURVEILLANCE STATE

By

Nathaniel Dean Fortmeyer

A Research Paper Submitted in Partial

Fulfillment of the Requirements

for the Degree of Master of Science

in the field of Professional Media and Media Management

Approved by:

Robert Spahr, Chair

Graduate School
Southern Illinois University Carbondale
March 28, 2017

AN ABSTRACT OF THE RESEARCH PAPER OF

NATHANIEL DEAN FORTMEYER, for the Master of Science degree in PROFESSIONAL MEDIA AND MEDIA MANAGEMENT, presented on MARCH 28, 2017, at Southern Illinois University Carbondale.

TITLE: SURVEILLANCE SELF-DEFENSE: PRIVACY IN THE POST-9/11 MASS SURVEILLANCE STATE

MAJOR PROFESSOR: Robert Spahr

The nature of digital information and the networked world has enabled the greatest advances in communication, education, art, science, and entertainment since the invention of the printing press. However, with each new day the systems and technologies to track people and predict their behavior only expand. Corporations and governments track anyone and everyone. Privacy has never been in such grave danger. The collection, storage, and analysis of data have enabled the expansion of the pervasive surveillance state. Journalists, whistleblowers, activists, and average citizens are all under attack. A democracy cannot thrive in an environment deprived of freedom of thought, information, and expression. The surveillance state chokes the light of freedom from such an environment, and democracy will suffer. Democracy will thrive if the citizens of the world rise up and continue the struggle for freedom, which is predicated upon the protections of privacy. Privacy allows journalists to work with sources and publish information so citizens may be informed. Privacy allows whistleblowers the ability to perform a vital public service: sounding the alarm when those in power abuse power. Privacy allows activists and dissidents the ability to exercise their First Amendment rights. Privacy allows the average person to have a secure space to exist away from the harsh gaze of society and develop mentally, spiritually, and emotionally.

DEDICATION

I dedicate this work to Dr. Arlene Tan; Sic Parvis Magna. Thank you for saving my life.

ACKNOWLEDGMENTS

I would like to express my very great appreciation to Professor Robert Spahr for overseeing my project, serving as my research project chair, and introducing me to HTML. This work would not have been possible without Rob's guidance, advice, and instruction. I would also like to thank my best friend and brother, Ryan Berry, and the love of my life, Alexis Holmes, for their unconditional love, support, and encouragement. My thanks equally extend to my parents, Kathy Edwards and Blaine Fortmeyer, for their love and support, both emotional and financial. My gratitude to Steve Sawyer at Morris Library, for his continued support over the years, as well as his judicious advice. I would also like to express my deep thanks to Leslie Love, a kindred spirit on this mortal coil; Leslie was always there for me, to keep me true, in every meaning of the word. I would also like to thank Olga Kaczmarczyk, for listening to me and giving perspective. And finally, I would like to offer my deepest gratitude to Lynne Frett, my friend and neighbor, for always looking out for me. Lynne, wise in the ways of the world, always ensured I did the right thing. I would not have completed this degree, and this paper, without her friendship.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

This research paper will address the dual threats of mass surveillance and data collection to privacy protections in the twenty-first century. Privacy is under sustained attack from governments and private corporations alike. The ability for an individual to be private and anonymous, to express intellectual curiosity and satiate it through the World Wide Web, is in danger. Governments, particularly the United States and its allies in the Five Eyes program, engage in mass surveillance against not just their own citizens, but every individual who uses digital technology.[1] Private corporations relentlessly track consumers, creating searchable databases cataloging their entire activity history.

The danger stems not just from this pervasive collection, but also from pervasive storage. As a result of technology's progression, computers are cheaper, faster, and more powerful, allowing government and corporations the ability to store massive collections of data in perpetuity. This aggregation of data, when paired with powerful statistical and algorithmic analysis, places a new, potent power in the hands of governments and corporations. Journalists and the sources with whom they communicate (particularly whistleblowers) as well as dissidents, activists, and average citizen, are all in grave danger.

There is hope in the face of such grave danger. Hope exists in free software, which has transparent source code and ultimately serves the end user. Hope exists in privacy enhancing technologies that block web trackers. Hope exists in encryption, which allows individuals to communicate privately and securely. The tools necessary to

make mass surveillance untenable already exist. It is only a matter of spreading the word, and awakening every human being to the potential to protect and preserve the integrity of their digital self.

CHAPTER 2

PRIVACY AND SURVEILLANCE

The Networked World and the Principles of New Media

The networked world of the Internet, and the subsequent layering of the World Wide Web atop it, has forever altered human civilization. The resultant information explosion, the greatest since the invention of the printing press, reverberates through every aspect of modern life.[2] Through the computer and the Internet, an individual has unprecedented access to information. This information glut, exponentially greater than the newspaper or television before it, has created a rich environment of data, accessible to humans at the speed of light (Postman, 2005).

With the doubling of technological capabilities inherent in Moore's Law, an individual needs neither a desktop computer nor a hardwired telephone connection; the telephone and computer have merged into the smartphone.[3] This same computer telephone also records images, audio, and video. The efficiency and ubiquity of modern computers have further enhanced human perception, reach, and knowledge. The repository of available knowledge has surpassed the human ability to digest it (Postman, 2005). What's more, this knowledge is malleable, and is represented in not just the language, mathematical diagrams, and images of printed books, but now sounds and moving images. The language of the Internet and the World Wide Web is the language of new media: computer data is represented as numerical information, and as a result of this numerical representation, it is subject to the principles of modularity, automation, variability, and transcoding (Manovich, 2001, p. 27-48).[4] The ability to cut, copy, and paste, combined with automation that allows for the removal of

human intentionality, has imbued the networked world with new powers (Manovich, 2001).

Not only do humans consume more data than they have at any point in history, they also generate more data than ever before. Just as the information explosion of the Internet increased the human capacity to amass data, it also increased the human capacity to generate not just data, but metadata. Governments and corporations collect and store not just data, but also metadata; this increase in metadata collection, retention, and analysis further erodes privacy.

Data and Metadata

Metadata, or data about data, is everything except the data itself. For example, a photograph is the data, while the metadata is the camera model, lens, time of day, and location where the photograph was made (Schneier, 2015a). Just as photography, telegraphy, and printing increased the ability to generate data, so have advances in computer technology and networks allowed for unprecedented increases in the generation of metadata.

There was a time when a photographer made a photograph with a film camera. The record existed as the data of the negative, and any ancillary details, unless explicitly recorded by the photographer, were either lost or difficult to surmise. In the digital world, when a photographer makes a photograph with a digital camera embedded in a smartphone, not only does he or she generate an image, but also a slew of metadata. By examining this metadata, one would know exactly what time of day the image was made, at what exact GPS coordinates, and camera's settings, such as aperture, shutter speed, and ISO. If the photographer was so inclined to send this

image to others via text or email, or post to social media, then further metadata is tied to the image, such as the physical location of the sender at the time of upload. The same information holds true for any individual who views the image electronically, unless the viewer goes to extreme lengths to subvert the tracking systems inherent in the electronic world. Currently, the United States of America kills people based upon metadata alone, in drone strikes and other military operations (Greenwald, 2014a; Granick, 2017).

This is the crux of the privacy problems inherent in the digital, networked world. As networked technology becomes cheaper, faster, and more efficient, the ability to store and analyze data will also become cheaper, faster, and more efficient (Schneier, 2015a; Greenwald, 2014a; Granick, 2017). Combined with the invisibility of the networked world, this pervasiveness of data collection and storage creates a system rife for abuse. Every leader, from feudal lords to the directors of the East German Stasi to the current director of the NSA, operates on the maxim that information is power. Currently in the United States, an individual does not retain any legal rights to the majority of his or her data; private companies specializing in data collection, known as "big data," make huge sums of money off of the buying and selling of data (Schneier, 2015a). There are very few legal restrictions in the United States which limit the ability of a corporation to collect, store, and sell customer data (Schneier, 2015a). The dearth of legal restrictions, combined with corporate greed and evolving ties with the United States government, results in a toxic environment of data mining and retention.

Big Data and Surveillance

The applications can be as frightening as they are intoxicating. In the best case

scenario, the consumer receives services, products, and advertisements tailored to his or her deepest, most specific needs and desires. In the worst case scenario, targeted advertisements haunt consumers with the invasive creepiness normally associated with stalkers. And stalking it is: the only difference between an obsessed stalker sifting through your garbage and a private corporation aggregating, analyzing, and storing your data is scale, storage, and analysis. In the case of private corporations, this information is used to amass consumer profiles and alter pricing for services, including medical insurance (Schneier, 2015a). Private corporations combine this invasiveness with analytical algorithm tools to further enhance the creep factor. The chain store Target was able, through analysis of loyalty card purchases, to correctly surmise when its female customers were pregnant, and used this information to send the expectant mothers coupons for pregnancy related products (Schneier, 2015a). The system Target used was so sophisticated, it even assigned each of the women an approximate due date.

Americans have more to fear than private corporations. The data mining threat is amplified in several different ways by the National Security Agency and other U.S. intelligence agencies. Not only is the data amassed by corporations available on the open market, but the NSA has unfettered access to this same information, and more. Beyond this corporate collection, the NSA has a much farther reach. Thanks to Edward Snowden's revelations, the role of the NSA in a broad, mass surveillance program has been public knowledge since 2013 (Greenwald, 2014). Edward Snowden and his revelations will be addressed more extensively in chapter four.

Defining Privacy

Daniel Solove (2007, p. 756) outlines just how difficult it is to define privacy, stating that privacy “is not reducible to a single essence” but instead is comprised of a plurality of different elements which bear a resemblance to one another. Definitions of privacy can fall on a spectrum anywhere from a strict definition, entailing only intimate details, to a broad one which defines privacy as the right to be left alone (Solove, 2007). However it is defined the importance of privacy has long been recognized in many societies. The United Nations (1948, Article 12) enumerated privacy among its Universal Declaration of Human Rights, asserting “no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor or reputation.”

Privacy can be violated through information collection via surveillance and interrogation, and it can also be violated through information processing, via aggregation and identification (Solove, 2007). In whatever way it is violated, though, privacy is often viewed as a fundamental right, a prerequisite for individual sovereignty (Solove, 2007). This individual sovereignty also fills a societal need, by allowing individuals a space to flourish, relieved from the friction of society, and thus free to develop and explore mentally, spiritually, and emotionally (Solove, 2007; Greenwald, 2014a; Greenwald, 2014b).

Why Privacy Matters

Before delving into the current, grave threats to privacy, it is important to underscore just how important privacy is. Often, supporters of government surveillance and corporate tracking of consumers state that privacy is relative and unimportant. In the case of government surveillance, supporters claim that privacy is a trade-off for

security, and that perfect security may be achieved at the cost of privacy. Supporters of corporate surveillance claim that big data collection allows corporations to better tailor products and services and increase efficiency. Both assertions are erroneous. There is no such thing as perfect security, and treating privacy and security as a binary choice overlooks both the importance of civil liberties and the realities of counterterrorism. The relationship between security and privacy is not a transactional one. Also, corporations do not violate consumer privacy in pursuit of helping the consumer. Corporations violate consumer privacy in pursuit of higher profits. Again, it is not a matter of a transactional relationship between consumer privacy and product quality.

What is more, as Glenn Greenwald (2014b) notes, the United States, under the dubious aegis of protecting its citizens has, "converted the Internet, once heralded as an unprecedented tool of liberation and democratization, into an unprecedented zone of mass, indiscriminate surveillance." This surveillance state became a reality in the wake of 9/11, and the resultant public fears, stoked by hawkish politicians, were used as justification. After 9/11, the United States government, under the direction of the Bush administration, pushed the Patriot Act, and also began a program of mass, illegal wiretapping (Granick, 2017; Greenwald, 2014a). The illegal Bush wiretapping program not only violated Constitutional protections, but was also the direct result of collusion with telecommunications giants, such as AT&T (Granick, 2017). However, the current surveillance state is not a targeted apparatus focused on probable cause and tailored surveillance; the current surveillance state is anathema to privacy, as well as several of the fundamental amendments in the U.S. Bill of Rights. This danger to privacy takes many forms and represents many dangers to journalists, activists, and the average

person.

All of us, not just terrorists and criminals, have things to hide (Greenwald, 2014b). Those who claim privacy does not matter do not even believe it themselves; they still put passwords on their accounts and locks on their doors (Greenwald, 2014b). Human behavior changes when we know we are being watched, and this change affects our curiosity, psychology, and emotional well-being (Greenwald, 2014b). Psychological studies have concluded that people are more conformist and compliant when they suspect they are being observed, and when these effects extend to individuals browsing the internet, then it leads to chilling effects and self-censorship (Greenwald, 2014a, Greenwald, 2014b, Schneier, 2015a).

Ironically, even those who decry privacy and profit from its erasure still take steps to protect privacy in their own lives. Facebook CEO Mark Zuckerberg, after declaring that privacy was dead, purchased four homes adjacent to his Palo Alto, California estate, to the tune of more than thirty million dollars, to ensure a “zone of privacy” (Greenwald, 2014b; Schneier, 2015a). Current F.B.I. Director James Comey covers the webcam in his laptop with tape.

The concept of total loss of privacy is nothing new; eighteenth century philosopher Jeremy Bentham designed the Panopticon, a prison institution where at any moment, guards could watch any of the inmates (Foucault, 1979; Greenwald, 2014b). Each cell is flooded with unremitting, harsh light, and although guards do not continuously surveil every prisoner, the Panopticon derives its power from the prisoners' uncertainty regarding when they are being watched, coupled with the awareness that, at any moment, they could be observed without their knowledge (Foucault, 1979).

Although guards could not watch all inmates at all times, the inmates could not see into the Panopticon, and would have no way of knowing when they were being watched, thus being forced to assume they were being watched at any given moment. This knowledge of possible surveillance would be the ultimate enforcer of obedience and compliance (Greenwald, 2014b). The Panopticon acts as a total surveillance tool, using the potential for mass, around-the-clock surveillance to induce fear and compliance (Foucault, 1979).

Today's mass surveillance creates a prison in the mind, and thus a much more subtle, much more effective means for societal control than mere brute force (Greenwald, 2014b; Foucault 1979). U.S. government surveillance programs, combined with the pervasiveness of networked computers, results in a new type of digital Panopticon, which not only operates in space, but also time. Viewed in the fourth dimension, the mass surveillance and data retention operations of the NSA allow the government the power to retroactively comb through every communication, web search, photograph, video, and sound recording of any individual who has used a computer or cellular device (Greenwald, 2014). Not only is this system rife for abuse, but it also creates a chilling effect that affects the way a citizen behaves (Greenwald, 2014; Schneier, 2015a). Awareness of government spying drives many Internet users to self-censor, and purposefully avoid looking up certain topics, information, or news, for fear of how they may be targeted or perceived (Greenwald, 2014; Schneier, 2015a). This chilling effect extends to potential political and social activists; many would-be activists fear, rightly so, increased government surveillance as a result of activism and protests, and U.S. intelligence agencies have a long, sordid history of spying on civil rights

leaders and protestors (Greenwald, 2014; Schneier, 2015a; Ventura & Russell, 2011; Brunton & Nissenbaum, 2015; Granick, 2017). Fossil fuel corporations have used similar tactics to target and discredit environmental activists (Fallis & Greenberg, 1998).

Considering such a system of mass surveillance, it is impossible not to reference *1984*, in which George Orwell (1950) describes a similar surveillance state, where each citizen is aware of the possibility that, at any moment, they are being monitored in real time by their own government. As Greenwald (2014b) notes, such a society, in which people can be monitored at all times, inherently "breeds conformity and obedience and submission," in contrast to the realm of privacy, in which one has access to an environment in which he or she "can think and reason and interact and speak without the judgmental eyes of others being cast upon us, in which creativity and exploration and dissent exclusively reside."

A system of mass surveillance renders off-limits all sorts of behavioral choices, chiefly among them dissent (Greenwald, 2014b). A common rebuttal to privacy activists is the claim that "I do nothing bad, I am harmless, I have nothing to hide" (Schneier, 2015a; Solove, 2007). This is the equivalent of saying "I am not concerned about free speech because I have nothing interesting to say" (Greenwald, 2014b). Dissidents and activists and journalists provide a public good and challenge the establishment (Greenwald, 2014b; Bernstein & Woodward, 1994; Brunton & Nissenbaum, 2015). However, even the average citizen, even if engaging in banal behavior, of which they are unashamed, should value privacy. The assumption that only those with something to hide should value privacy is a false one (Solove, 2007). Instead of framing the argument to cast suspicion on privacy, one could easily flip the script and cast suspicion

on those conducting surveillance (Solove, 2007).

A more refined expression of the “I have nothing to hide” argument is that NSA surveillance and other data mining programs are automated, and even if they do reveal sensitive information, it is only to a few government workers engaged in a fight to preserve national security, and only those engaged in illegal acts have anything to hide (Solove, 2007). It is not merely a matter of Orwell's Big Brother collecting information, but also of Kafka's world in *The Trial*, one centered on an indifferent, opaque bureaucracy that processes information (Solove, 2007). This bureaucratic storage of information can fundamentally alter the relationship citizens have with the institutions that control their lives (Solove, 2007). This storage results in a problem of aggregation, which Solove (2007, p. 766) defines as the “combination of small bits of seemingly innocuous data.” Through this aggregation, a person who otherwise feels he or she has nothing to hide is subject to powerful data mining and analysis, which can allow the government to glean much more information than the sum of its discrete parts, and even go as far as to predict future behavior (Solove, 2007; Schneier, 2015a). This relates to the privacy problem of exclusion, in which individuals are barred from accessing and correcting data (Solove, 2007). The problem of exclusion is particularly dangerous when coupled with an agency such as the NSA, which historically has enjoyed a high level of secrecy and little oversight (Solove, 2007; Greenwald, 2014a; Schneier, 2015a).

The fundamental problem with the nothing to hide argument is that it is based upon the assumption that privacy is about hiding bad things, and is a process centered on secrecy and concealment (Solove, 2007). Privacy, as it is enshrined in the Bill of

Rights, as well as the U.N. Declaration of Human Rights, represents a critical component of an individual's freedom and autonomy. Privacy facilitates freedom of thought, freedom of speech, and freedom of religion.

Free Software

Free Software is computer software distributed under terms that allow the software users to run the software for any purpose. Free software respects the users' freedom and community, allowing all users the freedom to run, copy, distribute, study, change, and improve the software (Stallman, 2010). Richard M. Stallman began the free software movement in 1983, he launched the GNU Project, a collaborative project with the goal of creating a freedom-based operating system. Richard M. Stallman also founded the Free Software Foundation in 1985, for the purpose of supporting the free software movement. Free software is free in the sense of liberty, although free software is often available at no monetary cost. Free software is sometimes called libre software, which borrows from the French or Spanish word for free as in freedom, as opposed to gratis.

The criteria for whether or not a piece of software is truly free depends upon the following criteria, known as the four essential freedoms: freedom to run the program as you wish, for any purpose (freedom 0), study how the program works, and change it (freedom 1), redistribute copies so you can help your neighbor (freedom 2), and the freedom to distribute copies of your modified versions to others (freedom 3) (Stallman, 2010).[4] Software that does not meet these criteria is proprietary software.

Free software is software that works for the user, and empowers him or her to both understand how the software works, and also change and distribute the code.

There are many advantages to free software, on both an individual and societal level. Free software grants users the ability to understand and determine the tools for electronic communication and creation. Free software allows more users to examine the source code, and thus increases the chances a software vulnerability will be observed and patched. Free software empowers the user, not private corporations, and is an important defense against the concentration of power. Many of the best tools for preserving privacy and combatting mass surveillance are free software.

Encryption

Encryption is the process of encoding a message or information in a way that only authorized parties can access it. Encryption is, by far, the single most important privacy enhancing technology (Schneier, 2015a, p. 215; Granick, 2017, p. 63).

Encryption does not preclude interference or interception of a message, but it does prevent the eavesdropper (commonly referred to as a “man-in-the-middle”) from being able to easily read the message; if data is stolen, but encrypted, generally the attackers will not be able to decode it (Granick, 2017). Without the corresponding key to unlock the message, known as the plaintext, the contents will remain invisible, and appear only as a ciphertext: a string of alphanumerical characters that are meaningless without the corresponding encryption keys.

Email encryption typically uses asymmetrical encryption, in which two keys are generated: a private key that remains on the user's device, which is never shared, and a public key that is posted publicly on the Internet and/or shared in person. The two keys are different, but still mathematically related (Mitnick & Vamosi, 2017).

The most popular method of email encryption is PGP, which stands for “Pretty

Good Privacy," and is a product of the Symantec Corporation (Mitnick & Vamosi, 2017, p. 34). However, the creator of PGP, Phil Zimmermann, also wrote an open-source version, OpenPGP, which is free. Werner Koch also created GPG (GNU Privacy Guard), which is also free. All three methods of encryption are interoperational (Mitnick & Vamosi, 2017). Hard drives, email accounts, individual files, and text messages can all be encrypted. Chapter six will cover specific encryption programs, such as Signal, in greater detail. Encryption is the most important tool for preserving privacy. The mass adoption of encryption would render mass surveillance untenable.

CHAPTER 3

MASS SURVEILLANCE STATE

FBI Civil Rights Surveillance: Dr. King and Black Lives Matter

African Americans, and in particular, African American civil rights activists, have a long history of being subjected to this level of surveillance. J. Edgar Hoover's FBI surveilled civil rights organizations in an attempt to subvert their work; Hoover's FBI routinely spied on Rev. Dr. Martin Luther King, Jr., as well as other prominent civil rights leaders, organizers, and activists, through illegal wiretaps, photographic surveillance, and physical observation of movements (Gage, 2014; Kayyali, 2014; Granick, 2017). The goal of such covert surveillance was to discredit civil rights leaders and their movement, and also use this information in attempts to fracture activists groups from within, strategies still used to this day (Kayyali, 2014). Particularly relevant to the current, invasive, pervasive surveillance state was the FBI's anonymous letter to Dr. King, written with the intended purpose of driving him to commit suicide, using personal information gleaned from their illegal surveillance (Kayyali, 2014; Granick, 2017). This information, including references to Dr. King's extramarital affairs (citation and reference of specific language from letter), combined with the intent to discredit, disgrace, and destroy Dr. King, underscores the dangers of targeted surveillance in regard not just to chilling effects on activism itself, but also a targeted campaign against a powerful civil rights leader. This same strategy can be used today, with much greater ease, precision, and depth, and on a mass scale. Although the FBI had to deploy extensive resources including wiretaps and physical surveillance, such intrusions are commonplace today, and it is merely a matter of searching an extensive intelligence

agency database for such potentially compromising information. President Obama's decision, in the final days of his presidency, to grant the NSA the ability to share illegally obtained information with a host of other intelligence agencies, including the FBI, increases the danger of such illicit smear campaigns against any viable threat to government power (Emmons, 2017).

History is repeating itself in the twenty-first century; Black Lives Matter (BLM), an international activist movement aimed at combatting systemic racism, police brutality, and racial inequality in the United States criminal justice system, is a frequent target of federal, as well as state and local, law enforcement surveillance (Jeffries, 2015; Reel, 2016; Choudhury, 2015; Joseph, 2015; Leopold, 2015).

Police crackdown on protesters is nothing new, but ubiquitous cell phone cameras and internet connections allow protestors and activists to livestream both protest events as well as subsequent law enforcement retaliation; in the case of Occupy Wall Street, captured footage was used to document journalists targeted for arrest (Goodman & Moynihan, 2012). However, the techniques used by law enforcement also evolve, and as Amy Goodman and Denis Moynihan (2012, p. xix) note, while law enforcement's targeting of journalists is nothing new, “police interference, through intimidation, forced relocation away from sites of newsworthy events, assault, destruction of equipment or erasure of digital media, and arrest” are all accelerating concurrently with the press and public's ability to record and publish events as they occur. The police, as well as private security corporations working with them, target protesters through the protesters' own digital devices.

Persistent Surveillance Systems

Founded by Ross McNutt, Persistent Surveillance Systems represents merely the latest incarnation of a private corporation bridging the gap between military industries and government mass surveillance. Persistent Surveillance Systems contributes to the growing trend of corporations developing military technology for the armed forces of the United States, and then turning around and deploying the same technology within U.S. borders, against American citizens.

In 2006, McNutt gave the U.S. military Angel Fire, a “wide-area, live-feed surveillance system that could cast an unblinking eye on an entire city” (Reel, 2016, p. 52). Built around an assembly of four to six industrial imaging cameras, the system was attached to the bottom of an airplane; as the plane flew overhead, the images were stabilized with the aid of computer software, stitched together, and transmitted to ground forces. The result was a searchable, constantly updating photographic map stored upon multiple hard drives. McNutt pitched the program as “Google Earth with TiVo capability” (Reel, 2016, p. 52). The U.S. armed forces deployed the system in Iraq. McNutt eventually upgraded the system with all-weather and nighttime capabilities, and later leased the system to Ciudad Juarez, Mexico.

The goal of Angel Fire is to take this searchable database and, once a crime is committed, rewind the footage to search for evidence and track the origin of a vehicle or a suspect. However, the goal is not just to identify an enemy, but an enemy network. As with other surveillance technology, there is no inherent safety mechanism to make value judgments. The “enemy network” could be a gang of drug dealers or terrorists. The “enemy network” could also be a group of activists exercising their First Amendment rights to peaceful protest, or a team of investigative journalists meeting

with a whistleblower.

Inevitably, a system based upon Angel Fire was used inside the United States. Since the beginning of 2016, Persistent Surveillance Systems has teamed up with the Baltimore Police Department, and through the funding of a private donor, deployed the same system within the Baltimore city limits. Persistent Surveillance Systems's Cessna sometimes flew above Baltimore for up to ten hours a day. The public had no idea the system was in use, and no public disclosure was made by the city of Baltimore to its citizens (Reel, 2016). The surveillance system was used extensively to monitor potential protests, in anticipation of the verdict in the case of the Baltimore police officers charged with the murder of Freddie Gray.

As Persistent Surveillance Systems monitored Baltimore from the skies, the city police department was the subject of an FCC complaint, originating from a civil rights group, which included charges the city used cell phone tower simulators, known commercially by the trade name StingRay, to spy on citizens; the police later admitted to the illegal spying in court (Reel, 2016). The StingRay device, which is also known as an IMSI-catcher, performs a man-in-the-middle attack.[6] By sending out a strong, false signal, the StingRay tricks mobile phones into thinking it is a mobile tower, and thus the mobile phones connect to the StingRay. The StingRay captures all data that the mobile device transmits, and all unencrypted communications are vulnerable to interception. The FBI has used the StingRay and similar devices to monitor activists, particularly those involved with the group Black Lives Matter.

Persistent Surveillance Systems also had a nine day trial with the Los Angeles County Sheriff's Department, to monitor Compton, a largely minority city south of L.A.

(Reel, 2016). After the trial, the city declined to purchase services, and a year later, the citizens of Compton discovered the surveillance trial. Angry protesters demanded new privacy protection from their local government, although even the mayor of Compton had not been informed about the program. McNutt believes the surveillance program does not threaten individual privacy, and met with a senior policy analyst at the ACLU to try and address criticism at the source. McNutt believes that, since the aerial images cannot identify specific individuals, the actions of all Persistent Surveillance Systems employees are automatically monitored by the software through logs, and tracking only occurs over public roads where individuals have no expectation of privacy, the program does not violate privacy (Reel, 2016).

Privacy advocates have expressed grave concerns regarding McNutt's assurances. Technology will continue to improve; the system McNutt uses will only become cheaper, faster, and more powerful. Also, although the airplane-mounted cameras cannot currently identify individuals on the ground, the time-coded nature of the footage means that it can be paired with other cameras on the ground. As was the case in Baltimore, police were able to pair the aerial footage from Persistent Surveillance Systems with street level, high resolution cameras in order to track and identify a suspect (Reel, 2016). Thus, the aerial, round-the-clock tracking from Persistent Surveillance Systems can be paired with parallel surveillance systems to form a synergistic toxicity to privacy and civil liberties.

CHAPTER 4

EDWARD SNOWDEN

In June of 2013, Edward Snowden began a public debate about privacy and surveillance that is not only still ongoing, but more relevant than ever. An NSA contractor and former CIA employee, Snowden became the most important whistleblower in modern American history when he revealed the extent of the mass surveillance apparatus of the United States of America. Snowden, echoing earlier Pentagon Papers whistleblower Daniel Ellsberg, risked his life to reveal widespread systematic deception to the American people, on the part of their own government. Snowden's meeting with journalists Glenn Greenwald, Laura Poitras, and Ewen MacAskill further echoed the clandestine meetings between journalist Bob Woodward and his Watergate source, Deep Throat.

Edward Snowden revealed the depth and breadth of a massive spying program that exceeded the distinction of foreign versus domestic; the National Security Agency of the United States was interested in one thing, and that was total acquisition of *all* communications. The NSA that employed Edward Snowden focused on neither foreign nor domestic communications, but instead on global communications. The explicit purpose of the NSA, and the programs on which Edward Snowden worked, was the total collection and indefinite storage of all electronic activities of every man, woman, and child on Earth. Daily, the NSA collects and stores telephone calls, text messages, emails, search queries, and web browsing histories, and with little-to-no oversight.

During the course of his duties, Snowden became concerned by the massive overreach of the domestic spying program (Greenwald, 2014). Snowden amassed a

treasure trove of documents proving the breadth and depth of the program: under the auspices of the United States's war on terror, the NSA was using the sweeping powers, authorized in the wake of 9/11, to acquire the telephone records and metadata of all Americans (Greenwald, 2014). Major telecommunications providers such as Verizon and AT&T secretly provided private customer data directly to the NSA, as did Facebook, Skype, Yahoo, AOL, Apple, Microsoft, Google, PalTalk, and YouTube (Greenwald, 2014). Microsoft also built backdoor access into their source code, allowing the NSA unfettered access to private computer systems (Greenwald, 2014; Schneier, 2015a). The alphabet soup of NSA subprograms, such as PRISM and XKEYSCORE, existed for the sole purpose of collecting all data on all Americans all the time (Greenwald, 2014).

Here it is helpful to quote the Fourth Amendment in its entirety:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. (U.S. Const. Amend. IV)

It would have been difficult indeed for the original authors of the Bill of Rights to foresee the role computers, smartphones, and the Internet would have in society. However, the authors did foresee the ramifications of the control of information, and the need to protect the privacy of individual citizens against government overreach, hence the requirement for probable cause and independent, judicial oversight.

Privacy law in the United States has always struggled with, and lagged behind,

the emergence of new technology, and in wake of the tragic events of 9/11, citizens and government officials alike are increasingly eager to trade civil liberties in exchange for the illusion of safety (Greenwald, 2014; Schneier, 2015a; Granick, 2017). Individuals tend to improperly estimate risk, and often fear more dramatic outcomes as opposed to mundane ones; generally, people are more afraid of flying than driving, even though the risk of fatality is much higher in an automobile (Schneier, 2015b). The same fear of the extreme and dramatic leads to the clouding of judgment regarding the threat of terrorist attack, and has been used as a pretext by the federal government to pass sweeping expansions of mass surveillance, often tapping directly into the roots of telecommunications providers (Greenwald, 2014; Schneier, 2015a; Burrington, 2016).

In the twenty-first century, a man or woman's computer is his or her castle. Many people use their smartphone, tablet, or laptop for all communications, business, interpersonal, or otherwise. Instead of navigating the Internet through a web browser, many smartphone users opt for applications, or apps, which often create direct access between a user and a website or service. These apps also must be downloaded as software, and require a user's permission to access his or her device. Data overreach tools are often embedded in these apps, and they collect data unrelated to app functioning (such as GPS coordinates or a user's contact list) and send it back to the controlling company. These techniques are in the source code, and thus exist in the background for the user, who often chooses convenience over control (Schneier, 2015a). The same holds true for Facebook, Google, and Google mail (Gmail): the service is, on the surface, free to all users. But there is a hidden cost: every piece of the user's data and metadata. Google scans the contents of all Gmail messages with an

automated algorithm; Google publicly claims that no human eyes scan the messages, and that it is simply for advertising research, but the implications are chilling, and these electronic messages, the modern equivalents of letters, are stored in an electronic castle, which often has a backdoor built into the source code (Schneier, 2015a; Mitnick & Vamosi, 2017). Yahoo and other free email providers similarly scan emails for fodder for advertisements (Mitnick & Vamosi, 2017).

With houses, papers, and effects, the government needs a warrant. The electronic castle, however, even if protected in one form, is vulnerable in another. Even if a sender possesses a secure computer, the transmission of information is vulnerable as it passes through the networked world, and is vulnerable on the device of the receiver. The documents Snowden passed to journalist Glenn Greenwald include evidence that the NSA has tapped into the undersea fiber optic cables that facilitate Internet traffic across the Atlantic Ocean (Greenwald, 2014a). The same documents also reveal that the NSA intercepted Cisco routers, en route through package delivery services to foreign markets, and installed backdoor technology to monitor foreign users (Greenwald, 2014a). Of course, many devices themselves are not secure, and easily hacked, and Snowden has also recalled instances of fellow NSA contractors capturing webcam footage of couples during physical intimacy, when the webcam was ostensibly turned off, and sharing them throughout the NSA office (Greenwald, 2014; Schneier, 2015a). Individual hackers, operating alone, can accomplish the same feat, and have (Schneier, 2015a).

The NSA and other federal agencies further undermine the Fourth Amendment with secret gag orders and Foreign Intelligence Surveillance courts, which are

ostensibly tasked with conducting oversight on intelligence agencies, but in practice act as a judicial rubber stamp for overreach (Greenwald, 2014a; Granick, 2017). The language of the Fourth Amendment clearly indicates that an invasion of an individual's privacy is severe enough of an act to warrant approval from a judge (U.S. Const. Amend. IV). However, FISA courts are secret courts that strictly control requests for information, have little to no oversight, and rubber stamp all requests for surveillance. Although judges have required a handful of FISA requests to be rewritten or clarified, the secret courts have yet to deny a request and exist under limited judicial and congressional oversight (Greenwald, 2014a). The United States government's intelligence agencies also use gag orders in order to prevent disclosure of mass surveillance programs; although many private corporations and tech companies readily comply with the NSA and FISA courts, even those that resist are prevented from disclosing U.S. government overreach to their users (Greenwald, 2014a; Schneier, 2015a). The email provider Lavabit offered email encryption and privacy protection to its users, one of which was Edward Snowden; the service was targeted by the U.S government as part of efforts to track Snowden, and after FISA court pressure and a gag order, the company's owner and operator, Ladar Levison, shut down his servers instead of complying (Greenwald, 2014a; Schneier, 2015a). Unfortunately, when it comes to taking a principled stand against illegal searches and seizures, Lavabit is the exception, not the rule.

Beyond the civil liberty concerns, the bulk collection of data and metadata is an ineffective, wasteful method of gathering intelligence and conducting counterterrorism operations. The true signal is lost in a sea of noise, and the needle disappears further

into a haystack (Schneier, 2015a). The bulk collection and storage of data allows U.S. intelligence agencies to retroactively gain intelligence on terrorists after the attack, but it does not prevent the attack itself. The 2013 Boston Marathon bombing is a case in point: the FBI and NSA could stretch back into the data and metadata of the Tsarnaev brothers after the fact, but were unable to predict the attack, despite one of the brothers having already been investigated by the FBI (Schneier, 2015a). Targeted investigations are what prevent terrorist plots, and these investigations have long been conducted within the bounds of the U.S. Constitution; a targeted, focused investigation yields more reliable evidence, and is a better allocation of resources than mass surveillance (Schneier, 2015a; Schneier, 2015b; Greenwald, 2014).

In light of Snowden's revelations, the United States government claimed that in many of these instances the NSA only collected bulk metadata. This does not mitigate the dangers of abuse and overreach. Even if the NSA does not intercept the data, and only collects metadata, the mass nature of the collection and analysis allow for reasonable deduction of the data itself. This is the electronic equivalent of a private investigator hired to follow an individual. Although a private investigator cannot always directly eavesdrop, and may not be close enough to physically listen in, he or she can still monitor the subject's movements, with whom the subject meets, when the subject meets with that individual, and where that subject meets with the individual (Greenwald, 2014; Schneier, 2015a; Fallis & Greenberg, 1998). From this metadata, a private investigator could deduce a subject's sexual proclivities, political affiliations, and activist intentions (Greenwald, 2014; Schneier, 2015a; Fallis & Greenberg, 1998). A private investigator can legally search a subject's garbage (it is considered abandoned

property), and gain further insight into his or her lifestyle (Fallis & Greenberg, 1998). Currently, this same information exists as a digital equivalent, in both data and metadata.

Whether used by Google or the NSA, the data and metadata collection and storage tools are faster, cheaper, and more efficient; for better or worse, these systems also possess a perfect memory. Unlike analog records and data, which require much more work to collect, store, and analyze, digital records and data follow the principles of new media, and these principles, combined with current digital transfer speeds and storage capabilities, allow an individual or organization to store entire decades worth of Census records on a pocket USB (Schneier, 2015a; Manovich, 2001). Snowden leaked thousands of documents to journalist Glenn Greenwald, and they all could fit on a single SD card (Greenwald, 2014). The NSA has already built a data center in Bluffdale, Utah, for the express purpose of storing, in perpetuity, data collected through mass surveillance (Greenwald, 2014).

The Snowden story not only exposed the unconstitutional mass surveillance apparatus of the United States government, but also exists as a case study in the evolution of the relationship between a journalist and his or her source. Given the depth, sophistication, and pervasiveness of surveillance and data collection tools, it is increasingly difficult for a source to communicate privately and confidentially with a journalist. On a risk assessment scale, the difficulty increases proportionate to the severity and scope of the target and story. A source within an organized crime syndicate or a lower-level law enforcement agency faces serious hurdles in order to contact and confer with a journalist. A whistleblower within a top-level defense

contractor such as Booz Allen Hamilton, the NSA proper, or the White House would face near-insurmountable barriers to secure communication.

The importance of private communications between a journalist and a source is clearly evident in the reporting of *Washington Post* reporters Bob Woodward and Carl Bernstein. Woodward and Bernstein (1994, p. 8) dedicated their seminal piece of journalistic detective work, *All the President's Men*, “to the President's other men and women-in the White House and elsewhere-who took risks to provide us with confidential information. Without them there would have been no Watergate story told by the Washington Post.” Woodward went to great lengths to preserve the anonymity of the key Watergate source, Deep Throat. Woodward would signal a meeting by moving a flower pot with a red flag on his apartment balcony, and the two met in the bowels of a parking garage in Rosslyn, Virginia (Woodward & Bernstein, 1994). Such protective measures are primitive compared to the current difficulties in evading electronic surveillance and guaranteeing security and anonymity to a source.

Long before their fateful Hong Kong rendezvous, Snowden attempted to communicate the gravity of the NSA leaks to Greenwald; Greenwald, however, was lax about encrypting his email, and procrastinated, despite Snowden's continued urging (Greenwald, 2014a). Snowden refused to reveal any meaningful information without a secure method of communication, and Greenwald was reluctant to invest the time in encrypting his email. Eventually, Greenwald encrypted his email (using a video tutorial Snowden made for him), and the two were able to communicate and set up a meeting (Greenwald, 2014a). More than a potted plant and a parking garage were required; Snowden gave Greenwald explicit instructions to purchase an air-gapped computer (a

computer that would never be connected to the Internet, to ensure that it could not be hacked and compromised), covered himself and his laptop with a sheet anytime he entered his password, insisted that Greenwald and the other journalists either remove the batteries from the smartphones or place them in the refrigerator, and disconnected the landline speaker phone in his hotel room, to prevent eavesdropping (Greenwald, 2014).

These surveillance countermeasures, which establishment figures derided in the popular press as symptomatic of Snowden's paranoia are actually the very thing that preserved Snowden's life, and allowed him to leak the critical documents (Greenwald, 2014a). As a result of his government work, Snowden was aware of the necessity for strong operational security, and if he had not taken measures such as email encryption, may have been apprehended or silenced by the United States before establishing a relationship with Greenwald and Poitras (Greenwald, 2014a). In the digital, fourth dimensional Panopticon, perfect paranoia is perfect awareness. And awareness is the first step toward effective defense.

What this means for every person is that now, more than ever, issues of privacy and security are central to existence. Technology and big data will shape the future of commerce, communication, science, and society. The same technical advances that made the internet, World Wide Web, and cell phones possible have also made mass surveillance possible. However, there is hope. Hope in the very real techniques that journalists, activists, and the average citizen alike can use to both thwart corporate tracking and make illegal, unconstitutional mass surveillance untenable. Together, every human on Earth can heed Edward Snowden's warning and fight the future.

Whistleblowers

Whistleblowing is the act of a man or woman who, “believing that the public interest overrides the interest of the organization he serves, publicly 'blows the whistle' if the organization is involved in corrupt, illegal, fraudulent, or harmful activity” (Nader, Petkas, & Blackwell, 1972). Whistleblowers act out of a sense of conscience and public duty, and are on the front line of defending citizens from arbitrary abuse at the hands of insidious, powerful, institutions (Nader, Petkas, & Blackwell, 1972). As Nader, Petkas, and Blackwell (1972, p. 4) note, within the poisonous atmosphere of a hierarchical organization, dissent is so restricted that “common candor requires uncommon courage.” The candor of whistleblowers serves the greater needs of a democratic society, namely the right of citizens to be informed, speak freely, and meaningfully participate in important public decisions (Nader, Petkas, & Blackwell, 1972; Greenwald, 2014a). In service to the precepts of democratic society, whistleblowers act as the “last line of defense ordinary citizens have against the denial of their rights and the destruction of their interests by secretive and powerful institutions” (Nader, Petkas, & Blackwell, 1972, p. 7).

Edward Snowden is the quintessential whistleblower. A national security insider with both CIA and NSA credentials, Edward Snowden put public interest ahead of his lucrative career and publicly exposed wrongdoing. In exposing the U.S. government's mass surveillance state and the systematic abuses upon which it was predicated, Edward Snowden served the greater needs of democratic society, informing citizens of not just the United States, but also the world, and allowing all of them to meaningfully participate in the debate regarding mass surveillance.

Journalists and Sources

Freedom of speech is not just one of the fundamental rights: it is the fundamental right, enshrined in the First Amendment of the United States Constitution.

> Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances. (U.S. Const. Amend. I)

The current, ever-expanding mass surveillance state threatens every promise of the First Amendment, while violating every protection of the Fourth Amendment. The government of the United States, and in particular, the National Security Agency, now possess the most extensive, sweeping SIGINT collection powers known to humanity. This surveillance apparatus, which exists to serve whoever holds power, regardless of his or her political affiliations, morals, and scruples, unchecked by any meaningful oversight, encroaches upon First Amendment freedoms. Chilling effects stretch beyond what an individual is willing to type into a web search box: chilling effects extend to activists and journalists. If citizens are reluctant to assemble and investigative journalists are criminalized for working with whistleblowers, democracy is endangered.

The massive overreach of the NSA data collection programs endangers not just privacy, but freedom. The ability to monitor, categorize, and search at will places undue strength in the hands of whoever occupies a position of authority, and if such an individual has a reason to stifle the freedom of citizens to assemble or the functioning of the independent press, he or she will have the adequate tools to target dissenters. However, Tor, PGP encryption, VPNs and operating systems such as TAILS are

effective enough that the NSA considers them a serious threat to its ability to conduct surveillance, in particular mentioning Tor in internal presentation documents (Greenwald, 2014).

CHAPTER 5

TOOLS AND TECHNIQUES FOR PRIVACY AND SECURITY

This chapter is dedicated to a range of privacy and security tools. Different individuals will desire different levels of privacy and security; there is no one-size-fits-all approach. More advanced privacy and security measures require a necessary trade-off between convenience and efficacy, and as such there will be a range in use among a given population. When implementing a system of cyber-defense, an individual should first do a risk assessment: an analysis of what the individual perceives to be the greatest threat, and what steps to implement to maximize security (Schneier, 2015b). An individual's defense will form in response to the perceived threat. An individual will take different countermeasures in response to a common cybercriminal, as opposed to targeted surveillance from a powerful nation state with limitless resources (Schneier, 2015a).

The following tools are useful for a wide gamut of individuals, from the average citizen to the investigative journalist to the activist. As technology evolves, so will these tools, which is why it is important to keep in mind not just the tools themselves, but the underlying network of information transmission and surveillance to which they respond.

DuckDuckGo

DuckDuckGo is an Internet search engine that emphasizes protecting users' privacy, as well as circumventing the growing filter bubble. Unlike Google, which profiles every user and tailors search results based upon browsing history and IP address, DuckDuckGo deliberately shows all users the same search results for a given term. Users can easily set DuckDuckGo as their default search engine, on both desktop and

mobile devices.

Web Browser Extensions

A web browser, commonly referred to as a browser, is a software application for retrieving, presenting, and traversing information resources on the World Wide Web. A user's web browser identifies an information resource through a Uniform Resource Identifier (URI/URL) that may be a web page, image, video, or other piece of content such as a file system stored locally on the user's computer. The most popular web browsers are Firefox, Google Chrome, Safari, Opera, and Microsoft Edge. Web browsers reveal the following information to websites: user's operating system, which version of the operating system, and sometimes what other software the user is running on his or her desktop (Mitnick & Vamosi, 2017).

A web browser extension (also known as an add-on) is a plug-in that extends the functionality of a web browser. Browser extensions are used for improving a browser's user interface, security or accessibility, blocking advertisements, and various other features that affect the user's interaction with the web. There are many types of extensions that can be used to control various aspects of browsing privacy and mitigate threats. The Electronic Frontier Foundation has developed two critical web browser extensions for security and privacy: HTTPS Everywhere and Privacy Badger (Electronic Frontier Foundation 2017a; Electronic Frontier Foundation 2017b).

HTTPS Everywhere is a collaboration between the Tor Project and the Electronic Frontier Foundation; HTTPS Everywhere is a web browser extension that encrypts the user's traffic with many major websites, thus making web browsing more secure. According to the Electronic Frontier Foundation, many sites on the web offer limited

support for encryption over HTTPS, but make it difficult to use (Electronic Frontier Foundation, 2017a). Many websites default to unencrypted HTTP, or feature encrypted pages with links that return to the unencrypted site. HTTPS Everywhere fixes these weaknesses by rewriting requests to these sites to HTTPS (Electronic Frontier Foundation, 2017a).

Privacy Badger is a free browser extension that promotes a balanced approach to internet privacy between consumers and content providers by blocking advertisements and tracking cookies that do not respect the Do Not Track setting in a user's web browser. Privacy Badger automatically blocks advertisers that track users across multiple sites (Electronic Frontier Foundation, 2017c). When a user views a webpage, that webpage is often made up of content from several different sources. For example, when a user visits cnn.com, CNN will load the actual news article (which sits on one server), images (which may sit on another server), ads from an ad company, and the comments section from a different company that's been contracted to provide the service (Electronic Frontier Foundation, 2017c). Using a modified version of Adblock Plus, Privacy Badger keeps track of any third-party source that seems to be tracking the user across multiple sites, and once it detects them, activates a program telling the web browser not to load any more content from that source.

Privacy Badger is primarily a privacy tool, not an ad blocker (although as a by-product of its privacy focus, it often does block ads); the EFF's goal is to prevent non-consensual invasions of privacy (Electronic Frontier Foundation, 2017c). In order to target advertisements specifically, a web user should download a traditional ad blocking extension such as uBlock Origin.

Web users should also be aware of a tracking technique known as canvas fingerprinting. Canvas fingerprinting, works by instructing the user's Web browser to draw a hidden image; since each computer renders the image in a slightly different way, the images can be used to assign each user's device a unique identifying number (Angwin, 2014). Canvas fingerprinting is possible because every computer is slightly different, containing different typographical fonts, software, clock settings, and other distinct features. Computers automatically broadcast some of their attributes when they connect to the web. CanvasBlocker and Canvas Fingerprint Blocker are two extensions that attempt to prevent canvas fingerprinting. Privacy Badger also blocks canvas fingerprinting, if it is attempted by a third-party across multiple sites.

At the time of this writing, the Electronic Frontier Foundation (2017b) maintains a web tool called *Panopticlick*, which tests the safety of the user's web browser against various types of tracking. Panopticlick rates the browser based upon tests for ad blocking, invisible trackers, third-party trackers, and fingerprinting. Panopticlick is available at https://panopticlick.eff.org/

Tor

Tor is free software, and was originally developed in 2004 by the US Naval Research Laboratory, to enable military personnel to conduct searches without exposing their physical locations. The Tor network is a group of volunteer-operated servers that allow users to preserve their privacy and security on the Internet. Tor stands for “The Onion Router” and routes web users’ traffic through different nodes, like the many layers of an onion. The Tor network allows users the ability to conceal their location and usage from network surveillance and traffic analysis, thus circumventing

censorship and mass surveillance. Everyday people, journalists, law enforcement agents, whistleblowers, activists, business executives, and the U.S. military all use Tor (Mitnick & Vamosi, 2017).

When an individual uses Tor, the direct line between the user and the target website is obscured by additional nodes. Every ten seconds, the chain of nodes connecting the user to the target site changes, without disruption to the user. As a result, if someone were to try and conduct surveillance on the user by backtracking from the destination website, he or she would be unable to because the path is constantly changing. As a result, Tor can be very slow. The benefit, however, is privacy, as well as the ability to access a world of sites that are not ordinarily searchable. Known as the Dark Web, these sites do not end with the common .com extension, but instead with the .onion extension (Mitnick & Vamosi, 2017). Many of these sites are maintained by individuals residing in countries with heavy repression and censorship. More information about Tor is available at https://www.torproject.org/

Signal

Signal is free software developed by Open Whisper Systems. Signal is a VoIP system for mobile phones that provides true end-to-end encryption for both iPhone and Android.[7] Signal's main advantage is that encryption key management is handled only between the calling parties, not a third party (Mitnick & Vamosi, 2017). The only copies of the encryption keys are stored on the users' devices, which means that Open Whisper Systems does not have them, and thus cannot be legally compelled to turn over the encryption keys to law enforcement agencies.

Another advantage to Signal is that is uses perfect forward secrecy (PFS). PFS

is a system that uses a slightly different encryption key for every call, so in the event that the encryption key is compromised, future calls will remain relatively secure (Mitnick & Vamosi, 2017). With PFS, if an attacker compromises one key, it does not jeopardize all future communications. More information about Signal is available at https://www.whispersystems.org/

Email Encryption and Secure Drop

Another choice for encrypted communication is to use an open-source email client such as Thunderbird along with Enigmail. Thunderbird is compatible with Enigmail PGP encryption, and the average computer user can download the program and generate a unique encryption key within a few minutes.

After publishing his articles on the Snowden revelations, Greenwald left the *Guardian* and helped found *The Intercept*, which helpfully provides the encryption keys of every staff journalist in order to facilitate secure communication between potential sources and the journalists. *The Intercept* also implemented a *Secure Drop* server, which facilitates the anonymous submission of leaked documents and provides a guide for how to securely, privately, and anonymously leak documents (Lee, 2015). Secure Drop is considered an industry standard for investigative journalists working with whistleblowers, and is also the software of choice for *The Washington Post*. More information is available at https://securedrop.org/

CHAPTER 6

CRYPTOPARTY

To the rhetorical question of how journalists, activists, and average citizens alike protect the integrity of their thoughts, communications, affiliations, and plans in the face of such an overwhelming surveillance state, the part of the solution may be found in cryptoparties: public workshops that introduce the basics of practical cryptography to the general public. Cryptoparties are the result of a grassroots movement to educate individuals and promote privacy and anonymity; a typical cryptoparty is a nonpolitical event open to the public. The movement began in Australia in 2011, when an activist with the nom de guerre Asher Wolf organized the first cryptoparty, to instruct participants on the installation and use of Tor, PGP, and OTR (Poulsen, 2014).

Edward Snowden hosted a cryptoparty in Hawaii, before his fateful Hong Kong meeting with Glenn Greenwald, Laura Poitras, and Ewen MacAskill (Poulsen, 2014). After his initial email to Greenwald (under the pseudonym Cincinnatus, using his Lavabit email account), Snowden awaited a response, and it was during this period that he organized a cryptoparty in Hawaii; while Greenwald procrastinated in regard to encrypting his email, Snowden used this time to act locally and help approximately twenty people encrypt their email and download Tor (Poulsen, 2014; Greenwald, 2014). Snowden went as far as to solicit a guest appearance from Runa Sandvik, one of the key developers for the Tor project, and Sandvik obliged, appearing at the Hawaii cryptoparty and speaking alongside Snowden (Poulsen, 2014).[5] Sandvik opened with her presentation about Tor, Snowden followed with a tutorial on hard disk encryption using the now-defunct TrueCrypt, and then the two mutually fielded questions and

discussed how to set up a Tor relay. Today, cryptoparties are as important as ever, and their role in educating and protecting the public will grow in proportion to the continued expansion of the mass surveillance state and the militarization of the police.

The author of this paper hosted a cryptoparty on March 6th, 2017, as part of a research project on privacy and surveillance self-defense. Held at the Carbondale Public Library, the cryptoparty focused on educating the attendees on how corporate tracking and state surveillance operate. Then, after discussing different elements of privacy and surveillance, the author walked the attendees through surveillance self-defense techniques. For more information on the techniques, see chapter five of this research paper.

The reactions of the attendees were as enthusiastic as they were visceral. Upon learning that their emails, texts, and web browsing histories are as private as postcards, many expressed audible disgust. If the reactions of this group of ten are any indication, people do care about privacy. The problem is privacy education and awareness, or rather the pervasive lack thereof. For this reason, surveillance self-defense awareness, and particularly events such as cryptoparties, serve a vital public service.

CHAPTER 7

PRIVACY AND SECURITY IN THE AGE OF PRESIDENT DONALD J. TRUMP

The supporters of President Obama often defended his expansion of mass surveillance programs, offering to overlook the threats to civil liberties these expansions represented. The defense centered on a trust in the individual; mass surveillance is scary, but, the supporters argued, President Obama can be trusted. However, this support underscores the danger of turning a blind eye toward mass surveillance and the inherent and inevitable pernicious impact it has on civil liberties: it is not merely a matter of the current administration and president, but also all future presidents down the line. The apparatus of mass surveillance exists after the Obama presidency.

The danger of this trust is exemplified in the 2016 election of Donald J. Trump, who has now inherited the most extensive mass surveillance network in human history (Emmons, 2016). Within his first one hundred days, President Trump and his administration have ratcheted up attacks against privacy. In addition to increased Immigration and Customs Enforcement (ICE) raids and a travel ban against seven predominantly Muslim-majority countries, Trump's administration has also cracked down on government social media accounts, in particular any which post accurate, factual information relating to climate change. At U.S. borders, travelers have been forced to surrender social media accounts and unlock their phones (Lacambra, 2017).

On April 3, 2017, President Trump signed a bill repealing internet privacy rules that were established in October, 2016. Despite heavy opposition from the American people, Congress passed, and President Trump signed into law, a resolution that repeals Federal Communications Commission (FCC) rules that protected consumer

privacy from Internet service providers (ISPs) such as Comcast, AT&T, Verizon, and Time Warner Cable (Tummarello, 2017). As a result of this Republican effort to pass a Congressional Review Act resolution, ISPs can now legally sell customers' data (such as browsing histories) and use new, invasive ways to track consumers and deliver targeted advertisements (Tummarello, 2017). If the first one hundred days are any indication, the Presidency of Donald Trump will be one of antipathy toward civil rights, and the protections they afford.

CHAPTER 8

CONCLUSION

The nature of digital information and the networked world has enabled the greatest advances in communication, education, art, science, and entertainment since the invention of the printing press. However, with each new day the systems and technologies to track people and predict their behavior only expand. Corporations and governments track anyone and everyone. Privacy has never been in such grave danger.

The collection, storage, and analysis of data have enabled the expansion of the pervasive surveillance state. Journalists, whistleblowers, activists, and average citizens are all under attack. A democracy cannot thrive in an environment deprived of freedom of thought, information, and expression. The surveillance state chokes the light of freedom from such an environment, and democracy will suffer.

Democracy will thrive if the citizens of the world rise up and continue the struggle for freedom, which is predicated upon the protections of privacy. Privacy allows journalists to work with sources and publish information so citizens may be informed. Privacy allows whistleblowers the ability to perform a vital public service: sounding the alarm when those in power abuse power. Privacy allows activists and dissidents the ability to exercise their First Amendment rights. Privacy allows the average person to have a secure space to exist away from the harsh gaze of society and develop mentally, spiritually, and emotionally. The tools necessary to make mass surveillance untenable already exist. It is only a matter of spreading the word, and awakening every human being to the potential to protect and preserve the integrity of their digital self.

REFERENCES

Angwin, J. (2014, July 21). Meet the online tracking device that is virtually impossible to block. *ProPublica.* Retrieved from: https://www.propublica.org/article/meet-the-online-tracking-device-that-is-virtually-impossible-to-block

Assange, J., Appelbaum, J., Muller-Maguhn, A., & Zimmermann, J. (2012). *Cypherpunks: Freedom and the future of the internet*. New York, N.Y.: OR Books.

Bernstein, C. & Woodward, B. (1994). *All the president's men*. New York, N.Y.: Simon & Schuster.

Burrington, I. (2016). *Networks of New York: An illustrated field guide to urban internet infrastructure*. New York, N.Y.: Melville House.

Brunton, F. & Nissenbaum, H. (2015). *Obfuscation: A user's guide for privacy and protest*. Cambridge, MA: MIT Press.

Choudhury, N. (2015, August 4). The government is watching #BlackLivesMatter, and it's not okay. *American Civil Liberties Union, Speak Freely*. Retrieved from: https://www.aclu.org/blog/speak-freely/government-watching-blacklivesmatter-and-its-not-okay

Cox, J. (2017, February 14). Matt Mitchell is arming underserved communities with anti-surveillance tools. *Motherboard*. Retrieved from: https://motherboard.vice.com/en_us/article/matt-mitchell-is-arming-underserved-communities-with-anti-surveillance-tools

Electronic Frontier Foundation. (2017a). *HTTPS Everywhere*. [Web page]. Retrieved from: https://www.eff.org/https-everywhere

Electronic Frontier Foundation. (2017b). *Panopticlick*. [Web page]. Retrieved from https://panopticlick.eff.org/

Electronic Frontier Foundation. (2017c). *Privacy Badger*. [Web page]. Retrieved from https://www.eff.org/privacybadger

Emmons, A. (2016, November 11). Commander-in-chief Donald Trump will have terrifying powers. Thanks, Obama. *The Intercept*. Retrieved from: https://theintercept.com/2016/11/11/commander-in-chief-donald-trump-will-have-terrifying-powers-thanks-obama/

Emmons, A. (2017, January 13). Obama opens NSA's vast trove of warrantless data to entire intelligence community, just in time for Trump. *The Intercept*. Retrieved from: https://theintercept.com/2017/01/13/obama-opens-nsas-vast-trove-of-warrantless-data-to-entire-intelligence-community-just-in-time-for-trump/

Fallis, G. & Greenberg, R. (1998). *Be your own detective*. New York, N.Y.: M. Evans and Company, INC.

Foucault, M. (1979). *Discipline and punish: The birth of the prison*. (A. Sheridan, Trans.).New York, N.Y.: Vintage Books. (Original book published 1977)

Gage, B. (2014, November 11). What an uncensored letter to M.L.K. reveals. *The New York Times Magazine*. Retrieved from: https://www.nytimes.com/2014/11/16/magazine/what-an-uncensored-letter-to-mlk-reveals.html?_r=0

Goodman, A. & Moynihan, D. (2012). *The silenced majority: Stories of uprisings, occupations, resistance, and hope*. Chicago, IL: Haymarket Books.

Granick, J.St. (2017). *American spies: Modern surveillance, why you should care, and*

what to do about it. New York, N.Y.: Cambridge University Press.

Greenwald, G. (2014a). *No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state*. New York, N.Y.: Picador.

Greenwald, G. (2014b, October). *Glenn Greenwald: Why privacy matters* [Video file]. Retrieved from: https://www.ted.com/talks/glenn_greenwald_why_privacy_matters

Jeffries, A. (2015, December 11). The black community needs encryption. *Motherboard*. Retrieved from: https://motherboard.vice.com/en_us/article/the-black-community-needs-encryption

Joseph, G. (2015). Feds regularly monitored Black Lives Matter since Ferguson. *The Intercept*. Retrieved from: https://theintercept.com/2015/07/24/documents-show-department-homeland-security-monitoring-black-lives-matter-since-ferguson/

Kayyali, D. (2014, November 12). FBI's “suicide letter” to Dr. Martin Luther King, Jr., and the dangers of unchecked surveillance. *Electronic Frontier Foundation*. Retrieved from: https://www.eff.org/deeplinks/2014/11/fbis-suicide-letter-dr-martin-luther-king-jr-and-dangers-unchecked-surveillance

Lacambra, S. (2017, April 3). The Bill of Rights at the border: Fourth Amendment limits on searching your data and devices. *Electronic Frontier Foundation*. Retrieved from: https://www.eff.org/deeplinks/2017/04/bill-rights-border-fourth-amendment-limits-searching-your-data-and-devices

Lee, M. (2015). How to leak to the Intercept. *The Intercept*. Retrieved from https://theintercept.com/2015/01/28/how-to-leak-to-the-intercept/

Leopold, J. (2015, August 11). Emails show feds have monitored 'professional

protestor' DeRay Mckesson. *Vice News*. Retrieved from: https://news.vice.com/article/emails-show-feds-have-monitored-professional-protester-deray-mckesson

Manovich, L. (2001). *The language of new media*. Cambridge, M.A.: MIT Press.

Mitnick, K. & Vamosi, R. (2017). *The art of invisibility: The world's most famous hacker teaches you how to be safe in the age of big brother and big data*. New York, N.Y.: Little, Brown and Company.

Nader, R., Petkas, P.J., & Blackwell, K. (1972). *Whistleblowing: The report of the conference on professional responsibility*. New York, N.Y.: Grossman Publishers.

Orwell, G. (1950). *1984*. London, England: Penguin.

Postman, N. (2005). *Amusing ourselves to death: Public discourse in the age of show business*. New York, N.Y.: Penguin Books.

Poulsen, K. (2014, May 21). Snowden's first move against the NSA was a party in Hawaii. *Wired*. Retrieved from: https://www.wired.com/2014/05/snowden-cryptoparty/#slide-1

Reel, M. (2016, September 4). Eye in the sky: Can airplanes solve street crime? Baltimore is finding out. *Bloomberg Businessweek*, 50-57.

Richards, S., Hernandez, J. & MacDonald-Evoy, J. (2015). Cellphone surveillance used on Black Lives Matter protesters at fourth precinct in Minneapolis. *North Star Post*. Retrieved from: https://www.nstarpost.com/news/cellphone-surveillance-used-on-black-lives-matter-protesters-at-fourth-precinct-in-minneapolis/

Schneier, B. (2015a). *Data and Goliath: The hidden battles to collect your data and control your world*. New York, N.Y.: W.W. Norton & Company.

Schneier, B. (2015b). *Secrets and lies: Digital security in a networked world*. Indianapolis, IN; Wiley.

Solove, D.J. (2007). “I've got nothing to hide” and other misunderstandings of privacy. *San Diego Law Review*, *44*, 745-772.

Stallman, R.M. (2010). *Free software, free society: Selected essays of Richard M. Stallman*. Boston, MA.: SoHo Books.

Tummarello, K. (2017, April 3). Trump signs bill to roll back privacy rules into law. *Electronic Frontier Foundation*. Retrieved from: https://www.eff.org/deeplinks/2017/04/trump-signs-bill-roll-back-privacy-rules-law

United Nations (1948, December 10). *Universal declaration of human rights*. Retrieved March 18, 2017 from: http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf

U.S. Const. Amend. I

U.S. Const. Amend. IV

Ventura, J. & Russell, D. (2011). *63 documents the government doesn't want you to read*. New York, N.Y.: Skyhorse.

ENDNOTES

1. The Five Eyes, or FVEY, is an intelligence alliance comprising Australia, Canada, New Zealand, the United Kingdom, and the United States. The Five Eyes nations routinely share signals intelligence, or SIGINT, and monitor billions of private communications worldwide. The Five Eyes program represents one of the most comprehensive espionage alliances in history.

2. The printing press was invented around 1440, by Johannes Gutenberg. In the ensuing decades, millions of volumes were printed, ushering in a new age of mass communication. The invention of the printing press lead to vernacular Bibles (Bibles published in a language other than Latin, enabling common citizens to read and interpret the religious text), a development that contributed to the Protestant Reformation. The printing press, and the resultant information explosion, allowed art, literature, and scientific theories, to transcend geographic borders. The internet, and the world wide web, is the next iteration of this unprecedented shift in information creation and exchange.

3. Moore's Law is the observation that the number of transistors in a dense integrated circuit doubles approximately every two years. It is named after Gordon Moore, the co-founder of Fairchild Semiconductor and Intel, who first made the observation.

4. Stallman enumerated the four essential freedoms using zero-based numbering, in which the initial element of a sequence is assigned the index zero. Computers programming uses zero-based numbering.

5. Snowden initially contacted Sandvik regarding Tor exit relays; Snowden personally operated several Tor relays, including a 2 gbps server he nicknamed “TheSignal”, and

emailed Sandvik to request official Tor stickers, as an incentive to his NSA coworkers, whom Snowden was attempting to convince to run additional Tor relay nodes.

6. IMSI stands for International Mobile Subscriber Identity. An IMSI is used to identify the user of a cellular network and is a unique identification associated with all cellular networks.

7. VoIP, or Voice over Internet Protocol, is a technology that enables the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet. VoIP works even if the device lacks a native means of making a phone call.

VITA

Graduate School
Southern Illinois University

Nathaniel D. Fortmeyer

nathanfortmeyer@gmail.com

Southern Illinois University Carbondale
Bachelor of the Arts, Criminology and Criminal Justice, May 2011

Southern Illinois University Carbondale
Bachelor of the Arts, Cinema and Photography, May 2013

Special Honors and Awards:

- Photography Studies Award, Spring 2012
- Jeanne Hurley Simon Memorial Scholarship, Spring 2013
- David A. Gilmore Photography Award, Spring 2013

Research Paper Title: Surveillance Self-Defense: Privacy in the Post-9/11 Mass Surveillance State

Major Professor: Robert Spahr