Fall 2015

Surveillance and Privacy in the Digital Age: A Primer for Public Relations

Robert McMahon
Arcadia University, info@robertwmcmahon.com

Surveillance and Privacy in the Digital Age: A Primer for Public Relations

Arcadia University
M.A. Program in International Public Relations

Robert W. McMahon

A THESIS
IN
MEDIA AND COMMUNICATIONS

Presented to the Faculties of Arcadia University in Partial Fulfillment of the Requirements for the Degree of Master of Arts

December 2015

Acknowledgements

Finishing this thesis and completing the degree program has been a rewarding experience intertwined with challenges, intellectual effort and hard work. I would like to extend my thanks to a number of individuals who have been instrumental in helping me achieve this goal.

I would like to thank my thesis advisor, Dr. Michael D. Dwyer, for his guidance, support and expertise on the process and the material. His calm demeanor and methodical approach turned the initially unwieldy and intimidating task of writing this document into a thoughtful and manageable experience. I am grateful for his targeted suggestions, his deep knowledge of media theory and his genuine enthusiasm for the writing process.

I would also like to thank the professors I experienced during my coursework at Arcadia University. Each one supplied the foundational material necessary to complete this final piece of the degree requirement and the inspiration to keep going from semester to semester. Particularly aligned to the subject matter presented in this thesis, I would like to thank Media Studies professor Michael Dwyer, Ph.D., Communication Law and Ethics professor Karen Porter, Esq., Organizational Cultures professor Karl Horvath, Ph.D. and Crisis Communications professor Steve Ryan, M.S. I believe the following work represents an intersection of the subjects learned in their classes.

Finally, I would like to thank my wife, Beth, for her support, encouragement and sacrifice throughout my pursuit of this degree. I would not have achieved this goal without her boundless enthusiasm and praise. I would also like to thank my family and friends who offered encouragement and kept me motivated to do something that will likely change my life.

Table of Contents

Abstract

The notion that "Big Brother Is Watching" has been around for decades, it is an often-used catchphrase to describe surveillance or privacy infringements. The evolution of the Internet, cellular networks and the growth of high speed connections worldwide has allowed an endless supply of devices to connect to this global network and produce an infinite supply of very specific, personal data. Without question these technological advancements have revolutionized industries and enhanced lives. However, the opportunity for "Big Brother" to watch has similarly evolved at a rapid pace. Not only is "Big Brother" watching, but he is also doing things with the information he is seeing. The political and cultural implications of these often-secretive activities have only recently started to become a topic of discussion in the general media. This paper will explore some theories of surveillance and privacy that inform our understanding of the subject even today, identify the entities that represent "Big Brother" in the digital age and highlight some recent examples of their activities. Finally, this paper will provide some answers to questions for consideration about this topic, specifically within the discipline of Public Relations.

Keywords: Surveillance, privacy, sousveillance, public relations, big-data, data-self, digital Panopticon, digital enclosure

"*Arguing that you don't care about privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say*."
Edward Snowden - @Snowden – October 12, 2015

Introduction

Picture a typical day for a typical American; let's call him Joe. Joe wakes up and gets started on his day. He dresses, puts on his smart watch[1], which will monitor how many steps he takes, his heart rate and determines if he is running, walking or cycling. Checking the weather on his smartphone[2] and the traffic report he hops into his car which is equipped with an EZPass transponder[3] and a gadget that monitors his driving habits so he can obtain, perhaps, a lower auto insurance bill. His smartphone is in constant contact with his wireless carrier, reporting where it is in the network. The GPS chip in the phone lets Google know where his favorite stops are, where he lives and where he works and the time between those destinations. He stops at the local Starbucks and purchases a latte with their mobile app[4] and that data is uploaded into their customer relationship management software. He is rewarded with another gold star and the promise of a free drink on his next visit. Arriving at work Joe swipes a badge to enter the building and logs onto his computer. Throughout the day the work he does on the computer is monitored and stored by his employer. Leaving for the day, Joe takes the fast route home, the toll road, and zooms through the tollbooth where the fee is deducted from his EZPass account. Multiple cameras along the way observed him and, since it was time for the local evening news traffic report, so did a few million viewers. Sensing his arrival home, his thermostat clicks on and sets itself to the appropriate temperature. He picks up a package left by UPS from his last

[1] Sales of this device have risen 457% from 2014 to 2015 according to Forbes
[2] Over 2 billion worldwide predicted for 2016
[3] Over 28 million EZPass transponders are in use today
[4] Over 12 million transactions monthly using the app

Amazon purchase using his American Express card and heads inside. After dinner and some chores he walks the dog while listening to a classic rock music stream from an online service. Back home he turns on the computer and does a little Internet surfing, a news site here and there, checks in on some Facebook friends, Google searches the latest model handgun, reads some reviews and leaves a comment. He looks up information about a rash he has by visiting some popular medical websites. After a while he watches some pornography clips to take his mind off that rash and heads to bed where he tells his smartphone to wake him up at six.

What do we know about Joe? As a friend or neighbor, maybe some of these details. But more shocking is what the government knows and what the marketing and advertising industry knows. In the case of the government, it knows everything. By everything, I mean everything. Either by direct and required access such as vehicle registration or driving license information or by more subversive and invisible ways such as obtaining a copy of everything Joe did over the Internet that day by directly taping into the major Internet backbone cables or collecting metadata[5] about his cell phone use. In the case of marketers, they know an awful lot and they are striving to learn more. They are also trying to connect together disparate bits and bytes of information. Through the use of web browser tracking mechanisms like cookies and beacons, marketers are able to collect a vast assortment of data about Joe and what he searches for and looks at on the Internet. This data is used to serve Joe specifically targeted advertising through his web browser and is further used to build a profile about Joe, his interests, opinions and even his physical location.

Another question to ask is what does Joe want us to know about him? In some instances Joe has voluntarily and willingly volunteered some of his information. He wears that smart

[5] Metadata is data about data. In the case of cell phones, it is a listing of the cell phone number, the location, dates, times and recipients of communications and other uniquely identifiable information.

watch because he wants to improve his fitness and his health and the watch motivates him to make those improvements. He chooses the insurance premium-reducing device with the understanding that it is monitoring his driving habits and if he behaves within accepted norms, he will be rewarded with a lower bill. He uses the Starbucks app because he loves the coffee and the occasional bonuses he is rewarded with by using the app. It is likely he talked to a buddy about his handgun interest, perhaps even went shooting with that buddy at the local range, but he did not ask advertisers to flood websites he visits with advertisements for guns. He told his doctor about that rash but, he did not tell his sister and he did not tell a credit-reporting agency. He knows he is telling his cellular provider who he calls and when because he receives a bill each month detailing those calls, it is likely he does not know his cellular provider gave that same information to his government. He may understand he is tacitly telling his Internet service provider about his web surfing habits, but he did not tell his employer about that pornography clip he viewed the night before.

Joe lives inside what will be described later as the "digital enclosure" and has, knowingly or unknowingly, been creating his "data self" or his online personality, complete with strengths, weaknesses and quirks, just like his actual personality. These concepts are relatively new and are born out of the digital age. This data self, living inside of the digital enclosure exists in a much larger structure known as the surveillance state. The actual self is capable of deciding who knows what, when they know it and often thrives in privacy. The data self does not live in an environment that permits such a filter to the recipients of information. The digital enclosure is not necessarily warm and secure like your house, but full of holes, leaks and windows.

This paper will investigate some of the theoretical underpinnings of the surveillance state, the infrastructure behind it and the evolution of its hegemonic prevalence in the digital age. It

will highlight some cases in the government and commercial sectors where the data self collides with questions about privacy, security, politics and culture. It will identify who is looking through the windows into your digital enclosure and what are they doing with that information. Finally, this paper will recommend some considerations for public relations practitioners when delving into this world by asking the questions, "What do we do with Joe and the information he is creating or leaving behind? What can we do? What should we do?"

Overview of Theories and Infrastructure

In this section, I provide an overview of some foundational theories of privacy and surveillance and how the digital age intersects with those theories and spawned new ones. It is organized into a framework of five sections that identify philosophers on the subject, implications of the digital age, sousveillance, privacy policy considerations and a term defining the era today.

Influential Philosophers

Some of the most frequently cited philosophers on the subject of privacy and surveillance are Jeremy Bentham and Michel Foucault. What have been described in the writings of Bentham and Foucault are the theories behind, and the tactics used to perform, surveillance. While politics, society and technology have evolved from their time through today, their core concepts remain applicable.

Jeremy Bentham, a philosopher and jurist, is considered the founder of utilitarianism and influenced the development of welfarism. Born in England in 1748, he was considered a child prodigy. He was sent to The Queen's College, Oxford, at the age of twelve. He earned a bachelor's degree and master's degree and trained as a lawyer. He became an authority on the philosophy of law and developed a reputation as a political radical. He advocated for the separation of church and state, legal and social reform and created a prison design called the Panopticon.

Before the technological times of today, surveillance was personal in nature. One person watching another, perhaps by hiding behind a tree or peering through a window or putting a glass next to a door to hear what was happening on the other side. This type of surveillance was secretive by design and the subject did not know he was being monitored. There were other

instances of surveillance that were not done in secret but rather quite openly. For example, Bentham's architectural design for prisons, the Panopticon, a structure that would allow one person to watch many others. Bentham's Panopticon design involved a circular building with a tower situated in the middle. The cells of the prison would face towards the tower and an observer would staff the tower. In this instance the intended subjects, the prisoners, never know if they are being watched or when they are being watched as they could not see inside the central tower. Thus, the prisoners are theoretically in a state of constant surveillance. Bentham felt this structure had application beyond prisons when he wrote,

> No matter how different, or even opposite the purpose: whether it be that of punishing the incorrigible, guarding the insane, reforming the vicious, confining the suspected, employing the idle, maintaining the helpless, curring (sic) the sick, instructing the willing in any branch of industry, or training the rising race in the path of education: in a word, whether it be applied to the purposes of perpetual prisons in the room of death, or prisons for confinement before trial, or penitentiary-houses, or houses of correction, or work-houses, or manufactories, or mad-houses, or hospitals, or schools. (Bentham, 1787)

As he foresaw the application of his design to other purposes, he also spoke of a vision for continuous observation and the application of power by the "establishment." The establishment could be an industry, governmental authority or education. Any sort of entity that held normative power over others would benefit from his vision as he articulated,

> It is obvious that, in all these instances, the more constantly the persons to be inspected are under the eyes of the persons who should inspect them, the more perfectly will the purpose of the establishment have been attained. Ideal

> perfection, if that were the object, would require that each person should actually be in that predicament, during every instant of time. (Bentham, 1787)

Recognizing the difficulty of having everyone under surveillance all of the time, he understood the importance of a population to think or believe they were under surveillance all of the time when he said, "This being impossible, the next thing to be wished for is, that, at every instant, seeing reason to believe as much, and not being able to satisfy himself to the contrary, he should *conceive* himself to be so." (Bentham, 1787) The notion that a population thinks they are always being watched is important when modern technology is applied. The results are interesting and not always as expected. In some cases, when the goal of this belief is to force a particular population into a certain desired behavior, an undesired behavior or resistance is spawned. In other cases a resignation or surrendering of personal rights or privacy prevail. Some examples will follow throughout this paper.

Michel Foucault, also a philosopher, built on Bentham's panoptic schema and applied it to other institutions. Born in 1926 in France, he was educated at the prestigious Lycée Henri-IV and the École Normale Supérieure, where his interest in philosophy was born. Louis Althusser, Jean Hypolite, Immanuel Kant and Karl Marx influenced him and Althusser even tutored him during his time at the École Normale Supérieure. His doctoral thesis submitted to the University of Paris was entitled, "*Madness and Insanity: History of Madness in the Classical Age,"* was a study of madness versus mental illness as a social construct. He went on to write about power, knowledge and control through societal institutions over the course of his career.

The key concept of Bentham's work, a person conceiving he is being watched even when he may not be, is expanded upon by Foucault when he considers power and the application thereof when he says, "He who is subjected to a field of visibility, and who knows it, assumes

responsibility for the constraints of power; he makes them play spontaneously upon himself; he inscribes in himself the power relation in which he simultaneously plays both roles; he becomes the principle of his own subjection." (Foucault, 1977) His concept is the subject of surveillance, because he knows he is being watched, will take care to police himself. Ultimately the subject will internalize the notions of power, monitor himself and conform from within the body.

Going beyond the architectural design created by Bentham, Foucault identifies the application of power over bodies when he outlines the activities of a town towards the end of the seventeenth century, which is faced with the plague. Desperate to control the spread of the disease, the townspeople are secured within their homes, locked in not from the inside, but the outside. Surveillance is applied as he describes in this scene, "Each street is placed under the authority of a syndic, who keeps it under surveillance; if he leaves the street, he will be condemned to death." Unlike the Panopticon, which is resource conservative, this particular event was quite the opposite. "Inspection functions ceaselessly. The gaze is alert everywhere: 'A considerable body of militia, commanded by good officers and men of substance', guards at the gates, at the town hall and in every quarter to ensure the prompt obedience of the people and the most absolute authority of the magistrates." "This surveillance is based on a system of permanent registration: reports from the syndics to the intendants, from the intendants to the magistrates or mayor." (Foucault, 1977) In this case, the subjects know they are being watched and when they are being watched. There is also no shortage of resources applied to this constant state of monitoring.

Foucault recognized the efficiencies of the Panopticon and application of it in a broader scope, "It is polyvalent in its applications; it serves to reform prisoners, but also to treat patients, to instruct schoolchildren, to confine the insane, to supervise workers, to put beggars and idlers

to work." (Foucault, 1977) Further, "Whenever one is dealing with a multiplicity of individuals on whom a task or a particular form of behaviour must be imposed, the panoptic schema may be used." (Foucault, 1977) He describes the benefits of this schema,

> In each of its applications, it makes it possible to perfect the exercise of power. It does this in several ways: because it can reduce the number of those who exercise it, while increasing the number of those on whom it is exercised. Because it is possible to intervene at any moment and because the constant pressure acts even before the offences, mistakes or crimes have been committed. Because, in these conditions, its strength is that it never intervenes, it is exercised spontaneously and without noise, it constitutes a mechanism whose effects follow from one another. Because, without any physical instrument other than architecture and geometry, it acts directly on individuals; it gives 'power of mind over mind'. The panoptic schema makes any apparatus of power more intense: it assures its economy (in material, in personnel, in time); it assures its efficacity by its preventative character, its continuous functioning and its automatic mechanisms." (Foucault, 1977)

In short, the panoptic schema is about the assertion of power over and in individuals. The goals are efficiency, continuous function and automation. These goals will appear in current day practice throughout examples in this paper. Vital and essential to the assertion of power over individuals, there is also the notion that over time individuals will assert power over themselves or self govern, in an effort to fit into norms created by the establishment behind the schema.

Surveillance in the Digital Age

What evolved from these seventeenth century examples are the tactics of surveillance. What once required an architectural structure is now done virtually by computers. What once required a human being to be on the street in front of your home now only requires a software program and an analyst in a bunker far away. What was once considered necessary only in certain, specific, circumstances like monitoring a terrorist or solving a crime, has now gained favor for nearly all circumstances and all people. Privacy and protection against unlawful search and seizure, once assumed as a given right and protected under the Fourth Amendment of the U.S. Constitution has nearly disappeared as electronic surveillance of the citizenry has expanded to include everyone within the country regardless of suspicion or court ordered warrant.

I suggest personal privacy, once fairly easy to maintain, has become increasingly more difficult in this digital age. For marketers, advertisers, data miners and corporations the activities of private citizens have become easily collected, categorized, commoditized, bought and sold. However, the private citizen rarely understands who or what is collecting their information and what is being done with that information. There is a notion that this asymmetrical sharing of information between consumers and marketers is acceptable because the consumer is benefiting from some sort of discount, convenience or customization of their digital life. Marketers feel this is a tradeoff that consumers are willing to make but a recent study found otherwise. "To the contrary, the survey reveals most Americans do not believe that 'data for discounts' is a square deal. The findings also suggest, in contrast to other academics' claims, that Americans' willingness to provide personal information to marketers cannot be explained by the public's poor knowledge of the ins and outs of digital commerce." (Turrow, Hennessy, & Draper, The Tradeoff Fallacy: How Marketers are Misrepresenting American Consumers and Opening Them

Up to Exploitation, 2015) The study found a different reason behind the "data for discounts" trope. In a word, resignation,

> Our findings, instead, support a new explanation: a majority of Americans are resigned to giving up their data—and that is why many appear to be engaging in tradeoffs. Resignation occurs when a person believes an undesirable outcome is inevitable and feels powerless to stop it. Rather than feeling able to make choices, Americans believe it is futile to manage what companies can learn about them. Our study reveals that more than half do not want to lose control over their information but also believe this loss of control has already happened." (Turrow, Hennessy, & Draper, The Tradeoff Fallacy: How Marketers are Misrepresenting American Consumers and Opening Them Up to Exploitation, 2015)

This belief that control has already been lost is a powerful notion, one that almost tacitly gives permission to continue the "data for discounts" program.

Looking further into our connected lives, Mark Andrejevic is a professor and chair of media studies at Pomona College, Honorary Research Associate Professor in the Centre for Critical and Cultural Studies at the University of Queensland and writes about surveillance in the interactive era. His work describes a "digital enclosure" that we live inside. He defines this enclosure as,

> …the creation of an interactive realm wherein every action and transaction generates information about itself. Although the term implies a physical space, the same characteristics can apply to virtual spaces. The Internet, for example, provides the paradigmatic example of a virtual digital enclosure-one in which every virtual 'move' has the potential to leave a digital trace or record of itself.

> When we surf the Internet, for example, Internet browsers can gather information about the paths we take-the sites we've visited and the clickstreams that take us from one site to the next. When we purchase items online, we leave detailed records of our transactions. Even our search requests are logged and preserved in the database memories of search engines. (Andrejevic, 2007)

This digital enclosure has ever expanding components. Consider the things that are connecting to the Internet today; the computer, the smartphone, the tablet and your refrigerator. There is a growth of interest in the "smart home" where everything from lights, music, thermostats, door locks and security cameras are connected to the Internet, streaming an endless supply of data about your status, location and activities. Much of this data is stored, often by third parties, categorized and sold. It can be searched and sorted to identify groups of people based on their digital activities and, as we will see later, individuals can even be identified for targeted advertising or other activities. The digital enclosure is only getting larger and more deeply imbedded in our day-to-day life as we desire more conveniences and comforts.

If the digital enclosure were like a house, then that house would likely have at least one resident with a personality. In addition to our actual personalities, a new theory of human identity has emerged, the "data self," and it is created within Andrejevic's digital enclosure. "Ultimately, consumers help to constitute themselves as entities to be marketed to through repeated building of the self (what I call a 'data self') from the totality of their digital data transactions." (Fernback, 2007) This "data self" is painting a picture that is a valuable tool for the advertising and marketing industries, whether the subject wants that picture painted or not. It is through the use of browser cookies, GPS chips in mobile devices, social media postings and product reviews that this data self is built.

Over time, the digital breadcrumbs we leave are collected, connected with other breadcrumbs and each subject of this surveillance is categorized, either as a "target" or "waste" for advertisements

> Marketers are increasingly using databases to determine whether to consider particular Americans to be targets or waste. Those considered waste are ignored or shunted to other products the marketers deem more relevant to their tastes or income. Those considered targets are further evaluated in the light of the information that companies store and trade about their demographic profiles, beliefs, and lifestyles. (Turrow, The Daily You: How the New Advertising Industry is Defining Your Identity and Your Worth, 2011)

What naturally evolves from this categorization of the subject is, as Turrow suggests, "…narrowed options and social discrimination…" (Turrow, The Daily You: How the New Advertising Industry is Defining Your Identity and Your Worth, 2011). This is an interesting side effect that is counter to the general notion that the Internet is a tool that democratizes everything for everyone and gives all people an equal voice.

Monitor Thyself

It is important to consider some types of surveillance as something desired and invited in by the residents of the digital enclosure. The terms "big data" and "analytics" were born out of our desire to monitor, understand, improve, predict or prevent behaviors. For example, consider the growth of wearable technology to help monitor and improve fitness. Through the application of sousveillance, a person can wear a device to track, collect and analyze a range of biologic data; steps taken, heart rate, sleeping cycles, in an effort to govern the self. Often this data is

stored “in the cloud” where it may be shared with a physician located a town away in an effort to improve and optimize health.

Another example involves current day law enforcement agencies. We are starting to ask our police officers to engage in sousveillance by wearing body cameras to record their activities, as well as those with whom they encounter, in an attempt to prevent unnecessary aggression or violence or to provide supporting evidence if that aggression was necessary.

In the workplace, keystroke loggers monitor the activity and output of workers so managers can make improvements; identify problems and reward or correct workers. We use big data to optimize supply chain networks, airline routes and make predictions about elections or the weather. We employ Radio Frequency ID (RFID) chips to track objects like our cell phones, NFL football players and shipping containers. Again, all of these things are desired by groups of citizens, not necessarily forced on them or even done in secret.

Telematics, an industry solely dedicated to monitoring worker activity continues to find new areas to grow. Delivery and logistics company United Parcel Service (UPS) is a readily identifiable user of this technology.

> Telematics is a neologism coined from two other neologisms — telecommunications and informatics — to describe technologies that wirelessly transmit data from remote sensors and GPS devices to computers for analysis. The telematics system that now governs the working life of a driver for UPS includes handheld DIADs, or delivery-information acquisition devices, as well as more than 200 sensors on each delivery truck that track everything from backup speeds to stop times to seat-belt use. When a driver stops and scans a package for delivery, the system records the time and location; it records these details again

> when a customer signs for the package. Much of this information flows to a supervisor in real time. (Kaplan, 2015)

Because of this real time flow of information, and the delivery driver's knowledge that data is being collected, drivers participate in the self-governing behavior that Bentham and Foucault envisioned. However, it does come at a price in terms of safety and overall job satisfaction. One UPS driver put it eloquently, "People get intimidated and they work faster. It's like when they whip animals. But this is a mental whip." (Kaplan, 2015) An unintended side effect of this monitoring is the creative use of shortcuts or tricks to provide false data to the system. Examples include; intentionally not delivering packages in order to save time, keeping the seatbelt secured, even when it is not being worn, to indicate to the sensors that it is in use.

Perhaps subconsciously channeling Foucault, a transportation industry consultant explained the core function of telematics, "The important thing is where the power lies. Drivers might not be happy being measured, but in the end they will yield." (Kaplan, 2015) Yield, or self-police like a prisoner in the Panopticon.

The consumption of media and goods also shows the somewhat voluntary nature that many will enter Andrejevic's "digital enclosure." The explosive growth of online music streaming via platforms like Spotify and Pandora allow users to create customized, personal, radio stations. Over time the platforms will also suggest other artists and songs based on the user providing data about their particular listening habits. Video streaming services like Hulu move traditional television viewing out of the living room and place it anywhere there is a broadband connection. In addition to the flexibility of viewing location, viewers are no longer bound to a set schedule of time. Programs can be viewed at anytime, a phenomenon known as time shifting. The convenience of whenever, wherever, is a powerful reason people will engage in this service.

However, logging into those services provides for the opportunity to collect information on tastes, habits, location and views. Millions choose to use online shopping portals like Amazon to purchase goods. While there is plenty of data collection going on through those transactions, the convenience of shopping from home and the potential for cost savings is a large draw to the service. A type of community is developed as the shopper has the opportunity to read reviews of a product by other shoppers, create their own reviews, evaluate the number of "stars" assigned to that product and make that calculation, "if others like it, then I will too."

Privacy Considerations

Part of the surveillance infrastructure goes beyond the fiber optic cables under the ocean and computers in a darkened room, but is built into privacy policy. Perceptions and definitions of privacy have evolved over time, but a recent study found a group of key terms that American's consider when they think of privacy. "Among all of the themes referenced in the open-ended responses to the online survey, security, safety and protection was the most frequently-referenced category." (Pew Research Center, 2014) Other top ranking key words included; personal, secret, hidden, rights, let alone and fourth amendment collectively totaling 47% of the responses.

As more and more activities go online, industries and businesses are giving consideration to their privacy policies. The privacy policy is a statement of what is collected, how it is collected and what is done with that information when you use that online service or interact with that website. One study found that publication of a privacy policy inherently meant that the users privacy was protected. "62% of respondents to a survey believed (incorrectly) that the existence of a privacy policy implied that a site could not share their personal information without permission, which suggests that simply posting a policy that consumers do not read may

lead to misplaced feelings of being protected." (Acquisti, Brandimarte, & Loewenstein, 2015) At the same time, "Beyond social networking sites, Americans express a broader loss of control over the way their personal data is managed by companies. Fully 91% of adults "agree" or "strongly agree" that "consumers have lost control over how personal information is collected and used by companies." (Pew Research Center, 2014) These two studies show the data self is confused and frustrated with the manipulation of privacy online.

Further adding to the confusion, a default setting is often highlighted at the time a choice of agreement is being made. The default setting is suggesting a normative behavior. "Sticking to default settings is convenient, and people often interpret default settings as implicit recommendations. Thus, it is not surprising that default settings for one's profile's visibility on social networks, or the existence of opt-in or opt-out privacy policies on websites, affect individuals' privacy behavior." (Acquisti, Brandimarte, & Loewenstein, 2015) In some instances the user is presented with the opportunity to make a decision, to "agree" to the policy and be permitted to use the service or "disagree" and be directed away from the site. Depending on the importance of the site to the user, this decision is really not a decision as much as a resignation of privacy in that instance.

The Digital Panopticon

Considering the historical theories covered earlier, the brief look at the infrastructure of surveillance, instances of desired surveillance and the question of privacy in this online age, I propose we live in a digital Panopticon today. As Foucault suggested earlier, goals of efficiency, automation and continuous function are in play now more than ever. Faster and more powerful computing systems and the growth of analytics software has seen to efficiency and automation. We are creating and using more and more devices that feed the goal of continuous observation.

Like the prisoner in Bentham's panoptic prison, we do not know who is watching us but we do know we are being watched and, for the most part, we have given up or resigned ourselves to this state of affairs.

The case studies in the next section will identify two broad categories of participants in the panoptic schema and some specific events that illuminate the current state of affairs in surveillance and privacy. The case studies will also indicate how these topics are becoming more intertwined in the national, even global, discourse and creating opportunities for Public Relations professionals involvement.

Case Studies

The purpose of this section is to identify some examples of surveillance and privacy infringements through the optics of their political and cultural implications. Four case studies will highlight specific activities, companies and power structures that the connected citizen has likely encountered, willingly or unwillingly, in this digital era.

Broadly speaking, I believe there are two categories of participants in the digital Panopticon, the government and the commercial sector. The following case studies point out just some of the impact each has on the digital enclosure and the data self, residing inside.

Facebook

It would also be difficult to have a discussion about privacy without talking about the largest social media platform on the planet. With over a billion users worldwide, Facebook is credited for being a great tool to stay in touch with friends, family and corporations. It also receives criticisms for an opaque and ever changing privacy policy. While the other case studies ahead will cover events that are historical in nature or currently ongoing, there is recent information about Facebook that points to a potential future impact of the data self's online activity in the United States.

In 2010 Facebook purchased a company call Friendster as well as the intellectual property of that company. In August 2015, Facebook was granted a patent on one item of that intellectual property which suggests a future plan for social media giant and, more importantly an interesting impact to their users. The patent, for authenticating users of Facebook, also suggests another use,

> When an individual applies for a loan, the lender examines the credit ratings of members of the individual's social network who are connected to the individual

> through authorized nodes. If the average credit rating of these members is at least a minimum credit score, the lender continues to process the loan application. Otherwise, the loan application is rejected. (Kokalitcheva, 2015)

To simplify, if a Facebook user is applying for a car loan, the lender can examine that user's social network, their friends, to decide if the loan seeker is a qualified risk. Under this model, your friends could have a decidedly negative, or positive, impact on an actual, practical and meaningful life event. Current laws governing lending practices in the United States prevent this type of activity. However, laws in other countries do not prevent this from happening today.

For potential borrowers who have marginal or non-existent credit history, companies like Lenddo offer the use of social media participation as a lending decision. Operating in Columbia, Mexico and the Philippines, their website touts the benefit of the service, "With Lenddo, your customers can use their social networks such as Facebook, Linkedin, Google, Yahoo and Twitter to prove their identity and creditworthiness." (Lenddo, 2015) Pointing towards the accuracy of this tool, Lenddo CEO Jeff Stewart said, "It turns out humans are really good at knowing who is trustworthy and reliable in their community. What's new is that we're now able to measure through massive computing power." (Lobosco, 2013) Siva Viswanathan, a professor of business at the University of Maryland, examined the use of social connections to augment data typically used by lenders such as credit history and income. "Online was not perfect, but having the information did allow better [lending] decisions. The question remains how much better." (Chideya, 2015) This particular use of Facebook, and other social media platforms, raises an interesting thought. "It's not at all clear how to help people navigate a world where the seemingly trivial act of accepting a friend request can have life-altering financial implications." (Chideya, 2015) Considering the privacy policy of most companies is vague or hard to locate,

how will a platform like Facebook explain to our data self that our online friends may impact the actual self's ability to get a loan?

Apple Computer

One of the world's leading technology companies, Apple Computer, found itself in an awkward position after the leak and subsequent publication of a National Security Agency program called Prism. A slide in the PowerPoint presentation leak showed when Prism started to collect data from various United States technology companies. For example, Microsoft started the timeline in 2007, Google and Facebook in 2009, Skype in 2011 and Apple in 2012. For the average, law-abiding consumer, the revelation was likely very surprising. For Apple Computer, the damage to their reputation and public relations could have been substantial.

With a long history of innovation and growth into a financial powerhouse, Apple Computer passed a milestone in February 2015. The closing price of Apple stock on February 10, 2015, caused Apple's market value to become, "…the first-ever U.S. company to close at over $700 billion. That's nearly double the next largest company on the list, Exxon Mobil." (Fitzpatrick, 2015) While this milestone is impressive, the revelation that the company has a market value twice that of an oil/gas industry giant is important. This valuation is a testament to the influence Apple has on consumers worldwide and traditional financial behemoths can be replaced in terms of influence. It has been widely reported that Apple revolutionized the music industry, the mobile phone industry and the tablet computing industry. They have a legion of fans, fanatics even, around the world and, as a publicly traded company, shareholders to satisfy. Having the Apple name and logo appear on one of the first leaked documents was something the company could likely not ignore.

A few weeks after the report, Apple released a statement refuting their voluntary involvement,

> Two weeks ago, when technology companies were accused of indiscriminately sharing customer data with government agencies, Apple issued a clear response: "We first heard of the government's "Prism" program when news organizations asked us about it on June 6. We do not provide any government agency with direct access to our servers, and any government agency requesting customer content must get a court order. (Apple Computer, 2013)

Going further, they identified themselves as a company acutely interested in their customer's privacy,

> Apple has always placed a priority on protecting our customers' personal data, and we don't collect or maintain a mountain of personal details about our customers in the first place. There are certain categories of information which we do not provide to law enforcement or any other group because we choose not to retain it. (Apple Computer, 2013)

Apple also went on to describe certain features and functionalities that help protect their customer's privacy,

> For example, conversations which take place over iMessage and FaceTime are protected by end-to-end encryption so no one but the sender and receiver can see or read them. Apple cannot decrypt that data. Similarly, we do not store data related to customers' location, Map searches or Siri requests in any identifiable form. (Apple Computer, 2013)

As the national debate over privacy and surveillance continues, Apple has used this issue to further solidify their position on privacy and even use it as a public relations tactic to retain existing customers and obtain new ones. In 2014, a year after the NSA leaks, Apple was set to launch another iteration of it's revered iPhone, the iPhone 6. Always a widely anticipated event with extensive media coverage, enormous lines outside of Apple retail stores around the globe, one feature was picked up on in the press, encryption. Apple's newest iPhone 6, "…encrypts emails, photos and contacts based on a complex mathematical algorithm that uses a code created by, and unique to, the phone's user — and that Apple says it will not possess." (Sanger & Chen, 2014) Historically, the inner technological workings of a particular device were not typically found in the media. Certainly specific tech related magazines and websites may have an interest in the deep tech details, but the talk about encryption is something that was becoming more and more prevalent in the mainstream. It was also alarming to law enforcement when, on commenting about the new iPhone 6, the New York Times said, "The National Security Agency and the nation's law enforcement agencies have a different concern: that the smartphone is the first of a post-Snowden generation of equipment that will disrupt their investigative abilities." (Sanger & Chen, 2014) This notion positions a very specific consumer electronics device as a barrier to the "war on terror" or even as a tool for terrorists and criminals, which is at odds with the position Apple is taking on the device and privacy in general.

Aside from governmental forms of surveillance, Apple also comments and takes action on surveillance through their privacy policy as related to marketing activities. "'We don't build a profile based on your email content or web browsing habits to sell to advertisers,' chief executive Tim Cook wrote in a letter that introduced its privacy Web site last year. 'We don't 'monetize' the information you store on your iPhone or in iCloud.'" (Peterson & Tsukayama,

2015) CEO Cook further elaborated the philosophy of Apple when he spoke of other Silicon Valley tech companies, "They're gobbling up everything they can learn about you and trying to monetize it. We think that's wrong. And it's not the kind of company that Apple wants to be." (Peterson & Tsukayama, 2015) Industry observers are taking notice of Apple's position on privacy and how they are leveraging it to their advantage. One observer, Rich Mogull noted, "It's important for Apple because it's a business differentiator. The way they are built, they don't make any money through collecting personal information. That's the core of Google's business." (Peterson & Tsukayama, 2015) Noted professor Dr. Joseph Turrow, from the University of Pennsylvania, also pointed out, "I do think there is something to be made as a selling point around privacy." (Peterson & Tsukayama, 2015) The use of privacy policy by Apple is unique, in comparison to others in the field, because it is clear, open and quite opposite of the typical use of the policy, which is often obscure and elusive to even find out about.

Health Searches

There has been a notion around our use of the Internet, that if you are not paying for the product or service then you are the product. One area where this concept is visible involves the use of the Internet to look up health related information. While many would consider this information private, much like our medical records, any sort of privacy regulation, like the Federal Health Insurance Portability and Accountability Act (HIPAA), does not protect our use of the Internet.

Doctoral student Timothy Libert at the University of Pennsylvania conducted notable research on this very issue. His report, "Privacy Implications of Health Information Seeking on the Web," looked into what happens when the average, uninformed, citizen turns to the Internet seeking sensitive health information. "I used a search engine to identify 80,142 unique health-

related web pages by compiling responses to queries for 1,986 common diseases. This selection of pages represents what users are actually visiting, rather than a handful of specific health portals." (Libert, Privacy Implications of Health Information Seeking on the Web, 2015) Taking this vast amount of websites, he ran them through a specially created software program that would identify how many of those sites would collect and pass user information onto third parties. His findings highlight a huge privacy breach, "91% of pages were found to make requests to third parties. Investigation of URIs revealed that 70% of HTTP Referer strings contained information exposing specific conditions, treatments, and diseases. This presents a risk to users in the form of personal identification and blind discrimination." (Libert, Privacy Implications of Health Information Seeking on the Web, 2015) While some of the description here is technical, the message is clear, when a person searches out an ailment on the Internet, nine times out of ten other parties will know about it and that information is being collected.

The risk of personal identification and discrimination is further detailed in the study. The study also investigated what entities were receiving this information and the largest, by percentage, was Google. While it may not be a big surprise that the search engine giant is receiving this information, it is surprising to know that a credit-reporting agency is also receiving this information. Researcher Libert connects the dots when he said, "I was really shocked to find data brokers like Experian involved. Here are the people who know every credit card balance you ever carried, and they also know your health interests? That's pretty alarming." (Ungerleider, 2015) The data collected is supposed to be anonymous. However a data broker, like Experian, could easily connect the bits and bytes together to actually identify the user. It is at this point when the potential for discrimination could occur. Personal identification could also occur in this way, "A visitor to WebMD's page on HIV/AIDS, by comparison, sends user

information to a staggering 34 different online advertising companies. Visits to enough pages on HIV and AIDS, combined with a user's web browsing history, can lead to advertisements for HIV and AIDS treatments being directly targeted toward the user—effectively outing their HIV status." (Ungerleider, 2015)

It is worth revisiting the concept of privacy as related to our health information. It is easily understood and known that the Federal Health Insurance Portability and Accountability Act (HIPAA) protects and makes private communications to our medical doctor, psychologist, psychiatrist or pharmacist. Put into effect in 1996, this act essentially ensures what is a said by or to a patient remains within the system of medical providers, health insurers and the patient. Providers and practitioners in the health care field are considered covered entities under the regulation and can face criminal as well as civil punishments if they violate the regulation. This regulation is what prevents, for example, the public relations person at a hospital from commenting to the news media about a particular patient. However, this regulation does not identify a company like Experian or Web MD as a covered entity.

The National Security Agency

It is impossible to have a discussion about privacy and surveillance without discussing the National Security Agency (NSA) and some of the prolific whistleblowers such as Mark Klein, Thomas Drake, William Binney and Edward Snowden, who brought the activities of the NSA to public light. The NSA is the government agency responsible for signals intelligence (SIGINT). SIGINT consists of monitoring, collecting, storing and analyzing global communication for foreign intelligence gathering and counterintelligence. It also is tasked to protect government computers and networks from cyber attacks.

Created shortly after the end of World War I, the predecessor to the NSA, known as The Black Chamber, started the process of intercepting communications over wires. Back then; those communications went over telegraph lines.

> So the Black Chamber chief, Herbert O. Yardley, and his boss in Washington, General Marlborough Churchill, head of the Military Intelligence Division, paid a visit to 195 Broadway in downtown Manhattan, headquarters of Western Union. This was the nation's largest telegram company – the email of that day.
>
> The two government officials took the elevator to the 24th floor for a secret meeting with Western Union's president, Newcomb Carlton. Their object was to convince him to grant them secret access to the private communications zapping through his company's wires. (Bamford, Building America's Secret Surveillance State, 2013)

The meeting was a success and many others like have been repeated over the decades. The types of wires have changed and the material transmitted through them has exponentially grown.

Fast-forward to the early 2000's and a former AT&T technician named Mark Klein discovered, and ultimately revealed, the existence of a secret room within one of AT&T's network facilities in San Francisco. The secret room, known as room 641A, was used by the NSA and contained equipment that could capture and analyze all the traffic passing through the fiber optic cables in that facility. Those cables represented a part of the Internet backbone and a device called a splitter was sending a copy to that secret room. "This splitter was sweeping up everything, vacuum-cleaner-style," Klein said, "The NSA is getting everything. These are major pipes that carry not just AT&T's customers but everybody's." (Nakashima, 2007) The quantity

and variety of information carried through those cables and others like it, has only increased since the revelation Klein made.

Other whistle blowers speaking out about the interception and use of this digital data came later, Thomas Drake and Edward Binney for example, but the most prolific whistle blower in this sector continues to be Edward Snowden. A former IT contractor to the NSA, Snowden collected and subsequently gave to select journalists an enormous amount of information regarding many different surveillance programs in use. With names like Prism, Muscular, Stellar Wind and Boundless Informant, Snowden revealed the existence of tools used to pry into your digital enclosure, peer into the eyes of your data self and look deep into its soul. For example, "The National Security Agency has obtained direct access to the systems of Google, Facebook, Apple and other US internet giants, according to a top secret document obtained by the Guardian. The NSA access is part of a previously undisclosed program called Prism, which allows officials to collect material including search history, the content of emails, file transfers and live chats, the document says." (Greenwald & MacAskill, 2013) The important consideration to understand is this access and collection is gathering information on United States citizens *within* the United States without their knowledge, approval or judicial process.

The infrastructure of governmental surveillance has evolved from the syndic on the street to buildings filled with cables, servers, digital storage and knowledge workers. Currently, a unique monument of government surveillance exists in Bluffdale, Utah. Built for the NSA, the generically named "Utah Data Center" is a repository for the data collected by their surveillance efforts. "Flowing through its servers and routers and stored in near-bottomless databases will be all forms of communication, including the complete contents of private emails, cell phone calls, and Google searches, as well as all sorts of personal data trails—parking receipts, travel

itineraries, bookstore purchases, and other digital ‘pocket litter.’” (Bamford, The NSA is Building the Country's Biggest Spy Center (Watch What You Say), 2012) The facility is one million square feet in size and uses enough power and water to support a small city. Historically, a facility like this one would be unknown to most citizens, but the revelations brought forth by the whistleblowers has elevated the NSA’s activities in the public consciousness and a heightened amount of media attention.

The response by the NSA, in the cases of the whistleblowers, was to attack the accusers. This was done through legal channels such as search warrants and criminal charges. Public relations tactics were brought to bear also. Generally speaking, the whistleblower was criticized in the press and the narrative was redirected away from the content of the leak and towards the damage done because that information was out in the public. There were challenges to the whistleblowers patriotism and concerns issued that their leak had affected lives.

Best Practices

This is the age of surveillance, sousveillance, privacy, data mining and the intersection of all these forces. Encompassing more and more of our daily lives, collecting more and more invasive and personal information about our lives and applying this information in ways that are hard to imagine, questions have to be asked by the Public Relations practitioner. A recently published study of one million websites highlights the depth the data self is subjected to surveillance online,

> Findings indicate that nearly nine in ten websites leak user data to parties of which the user is likely unaware of; over six in ten websites spawn third-party cookies; and over eight in ten websites load Javascript code from external parties onto users' computers." (Libert, Exposing the Hidden Web: An Analysis of Third-Party HTTP Requests on One Million Websites, 2015)

There is no question that when ninety percent of one million websites are monitoring visitors, sharing that data with the advertising industry that, in turn, categorizes those visitors as "American Royalty," "Blue Collar Comfort," "Diapers and Debit Cards" or "Small Town Shallow Pockets" (Experian Marketing Services, 2014), the companies behind those websites will eventually face questions from their publics.

Reflecting back to "Joe" in the introduction, "What do we do with Joe and the information he is creating or leaving behind? What can we do? What should we do?" Public relations will intersect with these issues in the form of crisis communications and image management. The crisis management component is certainly the most volatile and holds the most potential for damage and the Public Relations professional needs to plan for the eventuality. A suggested selection of best practices for the PR professional follows, to help navigate these

complex waters. They are based on the framework of a crisis consisting of five stages: Detection, Prevention/Preparation, Containment, Recovery and Learning. (Fearn-Banks, 2011)

Understand this is topic of consideration (Detection)

There is a growing national conversation about privacy and surveillance. As of this writing, it has been over two years since the original Snowden revelations and articles continue to be written as documents from the files he procured from the NSA are slowly released. In the United States, the legislative branch of government is discussing this topic, presidential candidates are taking positions and the judicial branch has made some rulings concerning the legality, or illegality, of mass surveillance.

Commercially, the conversation is growing about the use of ad blocking software in the Internet browser, which has a direct relationship to the persistent tracking, and categorization of consumers that advertisers are performing. More attention is being paid to the hacking of customer data, credit card information and identity theft. As more personal data is shared, stored or transported online consumers will be more concerned about how their information is protected. PR needs to be cognizant of this topic and how it may or may not be involved in any given scenario or corporate image management activities.

Start Early (Prevention/Preparation)

Public Relations practitioners are in a unique position to have a long-term outlook and the need to have a situational awareness beyond one small facet of an organization. Often, the PR practitioner is involved across departments within an organization and has the opportunity to connect dots together that may otherwise go unnoticed. For these reasons, it is important that a PR professional is involved in the early stages of a new product, service or even company. No project is started without thinking about and putting together a budget for example. The

involvement of the PR professional should have the same level of consideration. Technology is creating opportunities for growth that seem limited only by the human imagination. In the excitement of developing a new technology, website, service or spying capability, the PR professional should ask the question, "Though it can be done, should it be done?" Also, "If we do this, what are the ramifications in terms of the company image? Is this capability 'pro-privacy' or 'anti-privacy' and should this be revealed?"

Crisis management plan for revelations about surveillance (Prevention/Preparation)

Prepared organizations should have a crisis management plan covering a wide range of scenarios. Common events might include workplace violence, a toxic spill or a product recall. Consideration should be given to crisis events such as whistleblower activity or leaks of information by employees within the organization. This ties back into the previous questions of "Though it can be done, should it be done" and "If we do this, what are the ramifications in terms of the company image?" Having the answers to those questions early will help prepare for the crisis response if it becomes necessary.

A few elements of apologia crisis communications theory could be put into use for these responses. Apologia theory is defined as, "…an effort to defend reputation and protect image. But it is not necessarily an apology. The organization's effort may deny, explain or apologize for the action through communication discourse." (Fearn-Banks, 2011) Two strategies should be considered for scenarios like this. First, redefinition, which is a suggestion that the organization did not set out or intend to do the wrong thing. Second, dissociation, which is a suggestion that while the organization appears to have done something wrong, it actually has not.

Consider the data self (Prevention/Preparation)

If efforts are made, or the intention of an organization is, to protect the privacy of its clients, it is important to consider where the data self "lives" in the environment, what is collected and stored and determine if the location is safe. The PR professional does not necessarily have to have a deep technical understanding of the mechanics behind this topic, a general grasp of the core questions and answers is important.

Consider Apple Computers for a moment. In some instances they make a conscious effort *not* to collect information so they do not even have it to lose. If they are compelled by a court order or even suffer a server breach done in secret, certain elements of the data self are not even in their environment of servers. Other elements are encrypted in such a way that the data is useless without the key and Apple does not have the key.

The location of where customer data is stored is also important to know. There are essentially two places where the data self can live. First, within the walls of the company on servers they own, operate and control. The privacy policy of the organization and the laws of the country where it resides directly affect that location. If the organization pledges to keep the information private, the IT department understands other parties should not access the information and protocols can be put into place to implement the privacy goals. A second location is often referred to as "the cloud" which is simply a computer server outside of the organization and is often owned and managed by a third party. In this instance it is important to know what privacy policies are in place with that third party, what protections are offered and even how safe is the path between the two organizations. Geographic location is a consideration as well. "Clouds" located in the United States are subject to United States law, "clouds" located in other countries are not subject to those laws.

Opportunity to market against surveillance and privacy violations (Learning)

There is a growth of companies that are taking a position on mass government surveillance and privacy violations and marketing their product or service as a tool or platform to fight against these issues. A few highlight the varying places within the digital enclosure that resistance can be used.

Individuals and business alike have a need to backup precious data like photos, bank records, health records or other documents. Online, or "cloud" services, are available but the concern exists about the safety of the storage location and the path between your computer and that cloud. Spider Oak, for example, is a cloud storage provider that offers end-to-end encryption of your data and no knowledge of the contents of your data because they do not have the key. Another company, Tresorit, offers a similar service but they tout the idea that their servers are located in Europe, where they are protected by rigorous European privacy laws and are untouchable by United States law enforcement agencies.

As cited earlier in the case studies, a tremendous amount of surveillance, data collection, analyzing and categorizing is going on through the use of the web browser. Services like Tor market themselves as a way to surf the web anonymously while web browser extensions like Ghostery and AdBlocker protect web surfers from the prying eyes of marketing companies and data brokers by blocking their efforts to track the web surfer's activities.

A common thread of messaging by these companies and others like them revolves around the idea of "zero knowledge" about what you are storing on their servers and anonymous use of the Internet. They also position themselves as advocates for privacy and a way to fight back against the government surveillance apparatus.

Be a Sentinel (Learning)

As part of my research into this subject, I had the opportunity to personally interview Ahmad Douglas, an information security specialist in Philadelphia. With a strong background in computer science and experience in both the government and private sectors, Mr. Douglas provided a unique point of view and a capacity to take the highly technical subject matter of data security and explain it in an easy to understand way. During the course of my interview he commented about the feeling he had about his role in this complex networked world where the average citizen does not have the awareness or understanding to know what is being done to them in their digital enclosure. He said, "I view myself as a sentinel, it is important to be on the lookout for those who are not aware, do not know or understand." (Douglas, 2015) This mantra should be adopted and incorporated by the PR professional.

The PR professional should take the position of a sentinel within an organization, being on the lookout for pitfalls and the potential for crisis. While he or she may not posses the technical acumen to explain the mechanics of how a particular application or website works, the PR professional should be able to recognize the potential for privacy infringement, question the ethics and implications of surveillance activities and recognize potential outcomes of those activities. This PR sentinel can also observe the approach used by competitors in the field, as related to their treatment of the data self, that are invasive or ethically questionable and identify opportunities to develop and grow campaigns to promote their own transparent, ethical or protective treatment of the data self.

A final thought, consider the website, Ancestry.com for a moment. They offer a service where anyone can mail in a sample of their DNA, for the purposes of finding genealogical matches. The public relations sentinel should ask, "What could go wrong with this?"

Works Cited and Consulted

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015, January). Privacy and human behavior in the age of information . *Science , 347* (6221), pp. 509-514.

Andrejevic, M. (2007). *iSpy: Surveillance and Power in the Interactive Era.* Lawrence, KS, USA: University Press of Kansas.

Angwin, J., Savage, C., Larson, J., Moltke, H., Poitras, L., & Risen, J. (2015, August 15). *AT&T Helped U.S. Spy on Internet on a Vast Scale*. Retrieved August 15, 2015, from New York Times: http://www.nytimes.com/2015/08/16/us/politics/att-helped-nsa-spy-on-an-array-of-internet-traffic.html

Apple Computer. (2013, June 16). *Apple's Commitment to Customer Privacy*. Retrieved September 19, 2015, from Apple: https://www.apple.com/apples-commitment-to-customer-privacy/

Bamford, J. (2013, June 10). *Building America's Secret Surveillance State*. Retrieved September 26, 2015, from Reuters: http://blogs.reuters.com/great-debate/2013/06/10/building-americas-secret-surveillance-state/

Bamford, J. (2012, March 15). *The NSA is Building the Country's Biggest Spy Center (Watch What You Say)*. Retrieved September 19, 2015, from Wired: http://www.wired.com/2012/03/ff_nsadatacenter/all/1

Bentham, J. (1787). *The Works of Jeremy Bentham*. Retrieved October 24, 2015, from published under the Superintendence of his Executor, John Bowring (Edinburgh: William Tait, 1838-1843). 11 vols. Vol. 4.: http://oll.libertyfund.org/titles/1925

Blum, A. (2012). *Tubes: A Journey to the Center of the Internet.* New York, New York, United States of America: HarperCollins.

Chideya, F. (2015, September 17). *The Facebook of The Future has Privacy Implications Today*. Retrieved September 18, 2015, from The Intercept: https://theintercept.com/2015/09/17/facebook/

Douglas, A. (2015, November 21). Information Security Professional. (R. McMahon, Interviewer) Philadelphia, PA, USA.

Experian Marketing Services. (2014, October). *Mosaic USA Consumer Lifestyle Segmentation by Experian.* Retrieved November 2015, from Experian: http://www.experian.com/marketing-services/consumer-segmentation.html

Fearn-Banks, K. (2011). *Crisis Communcations: A Casebook Approach.* New York, New York, United States of America: Routledge.

Fernback, J. (2007). Selling Ourselves? Profitable surveillance and online communities. *Critical Discourse Studies , IV* (3), 311-330.

Fitzpatrick, A. (2015, February 10). *Apple is Now Worth Over $700 Billion*. Retrieved October 4, 2015, from Time: http://time.com/3704014/apple-700-billion/

Foucault, M. (1977). *Discipline & Punish.* New York, New York, USA: Random House, Inc.

Greenwald, G., & MacAskill, E. (2013, June 7). *NSA Prism program taps in to user data of Apple, Google and others*. Retrieved September 19, 2015, from The Guardian: http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

Hull, G. *Successful Failure: What Foucault can Teach Us about Privacy Self-Management in a World of Facebook and Big Data.* University of North Carolina, Charlotte.

Kaplan, E. (2015, March). The Spy Who Fired Me. *Harper's Magazine* .

Kirn, W. (2015, November). *If You're Not Paranoid, You're Crazy*. Retrieved November 27, 2015, from The Atlantic: http://www.theatlantic.com/magazine/archive/2015/

11/if-youre-not-paranoid-youre-crazy/407833/

Kokalitcheva, K. (2015, August 4). *Your Facebook friends could be the ticket to your next loan*. Retrieved November 22, 2015, from Fortune: http://fortune.com/2015/08/04/facebook-loan-approval-network/

Lenddo. (2015). Retrieved November 21, 2015, from Lenddo: http://www.lenddo.com

Libert, T. (2015, October). Exposing the Hidden Web: An Analysis of Third-Party HTTP Requests on One Million Websites. *International Journal of Communcation* .

Libert, T. (2015, March). Privacy Implications of Health Information Seeking on the Web. *Communications of the ACM* .

Lobosco, K. (2013, August 27). *Facebook friends could change your credit score*. Retrieved September 18, 2015, from CNN Money: http://money.cnn.com/2013/08/26/technology/social/facebook-credit-score/

Nakashima, E. (2007, November 7). *A Story of Surveillance*. Retrieved September 19, 2015, from The Washington Post: http://www.washingtonpost.com/wp-dyn/content/article/2007/11/07/AR2007110700006_pf.html

Pasquale, F. (2015, September 21). *The Other Big Brother: Government surveillance gets most of activists' scrutiny, but many of today's privacy abuses are happening in the workplace.* Retrieved October 24, 2015, from The Atlantic: http://www.theatlantic.com/business/archive/2015/09/corporate-surveillance-activists/406201/

Peterson, A., & Tsukayama, H. (2015, September 29). *How Apple is trying to protect your privacy as its products get more personal*. Retrieved September 30, 2015, from The Washington Post: https://www.washingtonpost.com/news/the-

switch/wp/2015/09/29/apple-is-selling-targeted-ads-but-its-new-privacy-policies-show-why-its-thinking-different-about-tracking/

Pew Research Center. (2014). *Public Perceptions of Privacy and Security in the Post-Snowden Era.* Washington: Pew Research Center.

Sanger, D., & Chen, B. (2014, September 26). *Signaling Post-Snowden Era, New iPhone Locks Out N.S.A.* Retrieved September 19, 2015, from The New York Times: http://www.nytimes.com/2014/09/27/technology/iphone-locks-out-the-nsa-signaling-a-post-snowden-era-.html

Sullivan, M. (2015, August 4). *Facebook patents technology to help lenders discriminate against borrowers based on social connections*. Retrieved September 18, 2015, from Venture Beat: http://venturebeat.com/2015/08/04/facebook-patents-technology-to-help-lenders-discriminate-against-borrowers-based-on-social-connections/

Turrow, J. (2011). *The Daily You: How the New Advertising Industry is Defining Your Identity and Your Worth.* New Haven, CT, USA: Yale University Press.

Turrow, J., Hennessy, M., & Draper, N. (2015). *The Tradeoff Fallacy: How Marketers are Misrepresenting American Consumers and Opening Them Up to Exploitation.* University of Pennsylvania, Annenberg School of Communication. Philadelphia: University of Pennsylvania.

Ungerleider, N. (2015, February 23). *The Latest Privacy Risk? Looking Up Medical and Drug Information Online*. Retrieved March 1, 2015, from Fast Company: http://www.fastcompany.com/3042763/privacy-risk-looking-up-medical-health-information-online