6-2017

When Personal Becomes Profitable: Data Collection and the Complex Link Between Corporate and Government Surveillance and the Risk to Civil Liberties

Justin Gump
Union College - Schenectady, NY

When Personal Becomes Profitable:

Data Collection and the Complex Link Between Corporate and Government Surveillance, and the Risk to Civil Liberties

By

Justin Gump

* * * * * * * * *

Submitted in partial fulfillment

of the requirements for

Honors in the Departments of History

UNION COLLEGE

March 10, 2017

ABSTRACT

Thesis Advisors: Andrew Feffer Ph. D. & Lori Marso Ph. D.

Personal data represents a commodity of increasing interest to both the United States government and large corporations. While their reasons differ, the two powerful entities have worked together to radically expand the domestic surveillance activities in the U.S. As the government surreptitiously expanded its domestic surveillance under the guise of its "war on terror," it quickly realized that the advanced technology and access to personal data held by many large corporations presented a valuable source of surveillance information. These companies, in turn, similarly saw an opportunity for revenue in both the sale of the data and large governmental contracts to provide the technology and infrastructure to support the surveillance activities. Thus, a disturbing yet symbiotic partnership has developed, and with it a political environment that thwarts efforts to disclose and provide appropriate regulation to supervise these activities. All of this leaves the civilian population at an increased risk—a direct result of an industry that treats the individual as both a product and a consumer. In turn, the transition from personal information to profitable information has created a myriad of social and political implications that have not yet been fully analyzed or understood. Only the future will tell how these developments will ultimately play out, whether in favor of corporate-government interests, or the protection of civil liberties. This is a critical decision for the future of the United States, and the overarching issues surrounding privacy in the digital age have not been adequately addressed by either the legislative or judicial branches of government. As technological developments continue to advance, and the demand for, and value of, personal data continues to increase, the insistence that these issues be addressed will seemingly need to come from American citizens, as their right to privacy is continually being eroded. One can only hope that this insistence is not brought about by catastrophic circumstances.

Table of Contents

Chapter One: Introduction

The data collection industry is worth more than three hundred billion U.S. dollars as of 2012 (Morris 2012). Technological advances have enabled both the U.S. government as well as large private firms to consolidate massive amounts of information on every single person active on the internet. Through the use of agencies such as the CIA, FBI, and most notably the NSA, the U.S. government has created the largest and most comprehensive surveillance state in the history of the world. While certain levels of classification are necessary for the war on terror, the government has chosen to not disclose many aspects of its surveillance programs since the attack on September 11, 2001. However, with the aid of whistleblowers such as Edward Snowden, the public has now been given a comprehensive view of just how pervasive the American government's surveillance of its citizens truly is. Through the use of complex and invasive technologies, the government has essentially ignored its citizens' rights to privacy set forth within the U.S. Constitution. What is more, private data broker firms and corporate communications companies have utilized similarly invasive forms of surveillance technology to not simply collect information on people, but also to sell and profit from it in various ways. With personal data representing a precious commodity to both corporations and government, the link between the surveillance practices of the two entities has become extremely complex, subsequently creating numerous implications for society as a whole. In my thesis, I will contest the legitimacy of a collaborative, mutually beneficial relationship between corporate and government surveillance. In doing so, a history of the National Security Agency will be studied to argue how the agency has revolutionized surveillance technology leading to a myriad of social and political changes. With this established, the connection between government and corporate surveillance will be elaborated upon, using numerous examples of collaboration to argue how the

two entities symbiotically use each other for legal circumvention and profit. This mutually beneficial surveillance relationship will be shown to entail an encroachment on civil liberties most Americans fail to recognize—both surveillance and data collection reform are regularly inhibited in a variety of ways through the powerful combination of government and corporate forces, eliminating chances for greater oversight in a business that deals in sensitive, personal information. "'Information is power, and the necessary corollary is that privacy is freedom.' How this interplay between power and freedom play out in the information age is still to be determined" (Huhne 2013). The idea behind this insightful point will be used to examine how the issues of this complex interplay may ultimately be resolved going forward.

Chapter Two: Origin of the Modern American Surveillance State

The U.S. government came to have the most advanced and invasive surveillance state in the world through a radical reshaping of the National Security Agency (NSA). In explaining the actions and the decisions made by the NSA, it is beneficial to provide a brief history of the agency as well as its fundamental purpose. First and foremost, it is essential to understand that the NSA was designed to surveil foreign affairs, not domestic. It was first conceptualized after the surprise attacks on Pearl Harbor by the Japanese in the midst of the Second World War. In 1952, the idea became a reality; the NSA was created to monitor foreign threats and prevent surprise attacks (Burns 2005). While the agency grew in capabilities from that point on, it remained largely uncontroversial and unknown to the majority of Americans at the time.

However, during the Nixon administration, the NSA overstepped its bounds through the tapping of American citizens' phone calls (United States 1974). From that point on, Congress made it explicitly clear that the NSA had no power to conduct any form of spying operation on American citizens. However, with the attacks on September 11, 2001, the fate and purpose of the National Security Agency was forever changed. The federal government capitalized on a sudden influx of fervent patriotism and anger running through the American public, taking advantage of this surge of emotion to expand its powers, perhaps best epitomized by the passing of the USA Patriot Act. Standing for **U**niting and **S**trengthening **A**merica by **P**roviding **A**ppropriate **T**ools **R**equired to **I**ntercept and **O**bstruct **T**errorism, this act essentially gave the Bush administration free reign to design and implement far more aggressive methods in the war on terror.

In looking for more effective approaches to combat and prevent terrorism, the Bush administration went to the NSA to gain more insight as to what could be done to prevent another

attack. The head of the NSA, General Michael Hayden, was given a radical new authority through the President "using both his inherent power under Article Two of the Constitutional authorities and the provisions of the AUMF - the act passed by Congress, the Authorization for the Use of Military Force" (United States 2005). This controversial decision was the beginning of the Bush administration's path down the slippery slope of infringing on the protections afforded to US citizens by the United States Constitution, more specifically the Fourth Amendment. However, acting on the clear orders given to him by Vice President Dick Cheney, Hayden essentially told his employees to adopt a no holds barred approach and, under his authority, seek out far more aggressive surveillance programs that could be utilized. Many hyper-invasive programs already existed within the walls of the NSA at this time; the only change was that they had now been authorized (PBS 2008). Not surprisingly, this sudden fundamental change in NSA policy was kept secret from a large majority of the thousands of employees within the agency. Hayden and his small circle of top agency personnel knew they had to tread lightly and discreetly in the practice of surveilling the American people. Hayden himself even came out in an interview stating how he essentially knew, deep down, that this would one day come to light and it would not be received well by the public (Hayden, Wiser, Gilmore 2014). The men and women of the NSA all knew their basic guidelines were never to spy on innocent American citizens. To do so would be a violation of the citizens' privacy rights—this was the clearest breach of the public trust that could be effected by any NSA agent and he or she was constantly reminded of such prior to 9/11.

However, with his new authority, General Hayden began creating and implementing numerous programs to use on the general public such as *Trail Blazer* and *Prism*. Programs such as these were designed to monitor and collect various forms of data in a dragnet fashion, largely

ignoring the right to privacy that is outlined in the Constitution. “Hayden revealed that his insistence that it was legal for the NSA to conduct warrantless surveillance was not based on even a nodding familiarity with the constitutional issues involved,” but rather the simple fact that his orders were his orders and he would follow them without question (McAvoy 2010, 167). In defense of Michael Hayden, it is worth mentioning that the man has been a solider for the majority of his life, willing to sacrifice himself for his country and what he believes will “save” it. However, there were situations in which Hayden could have chosen less invasive techniques while still achieving the same effect. For example, despite the fact that certain programs such as *ThinThread*[1] existed and could be used for the internet surveillance in a more constitutional manner, Hayden chose to use the data-network surveillance program, *Trailblazer*. While *ThinThread* was designed with the intentional parameter to only collect data coming in or out of the country, Hayden instead chose a program that indiscriminately analyzed domestic networks as well. While *Trailblazer* would eventually be abandoned by the agency in 2006 due to its extraordinary cost of maintenance[2], it evidenced the sudden inundation of increasingly invasive surveillance programs and techniques implemented by the agency to use and analyze domestic data and metadata. With all the actions of the NSA taking place behind closed doors, the ignorance of constitutionality displayed by Hayden spawned what would become the most advanced domestic surveillance state in US history.

Representing a significant breach of the privacy of unknowing American citizens, agents involved with the projects knew they had to be extremely secretive, and also keep the circle of

[1] *ThinThread* was a program that could capture and sort massive amounts of phone and e-mail data. It was the brainchild of veteran crypto-mathematician Bill Binney. Major contributions to the program were also made by Binney’s fellow crypto-mathematicians, Kirk Wiebe and Edward Loomis (Hayden, Wiser, Gilmore 2014).

[2] In a 2005 Senate hearing, General Mike Hayden admitted that *Trailblazer* was hundreds of millions of dollars over budget and alarmingly behind schedule (Lipowicz 2005).

informed NSA employees as small as possible. However, it was only a matter of time before the veteran cryptologists William Binney, Kirk Wiebe, and Edward Loomis who had created the *ThinThread* program, along with its protections, became aware of what was now being done. More knowledgeable as to the capabilities of the program than anyone else, the members of the *ThinThread* team felt they could simply not be a part of what they saw as clearly illegal activities. Loomis had worked for the agency during the Nixon era and went on record saying he saw undeniable parallels between the environment he worked in then, and the environment he found himself working in now- the laws were once again being ignored in the face of a perceived threat. Binney went on to explain in a PBS interview years later that "the code itself that we [*ThinThread* team] had created evaporated. All the programmers that worked for me, they left for other jobs after *ThinThread* was killed" (PBS 2008). Thus, at the end of October, 2001, Wiebe, Binney, and Loomis were left with no choice but to resign as well. These veteran cryptologists had been a part of the agency for decades. They would not allow themselves to be associated with the illegal actions that were rapidly expanding, and would continue to do so after they left. The troubling fact was, "with the rapid growth of technology and the ripe environment of the post-9/11 landscape, the NSA and intelligence community could only get bigger and bigger" (Verble 2014). In the years following the departure of the *ThinThread* team, the NSA continued to collect massive amounts of data on millions of Americans. By the year 2008, the NSA was spending 10 billion dollars a year on data collection alone (DNI Budget Report 2009). The amount of information being collected was growing out of control, yet both the Bush and Obama administrations had made it clear through numerous statements that they were going to continue to deny any and all allegations that the NSA was possibly spying on innocent American citizens. "'This is not a domestic surveillance program,' Cheney told radio host Hugh Hewitt, adding that

‘what we're interested in are intercepting communications, one end of which are outside the United States, and one end of which we have reason to believe is al-Qaida-related’” (Braun 2013, 1).

Foreign Intelligence Surveillance Courts: The Initial Link Between NSA Surveillance and Corporate America

While the radical expansion of NSA surveillance programs continued to increase in the decade following 9/11, the fact of their existence still remained unknown to nearly every American. Programs were collecting massive amounts of online data in any and all forms on millions of American citizens. Furthermore, with the use of secret warrants authorized by the FISA courts [Foreign Intelligence Surveillance Act of 1978], Hayden was enabled to surveil and attain Americans’ data and call records from the largest communications companies in the country (McAvoy 2010). The fact that a classified, foreign affairs appellate court was given the authority to declare lawful a United States federal action that was entirely domestic is ludicrous—both the agency and the court were designed around surveillance law that only “allows the government to acquire foreign intelligence information concerning non-U.S.-persons… located outside the United States” (Greenwald 2013). This is a testament to the fact that, by the mid 2000s, the entire purpose and function of the NSA had completely changed; not only was the agency conducting controversial domestic operations, the court designed to limit its power and judge its actions was intentionally limiting legitimate constitutional oversight. Essentially, in the name of “the war on terror”, companies such as Verizon, Facebook, Microsoft, Google, Yahoo and others were forced to open up all of their records to the eye of the NSA, while at the same time, never given the legal ability to disclose or reveal such actions to their customers (Lee 2013).

Despite the fact that such an action by the federal government clearly required further judicial review, the warrant from FISA technically made its actions legal and thus, the massive domestic spying program known as PRISM was formed in 2007. “Although domestic surveillance does not fall under the NSA's purview,” this new program enabled “warrantless wiretapping and electronic surveillance of communications involving U.S. citizens” (Atkins 2011). Not only was the agency conducting large-scale operations on American citizens, these controversial activities were being facilitated by the federal government's manipulation of the law. District and appellate courts such as FISA are obliged to base their judgments using a strict and rigid interpretation of the Constitution. However, the actions of the FISA courts demonstrated just how far the NSA was willing to go in the effort to maintain its ability to collect American citizens’ data and metadata. While the agency hid behind the facade of solely targeting and surveilling terrorists or suspected terrorists, the federal courts were pressured into turning a blind eye to what was truly occurring, ignoring the “need to rework FISA and NSA protocol to adhere to the Constitution and protect US citizens from this overreach of power” (Verble 2014). What is more, the NSA’s collection of citizens’ data through programs like PRISM now meant major American corporations were involved with the process of surveilling the population in dragnet fashion. This relationship between government surveillance and big business has only grown since 2007 and, with the leaks provided by Edward Snowden, much of the details surrounding it have become known to the public.

In response to allegations of giving away customer data to government, nearly all of the accused companies have either not responded, or chosen to deny in various forms of overly-legalistic language. Mark Zuckerberg responded to the media saying “Facebook is not and has never been part of any program to give the U.S. or any other government direct access to our

servers;" Microsoft stated, "We only ever comply with orders for requests about specific accounts or identifiers…Google's Zunger says that Google only responds to "specific orders about individuals" (Lee 2013). Across the board, the companies have denied ever granting companies *direct* access to their servers. However, aided by *The Guardian's* leaking of Snowden's documents on PRISM, top-secret NSA slides have stated that the program involves "collection directly from the servers of these U.S. service providers: Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, Youtube, Apple" (Lee 2013). Making matters worse, while the rules regarding PRISM and those under "section 702 of the FISA Amendments Act" assert that the NSA can only collect data on someone who has been found to be in either deliberate or inadvertent contact with a foreign target, documents "from Snowden showed that the NSA breached privacy rules thousands of times a year" (MacAskill 2013). However, even with all the damaging evidence against FISA and the NSA, the federal government responded by simply enacting "a new, highly diluted FISA law—the FISA Amendments Act of 2008 (FAA)," legalizing "much of the Bush warrantless NSA program" (Greenwald 2013). As in so many other cases with the NSA, the lack of oversight and legitimate judicial review enabled the agency to vastly overstep its authoritative bounds with little to no risk of punitive consequences. The FISA courts have evolved to essentially function as a rubber stamp in their permissiveness and unjustifiable interpretation of constitutional rights to privacy.

On top of all this, the FISA courts have legalized spying on the activity of people's phones, which has in turn created a never ending flood of secret warrants to all telephone providers. While the argument is based on national security, such an expansive project demands a more thorough examination of constitutionality. The numbers make this clear by themselves: "One of the larger carriers, AT&T, responds to roughly 700 requests a day, 230 of which are so-

called ‘emergencies,’ exempting them from standard court orders” (Whitehead 2012). While the official number for 2012 is approximately 1.3 million, “The number of requests is almost certainly higher… and the number of people affected much higher, because a single request often involves targeting multiple people” (Whitehead 2012).

Chapter Three: Government Surveillance Outsourcing and The Role of the Corporation

Why did companies turn over our data so willingly? While many of the company executives claim the contrary, the unfortunate truth that is beginning to become increasingly apparent is that companies do not simply hand over customer data to the government as a result of a farcical overproduction of FISA warrants—they do so willingly because they make a profit. In understanding the link between corporate and government surveillance, it is essential to realize that corporations are not simply giving away customer data. They are more or less choosing to do so for the same reason they do anything—to make a profit.

With the huge market for smartphones in the United States as well as abroad, large corporations involved with the technology have acquired a massive arsenal of possible surveillance capabilities. Even though the United States government has amassed a huge range of similar capabilities over the past decade, the incentives offered by access to corporate servers' data and metadata trump much of what the NSA and FBI are capable of. Thus, while "government agencies are increasingly acquiring the technology to track cell phones themselves, most rely on cell phone companies to provide them with the user data" (Whitehead 2012). What is more, the "private sector partners with government and local law enforcement agencies in developing technology to conduct extensive domestic surveillance" in exchange for generous contracts. With this, government spying is no longer reserved to agencies like the NSA and FBI. Federal, state and even local police forces are now able to utilize previously nonexistent technologies, such as "Stingray" cellular phone tracking—an invention by Harris Corporation. After a recent ruling by the United States Court of Appeals, it was deemed lawful to track cellular devices without first acquiring a warrant, essentially creating a useful tool for

government and police forces to circumvent legal restrictions (Whitehead 2012). This circumvention has been intensified by what is essentially an extraordinarily powerful, military grade piece of technology—Stingray. "ACLU privacy researcher Christopher Soghoian" explains how "the government uses the device [Stingray] either when a target is routinely and quickly changing phones to thwart a wiretap or when police don't have sufficient cause for a warrant" (Walker 2013). While this explanation leads one to assume Stingray is reserved solely for serious criminals or people suspected of a serious crime, it opens the door for police forces to use the technology in far more invasive and expansive ways. As with *Trail Blazer* and *Prism* before it, this legitimate technology is not the problem—it is the abuse of the technology.

Not too long ago, wiretapping a phone required significant time and resources, and often yielded insufficient results. On the other hand, Stingray appears to be so radically advanced that many people caught committing crimes by the device have been released simply to avoid any discussion of the technology in court (Pagliery 2015). However, according to a recent document from a New Jersey district court regarding a Stingray case that did receive judicial review, the suitcase-sized device is not only capable of tracking information like who someone called and the duration of the conversation, it can essentially extract the entire digital-footprint[3] of a phone from *over a mile away* (18 US code 2012). What is more, as if a mile-wide radius was not extensive enough, federal planes now fly over various parts of the country and, with the same mobile appearance as any cell tower, collect the passive digital-footprints of all mobile devices caught in the data dragnet below (Pagliery 2015). This impressive piece of technology would never have been made possible without the interplay between Harris Corporation and the government. This is merely one example of the corporate-government relationship that manifests

[3] A digital-footprint refers to the trail of data left behind via any digital service. An active footprint is data the user knowingly shares; a passive footprint is data extracted without the knowledge of the user.

itself in society in countless ways. However, while Stingray is remarkably advanced, its relatively high price still makes it difficult to acquire by most police forces' standards, and thus it is used most widely in larger cities like New York and Los Angeles. However, this by no means deprives lesser funded police departments from obtaining similarly advanced techniques of cellular tracking and surveillance—yet, instead of doing the surveillance themselves, many police departments simply employ corporations.

This has developed a new market in which telecommunications corporations can profit directly from sharing their own customers' data. While government agencies and police forces are now able to afford various spying technologies, the technologies still are not free. As government budgets tighten, the telecommunications corporations have responded happily to this new opportunity to increase profit margins, providing police agencies with prices for acquiring various pieces of information one has on his or her mobile phone. For example, "Sprint charges $120 per target number for 'Pictures and Video,' $60 for 'E-Mail,' $60 for 'Voicemail,' and $30 for 'SMS Content'" (Whitehead 2012). The capabilities of cellular companies like Sprint are so advanced that just one employee can track upwards of 300 people at the same time. Offering a better perspective of how widely used this surveillance contracting is becoming, Sprint employs a staggering 110 people to solely manage this service—that's a possible 33,000 people being tracked at any point in time by just one cellular provider (Whitehead 2012). One can only speculate as to the capabilities possessed by AT&T and Verizon Wireless, two significantly larger telecom corporations.

While major corporations have been repeatedly contracted by government agencies to increase dragnet surveillance, smaller, more specialized companies have also been utilized to experiment with revolutionary technologies most people would struggle to comprehend. A

unique example can be found through former Air Force pilot Ross McNutt's company, Persistent Surveillance Systems (PSS). McNutt worked extensively with the Air Force during the military campaigns in Iraq and Afghanistan, not as a pilot, but as an engineer who theorized and successfully implemented a new-age form of aerial surveillance that helped hunt down bombing suspects over wide swaths of desert and urban terrain (Schulz, Pike 1). McNutt has since retired from working with the military, but he realized the significant impact his technology could have on domestic surveillance. Soon after, he formed PSS and his *HawkEye II,* 'eye in the sky,' technology has now been used in numerous cities across the United States. To elaborate, McNutt's revolutionary form of surveillance "involves the deployment of [192] megapixel cameras on a Cessna aircraft, which circles over a city for up to 10 hours at a time," ultimately giving law enforcement the ability to examine 30-square-miles of land and "retroactively track any vehicle or pedestrian within that area. It is the ultimate Big Brother 'eye in the sky'" (Stanley, 1). When asked to describe his idea in layman's terms, McNutt essentially stated, "Imagine Google Earth with TiVo capability" (Reel 2016, 1). To be clear, the issue does not necessarily lie in McNutt's invention, and there is no denying the potential benefit it has to deter crime, a point Ross McNutt stresses when he pitches his idea to metropolitan police divisions. Rather, the issue lies in the fact that a deterrent such as this cannot achieve McNutt's stated goal when it is being used on communities and cities across the country without the citizens being made aware.

Despite attempts by the FBI and police to keep McNutt's technology a secret, information about the "eye in the sky" being used over the skies of Compton eventually leaked in 2013, and thus the ACLU and other organizations seeking to protect civil liberties immediately demanded answers from the FBI. Even the Mayor of Compton, Aja Brown, was furious about

not being informed whatsoever, publicly stating, “There’s nothing worse than believing you are being observed by a third party unnecessarily” (Jennings, Winton & Rainey 2014, 1). A spokesman for the Bureau, Christopher Allen, met these demands for answers with a blunt claim that the FBI’s aerial technologies “are not equipped, designed or used for bulk collection activities or mass surveillance” (Harress 2014, 1). Yet, as has been the case countless times before, this statement simply was not true, and by 2015 there were numerous claims throughout the country that this technology was indeed being used to surveil civilian populations in several American cities, most notably Baltimore. Baltimore provides a unique example of how police forces can circumvent public disclosure of their new forms of handling crime and surveilling the public. One of the key ways the public becomes aware of and is able protest these new, invasive technologies is by denying the necessary funding for these costly practices. This occurs through city councils and elected officials either denying or allowing their police force an allocation of funding based on whether or not they believe the proposal is necessary and ethical—obviously their decisions are heavily influenced by public opinion. Considering the Baltimore Police Department’s long-running history of racial bias, as proven by a recent 163-page report by the Justice Department, one can likely speculate that a proposal for this costly technology system[4] would have been unsuccessful (Grinberg 2016, 2). Yet, all it took was a massive, individual donation from Texas based billionaire and former Enron trader, John Arnold, to completely circumvent this process of public oversight and thus, the “Baltimore Program” was given the green light to begin spying on an entire city without its knowledge or consent (Reel 2016, 7).

This unique form of surveillance in Baltimore highlights many issues surrounding corporate involvement in federal and state affairs. While PSS’s technology undoubtedly benefits

[4] According to Ross McNutt, a contract between his company and a metropolitan police force would cost approximately $2 million a year (Reel 2016, 4).

the fight against crime, its lack of disclosure has dangerous implications for communities as a whole, especially in places like Baltimore where a lack of trust between the police and the civilian population has been at the heart of countless protests, both peaceful and violent. Systems like McNutt's *HawkEye II* being privately funded by billionaires as a means to circumvent public approval are clear evidence that something is wrong, and perhaps unconstitutional. What is more, implementing it the way the Baltimore Police Department did gives off the notion that they know what's best for everyone, and the masses should remain blissfully ignorant, unaware that every resident of the city has literally been converted into a data point on a screen that tracks everywhere they go within a 30-mile radius. Further, the Baltimore Project is not an isolated incident in regard to the mutually beneficial relationship between police forces and private companies dealing in weapons technologies. ACLU attorney David Rocah describes it best, stating:

> What the secret funding from the Arnolds meant is that it [*HawkEye II*] didn't even have to be disclosed to the city's purchasing folks and the mayor didn't know, the city council didn't know… nobody knew. The fact is that surveillance technologies are acquired by police departments all over the country all the time with zero public input, even where the Arnolds aren't secretly funding it. This case is just an extraordinary, an extreme, example of a larger problem. (Dart 2016, 3)

One can clearly see how this represents a dangerous development in terms of the mutually beneficial relationship corporations have developed with federal and state institutions. While it would be unfair to ignore the arrests that have resulted from data vending, the growing use of the service "blurs the lines between law enforcement charged with protecting the public

and corporations seeking to profit from it" (Boghosian 2013, 43). The merits of this system would be clear in an ideal world; however, that is not the world we live in, and the habitual abuse of power in today's world leads one to envision a number of ways citizens could suffer from this symbiotic relationship. With the massive amounts of power wealthy corporations control, selling their own customer data as a means of assisting in the apprehension of people without any actual warrant could lead to exploitation. Ultimately, it would simply be a heightening of the degree of exploitation already occurring— "Police and private business have built a leviathan surveillance network" with a dearth of accountability (Boghosian 2013, 99). With it, police departments gain an invaluable form of surveillance; telecommunications companies gain profit—everybody wins, except us. The masses are given no control over their mobile privacy rights and, as taxpayers, they are essentially funding the entire operation in the first place—we are indirectly paying corporations to give our personal information to the police through tax revenue. As this data vending continues to grow, America's public sphere risks falling under a veil of corporate-government domination. Just as data vending has created a collusive relationship between government and corporation, data mining as a whole has evolved into a multi-billion dollar industry with significant interplay between government and the private sector.

Fusion Centers: The Start of Data-Mining Collaboration Between Government and the Private Sector

Along with the questionable legality of the domestic spying program, the actual implementation of the surveillance mechanisms created a highly secretive, collusive relationship between the government and private security companies. Functioning essentially as regional intelligence sharing facilities, fusion centers were built throughout the country beginning in 2003, proposed as a key tool in antiterrorism that would be primarily managed by the Department of Homeland Security (Isikoff 2012). The construction and maintenance of these

fusion centers has cost the government billions, yet the evidence of any significant increase in national security has yet to be proven. However, while fusion centers have achieved little more than an increase in the federal deficit, they have indeed created a profit—a corporate profit. Through the government's creation of what are essentially numerous state-of-the art data-mining facilities, the private security companies have been able to scour "public databases and other sources to gain information related to spending habits, real estate transactions, and insurance claims" (Boghosian 2013, 156). As the commodity of personal data continues to increase in value, private security companies have been enabled to profit in more ways than one via their continued fusion center contracts. Made more concrete by the actual figures, "approximately 1,931 private security companies and 1,271 government organizations are currently engaged in intelligence gathering" across the country, and while the threat of terrorism has somewhat declined since 9/11, intelligence gathering has increased exponentially (Boghosian 2013, 100). Facts such as these begin to suggest the idea that, while terrorism is a very real danger, the enhancement of surveillance is creating a dangerous weapon against the domestic civilian population as well. To elaborate, fusion centers have not simply failed to effectively stop terrorism, they have become vehicles for government discriminatory racial and religious profiling, consistently spying "on American Muslims without a justifiable law enforcement reason for doing so" (Isikoff 2012).

This disturbing trend fuels bigotry and racism towards the 3.3 million Muslims living in the United States, of which only a handful are in any way a threat to national security. Making matters worse, while many forms of surveillance such as these are done covertly, there is so much unabashed hatred of Islam in parts of the country that many politicians have publicly endorsed surveilling innocent Muslims, such as Senator Mitt Romney who "openly called for

fusion centers to wiretap mosques and spy on foreign students" under the auspice of fighting terrorism (Monahan & Palmer 2009, 628). This kind of political rhetoric can have dangerous effects on uninformed citizens who may take it is a confirmation that all Muslims living here and abroad are indeed a threat to their safety, a belief that is simply untrue and quite dangerous. What is more, fusion center surveillance has not only been used as a means of religious profiling, it has also been used against groups with 'unpopular' beliefs regarding more specific issues in the country, such as animal rights activists and anti-war protesters. Despite these groups solely protesting in legal, non-violent ways, "union and labor activists, environmentalists, and animal-rights protesters have also been documented targets of surveillance under the dubious rationale of preventing terrorism" (Monahan & Palmer 2009, 628). Surveillance projects such as these rely on the capabilities of fusion centers across the country, and to be clear, they are illegal based on the operating principles governing when it is acceptable to surveil and collect information on one or more persons. To elaborate, Title 28, Part 23 of the Electronic Code of Federal Regulations states:

> A project shall collect and maintain criminal intelligence information… only if there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity. A project shall not collect or maintain criminal intelligence information about the *political, religious or social views* [italics added], associations, or activities of any individual or any group, association, corporation, business, partnership, or other organization unless such information directly relates to criminal conduct or activity and there is reasonable suspicion that the subject of the information is or may be involved in criminal conduct or activity. (28 CFR 23.20)

Generalized surveillance of mosques and the collection of information about non-violent protesters and foreign students is clearly in violation of this statute. The way in which this criterion is routinely circumvented is by manipulating what can be deemed as a 'reasonable suspicion,' even though 'reasonable suspicion' is clearly defined in Part 23 of the ECFR as well. In the end, these unlawful surveillance practices contingent on fusion centers occur so frequently because there is simply not enough internal oversight. When the information collected does ultimately bring about some form of crime prevention, it is publicized and used as a defense of such practices. Yet, far more often than not, the massive amount of data collected on innocent people via fusion centers yields no positive results whatsoever, and the cost of doing so is immense. This is how the door for data-mining collaboration between government and the private sector has been opened.

Federal and especially state governments are unable to afford the costs of maintaining fusion center surveillance on their own. To collect the significant quantities of data they desire, they have no choice but to contract private agencies who do not have the same set of values and restrictions as the Department of Homeland Security(DHS)—the ultimate priority of the DHS is counter-terrorism, not making a profit. A major challenge for these private security companies is how they navigate the balance between making a profit and not infringing upon citizens' right to privacy. According to recent studies, it appears these "private companies may have a more lax orientation to privacy protection than do government agencies," and thus DHS agents working in "fusion centers can circumvent some privacy protections by working with them" (Monahan & Palmer 2009, 631). Personal, protected information belonging to innocent people is being outsourced to private companies whose employees have no stated obligation to serve the public, and now it appears it is purposefully being done so that sensitive, personal data can be moved to

a less regulated environment. Another troublesome aspect of these third-parties gaining access to fusion center databases is the fact that many of them are not as secure as they lead DHS agents to believe. Whereas the firewall and database protections of the Department of Homeland Security are nearly impenetrable, privately contracted companies lack the same capabilities, and thus "[h]ackers may now gain access to a wealth of additional, potentially damaging information" that leads to widespread identity theft (Monahan & Palmer 2009, 631).

Ultimately, fusion centers have been revealed to be largely an expensive, biased enterprise, damaging social relations at the expense of the taxpayer and straining the bounds of U.S. citizens' First and Fourth Amendment rights. What is more, after fourteen years of questionable results at a cost of an estimated 1.4 billion dollars, one cannot help but question whether or not the intricate symbiotic link between government and corporations is the underlying reason for continued funding and construction of fusion centers—especially as personal data continues to grow exponentially in value.

Chapter Four: Big Data Corporations and Why You've Never Heard of Them

The government is not alone in its desire for your personal information. While data-mining has been established for some time, the digitalization of American society has enabled a meteoric rise in the industry. Furthermore, in attempting to keep its practices secret and uninhibited, the government has helped enable the data collection industry to expand at even greater speeds through remaining highly unregulated and unknown to a large majority of the population. This has in turn allowed companies like Acxiom to post annual sales of 1.13 billion dollars, yet still remain completely unrecognizable to almost any American you talk to (Singer 2012). Conversely, large data-collection firms almost certainly know a good deal about you. While the specific ways in which companies like Acxiom independently collect personal information will be touched upon below, one might be surprised as to how these companies collect this information in direct collaboration with state and federal government.

State and federal governments have massive amounts of information stored on civilians in the United States—this is simply the way in which our society functions. If you want to drive a car, then you need to get a license at the Department of Motor Vehicles; if you want to travel to a different country, you need to apply for a passport through the Department of State; if you want to receive mail, you must tell the United States Postal Service what your address is, etc. This personal information has value to businesses in myriad ways, but most people assume the personal information they disclose to the government is a private exchange. Yet this is not the case: in fact, selling personal data has been a lucrative practice done at many levels of government for some time now.

Data collection firms such as Acxiom are actually the biggest customers for these various agencies, and data brokers are all too happy to hand over vast sums of money in exchange for equally vast amounts of personal information—one could go as far as to say that, "government data [is] the lifeblood for commercial data brokers. And government dragnets rely on obtaining information from the private sector" (Angwin 2014, 73). To elaborate, one of the most valuable pieces of civilian data sold by state governments are driver's licenses and traffic violation records. In fact, "Florida alone makes about $62 million a year selling driver's license data;" similarly, the "U.S. Postal Service generates $9.5 million in revenue a year allowing companies like Acxiom to access its National Change of Address database" (Angwin 2014, 69). State governments and federal agencies sell information like this every day. Even our elections, one of the country's oldest and most sacred practices, is not protected from this corporate-government collaboration. To participate in the United States elections, citizens are required to fill out a form from the government that requires personal information such as one's name, address, and date of birth. Most people assume the information they divulge in order to take part in one of America's most sacred processes will be free from any and all profit-driven disclosure, and unfortunately they are mistaken.

Federal voting records are sold to data brokers in all states; in fact, a "2011 study found that a statewide voter list sold for as little as $30 in California and as high as $6,050 in Georgia" (Angwin 2014, 74). This is done every year, and it enables data brokers who continuously amass voters' data to build elaborate profiles on people who do not even know they are being observed. While some may view this as an unjust practice, it is completely legal and the data brokers who specialize in it, such as Aristotle Inc., proudly boast the "ability to identify 190 million voters by more than '500 consumer data points' such as their credit rating and size of their mortgage"

(Angwin 2014, 75). The dangers brought about by this corporate-government collaboration raise serious concerns about the integrity of the US elections, especially when one considers the point of view that the electoral college has enabled the votes of certain states to, in a sense, carry far more weight than that of another. What is more:

> Guess who buys Aristotle's enriched data? Politicians, who are sometimes using government money. Aristotle crows that 'every U.S. President—Democrat and Republican—from Reagan through Obama, has used Aristotle products and/or services…' In fact, an intrepid 2012 thesis by a Harvard undergraduate… found that fifty-one members of the U.S. House of Representatives bought data from Aristotle using some of their congressional allowances, allowing them to identify their constituents by the age of their children, whether they subscribe to religious magazines, or if they have a hunting license. (Angwin 2014, 74)

Most people are baffled upon hearing this, yet it is completely legal and occurs more and more every year. In turn, the integrity of American elections and bipartisan politics—areas already under harsh scrutiny, and for good reason—are thrust into an even more precarious environment. Imagine the impact this plethora of voter data, when coupled with the droves of consumer data, could have when the next cycle of redistricting takes place in 2020; the opportunity for gerrymandering would be greatly increased and this data would technically allow it to be conducted without clearly violating the Voting Rights Act. In other words, come 2020, state politicians could gerrymander district lines without explicitly showing favor to a given party, but instead by encapsulating within their district the largest concentrations of people whose hundreds of 'consumer data points' correlate to a strong likelihood of voting for one or

more specific candidates. The idea of aggregated consumer data points correlating to a specific political party is by no means an exact science, yet it is a game of numbers that often proves itself to be correct in significant quantities. Thus, as the trend continues to grow, congressional districts—the building blocks on which our democracy rests—may be so analytically manipulated as to make true electoral competiveness an abnormality. For evidence of this growing development, one need not look further than states for whom levels of gerrymandering are already extreme, such as Pennsylvania and North Carolina:

> In the election of 2012, Barack Obama won the state of Pennsylvania with 52 percent of the vote. Democratic House candidates won 51 percent of the vote. But Democratic House candidates won only 28 percent of the state's seats. In North Carolina, Democratic House candidates won 50.6 percent of the vote, but Republicans seized 9 of the 13 congressional seats. By 2014, they would have 10. The list goes on. (Wagner 2016, 2)

The greatest testament to the significant impact mass data analysis will have during the next redistricting cycle perhaps lies in the degree of influence this same process had in the previous cycles. After all, even though the technology behind data collection has grown exponentially in recent years, the general theory of compiling large amounts of data to make voter predictions has been around long before computers. That being said, with the proliferation of computing technology, "fancy pencils… parchment sheets and desks covered with papers have given way over the last two redistricting cycles to very powerful computer programs" (Daley 2016, 104). Of all these computer programs, the most effective and widely used is a program called *Maptitude*. Maptitude is an advanced data-analysis software specifically designed for redistricting. It is a product of the Caliper Corporation, a company just 30 years old whose

executives shrewdly recognized the gains they stood to make if they could make quality redistricting software affordable. Whereas such software existed even as early as the late 1980s, it "then priced between $500,000 and $1 million," greatly "beyond the reach of most state legislatures" (Daley 2016, 112). Today, Caliper can license Maptitude's complete services for less than $5000.[5] Building upon this, while Maptitude data analysis provides one with the platform to favorably redistrict, it is the statistical wunderkinds hired to operate this software that truly bring about the algorithmic magic. One of these gifted statisticians, a man named William Desmond, was helpful enough to explain how this software works in laymen's terms.

William Desmond is a senior micro-targeting analyst for a specialized data broker called Strategic Telemetry. His past work has played a pivotal role in various elections, most notably his significant contribution to the Obama campaign in the 2008 presidential election. Desmond's entire professional life has been devoted to this type of political data analysis, evidenced well by the exceedingly blasé manner with which he describes the seemingly omnipotent predictions he can make with just a few clicks of his cursor. In a recent interview, Desmond explained how, "Maptitude comes preloaded with all the census data you could ever imagine, and some that you had no idea was even collected" (Daley 2016, 107). The software processes all this data and outputs discernible layers of information, the smallest of which is called a census block, which essentially corresponds to a city block. From here, the layers build upon themselves—census blocks form a census tract, these tracts create cities, and then counties, and ultimately entire congressional districts are laid out in predictive configurations that allow political campaigns to see their electorate in an entirely new light. If one desires even greater accuracy, simply plug in

[5] The complete price listings for all of Caliper Corporation's Maptitude services can be found at http://www.caliper.com/maptpric.htm

more data collected from third-parties. If done properly, one single census block can become a complex entity with its own array of layers—in a sense, increased data enables "the statistics [to] get even more granular: total population, male population, female population, white population, multirace[sic], mixed race, 'every other race,'" etc., all combine to reveal shockingly precise voter predictions (Daley 2016, 107). This software is exceedingly difficult to comprehend for the vast majority of people, but its brilliance lies in the fact that it can take incomprehensible terabytes and interpret them into projections simple enough for even a politician to understand—and this is where the danger lies.

The prevention of gerrymandering has arguably never faced a more daunting obstacle than advanced data software such as Maptitude. As the amount of purchasable 'consumer data points' about civilians continues to skyrocket, the ability to disguise discriminatory gerrymandering via complex software increases as well. What is more, according to William Desmond, the current state of political data mining has already put the Voting Rights Act in serious jeopardy. Desmond would be the first to tell you that, "[i]f your goal is… to create districts that will reliably perform for a specific party," and you are capable of using Maptitude "correctly, you can create an index that bounds enough of the right people, in the right way, to guarantee a result throughout the decade, no matter the overall direction of the electorate" (Daley 2016, 108-9). What is more, considering the exponential rate at which technology advances, one can only imagine what these types of data-analysis programs will be capable of even as early as 2020 when the next redistricting cycle occurs. Whereas most people are wholly unaware about the existence of the current technology, people in Desmond's field are keenly aware of its implications, and indeed they have speculated as to the remarkable capabilities that will be

available to well-funded political campaigns in the not-so-distant future. It is the belief of micro-targeting analysts such as Desmond and his peers that:

> 'Once people get really serious about trying to win state legislatures, it's going to be somebody building predictive models to tell you what that area is going to look like at some point in the future. Knowing the technology, that's where it easily could be. Now, it would take a huge investment in resources…' [but] that's the next political Moneyball[sic]. Now that the Citizens United decision has unleashed limitless dark money, it only takes one billionaire to write an eight-figure check and bet that his or her side could fine-tune a model so smart and intuitive that it locks in control of the House for another decade. An upfront investment like that would probably save money merely by taking potentially competitive races off the table for ten years. (Daley 2016, 118).

While the technological capabilities of the future and their potential impact in relation to gerrymandering are indeed daunting, for the sake of this argument, it is of vital importance to point out that the technology and its creators are not the issue. The true problem lies in the fact that the massive exchange of data and money between governments and the thousands of data brokers has enabled these technologies to inadvertently become a genuine threat to our democracy. These technologies have essentially been weaponized by the limitless ammunition that is available civilian data. What is more, whereas a significant amount of this data is made available by brokers seeking a profit, an equally substantial amount of information is being sold by government entities whose general obligation is to the people, not shareholders. This symbiotic relationship between the government and private data firms marginalizes the privacy of civilians who have no choice but to disclose their information if they want to be functional

members of our society. What is more, for the data brokers themselves, this merely represents the tip of the iceberg when it comes to the numerous, inconceivable ways in which they secretly collect information about you.

A key factor to the growth of personal data as a precious commodity has been the rise of the internet. Nearly every single online action conducted by an individual is of worth to one company or another. In a sense, while the internet is a public domain many people believe to be free (although internet is not a basic utility), participating in the "free" services provided by the internet means an unwritten agreement that the actions and information divulged online is a commodity that one no longer owns. "Personal data is the new oil of the Internet and the new currency of the digital world" (Angwin 2014, 71). The ways in which this personal data can be extrapolated from the digital world are both wide-ranging and highly complex, and data broker giants such as Acxiom have literally boiled this extrapolation down to a science—a science responsible for "the growth of a multibillion dollar industry that operates in the shadows with virtually no oversight" (Kroft 2014, 1).

The titans of this industry are companies like Acxiom, Experian and Alliance Data Systems' subsidiary, Epsilon. Despite having a combined market capitalization of nearly $30 billion[6], these same companies were once federally investigated and subsequently described by Jay Rockefeller, former chairman of the Senate Commerce Committee, as "the dark underside of American life… in which people make a lot of money and cause people to suffer even more" (Bachman 2013, 1). Rockefeller's criticism stemmed not only from the way in which these companies profit at the expense of the American people, but also from the secretive manner with

[6] According to *Yahoo Finance* as of 2017, Alliance Data Systems has a market cap of $12.2 billion, Acxiom has a market cap of $2.29 billion, and Experian has a market cap of $14.74 billion, all of which combines for a staggering $29.23 billion.

which they operate. According to Rockefeller during this 2013-2014 investigation, these companies were allegedly “stonewalling” him, refusing to cooperate and hand over data or relevant information about how their data-mining process works (Kroft 2014, 4). That being said, one of the big three, Acxiom, recently chose to make somewhat of a concession, offering the public a slight window into how this ‘dark underside of American life’ actually works—their intention was to gain positive PR, yet the result was not quite what they desired.

While companies like Acxiom routinely collaborate with government entities to compile information about individuals, the greatest resource at their disposal is online tracking via HTTP cookies. Cookies came about with the rise of the internet, and while the true way in which they function is rather complicated, the service they provide enables every website a user visits to autonomously install small pieces data—or cookies—on the user’s browser. If you continue to use the same browser that the cookies were initially installed on, these cookies will then track your online activity long after you have left the site from which they came, and third parties with authorization from that site can observe you via these cookies. This innovation represented a revolutionary step for online advertisements in the early 2000s, and today cookies have become the essential lifeblood for this industry. When people first discovered what cookies were capable of in the late 1990s, as well as how they were being used by more and more advertisers, there was understandably a fair amount of outrage. Many people felt their rights had been violated, and by 2000 “a federal class action suit was brought against the online advertising company DoubleClick, alleging that its installation of cookies on the computers of website visitors was violating laws that limit wiretapping, hacking, and electronic surveillance” (Angwin 2014, 65). In what seems to be somewhat of a rare occurrence, judicial oversight stepped in and agreed with

the concerns of the people, ultimately deciding this was indeed a violation of Fourth Amendment rights.

Yet, after an appeal was filed, the typical perspective of the courts in regard to online surveillance seemed to return, and a judge from an appellate court in the Southern District of New York found that:

> [T]he DoubleClick-affiliated Websites are 'parties to the communication[s]' from plaintiffs and have given sufficient consent to DoubleClick to intercept them… Her ruling amounted to a free pass for corporate Internet surveillance: when a person visits a website, the website is free to invite others to secretly wiretap the visitor. (Angwin 2014, 67)

Despite being relatively unknown, this court decision was one of the most critical rulings in recent history as it relates to the internet. It essentially laid the foundation for online advertising, an industry valued at $125.82 billion in 2014 with projections to be worth an estimated $220.38 billion by 2019.[7] This profitable industry hinges upon cookie tracking, and it is companies like Acxiom that have mastered the science of mining them throughout the digital world. This enables Acxiom to compile massive aggregations of data that can then be deciphered through macro placement algorithms to reveal patterns such as purchasing trends, online betting habits, voter tendencies, etc. It is through this scientific process that data brokers have found great success. Marketing firms and businesses themselves purchase subsets of data from Acxiom at a great cost because the insight they gain can ultimately pay dividends in the long-term. What is more, social-networking corporations like Facebook and Twitter have paid Acxiom huge sums

[7] Statistics provided by marketsandmarkets.com's report, "Online Advertising Market by Search Engine Marketing, Display Advertising, Classifieds, Mobile, Video, Lead Generation, Rich Media - Global Advancements, Forecasts & Analysis (2014 - 2019)" http://www.marketsandmarkets.com/PressReleases/online-advertising.asp

of money simply to learn the ways in which they can enhance and integrate their own HTTP cookie tracking systems (Angwin 2014, 70). Although this exchange required these social-networking giants to pay millions of dollars, the millions of users that visit their websites every day made the purchase a simple decision from an economic perspective.

Thus, these invasive tracking methods conceived by big data companies have now been put in the hands of some of the largest and most powerful tech corporations in the world, subsequently enabling the overall size of the data dragnet to expand at an exponential rate. The implications of this development are very significant for average citizens whose real lives are being surveilled through the digital footprints they unknowingly leave behind. Although some people choose to ignore the dangers brought about by this issue, the truth of the matter is that it places our general rights to privacy on a slippery slope—privacy both in the digital sense and the physical sense. Preventing this erosion of privacy will not be without struggle and effort from numerous parties, yet attempting to reclaim it after it has been lost will almost certainly be futile. In the end, one of the strongest lines of defense for American civil liberties is a coalescence of the people themselves, and unless enough of them can truly appreciate the risks to their privacy brought about by wide scale data mining, it is hard to imagine that these critical rights will not be further undermined.

Chapter Five: The Inherent Risks Created by an Industry That Treats the Individual as Both the Product and the Consumer

While the data collection industry is creating jobs and helping numerous businesses advance and develop, it also comes with a high level of risk that calls for increased oversight and accountability. With any business that deals with sensitive information about people's lives, the risk of a security breach is immense. As one might expect, data collection companies have been hacked before and put people at risk who never even knew they were being watched. Building on this issue, it is critical to remember that data-collection firms do not simply collect swaths of internet activity, they "handle giant troves of sensitive personal information for many retailers, banks and other companies that deal directly with the public" (Sarno 2011). As these companies grow in number and size, they have increasingly become a popular target for hackers, a serious threat in today's world.

Making matters worse, while one would expect this industry to be characterized by high levels of supervision and transparency, minimal amounts of regulation and oversight actually create the exact opposite environment. The internet is the "wild west" of the digital world—lawless and nearly impossible to fully govern. While this enables vast amounts of crime in countless ways, we should not be so naïve as to think powerful corporations do not bend and often break the law as well in the quest for the almighty dollar. Yet, even when the improper collection of data by a corporation is discovered, the established punishments are so insignificant that corporate surveillance misconduct seems almost economically rational, albeit immoral. For example, three years ago Google "reached a $7 million settlement with thirty-seven states and the District of Columbia" because the company's *Street View* vehicles were not just collecting panoramic photos, they were gathering massive quantities of private data, "including email and

text messages, passwords and web histories," via unsecured Wi-Fi networks (Boghosian 2013, 100). Google has a market capitalization of almost 600 billion dollars. A seven-million-dollar punishment is not even a slap on the wrist—constituting less than two thousandths of one percent of Google's market cap—it is entirely irrelevant.

Children's Personal Data: Get Them While They're Young (and Maybe You'll Get Them for Life)

Another example regarding corporate surveillance misconduct and the lack of repercussions is the various ways in which children's information is collected. While specially catered advertisements are enticing generally, their effects are even more pervasive on the most impressionable members of society—children whose embrace for technology has increasingly begun at a younger age. Businesses like "McDonald's, the Walt Disney Company, and a host of other corporations" are keenly aware of this truth, and thus they "try to access children as early as possible by routinely engaging in deceptive, inherently exploitative marketing practices" (Boghosian 2013, 108). As insidious as this may sound, it is nothing short of brilliant in the way in which it grooms children to be lifelong patrons of a given company. Children are literally built to absorb information at a young age from the moment their hippocampus develops and concrete memories are made possible. This cognitive adaptation is one of the most essential parts of human development. It can enable children to become bilingual, it can train them to become talented musicians, and it can also lead them to unwittingly develop strong bonds with certain brands and products. The key to all of this is essentially the idea that children are unaware it is even happening—it is subliminal. And with enough reinforcement, these subliminal messages can become embedded into a child's thinking long after he or she has become an adult.

What is more, although children of today's generation are more technologically savvy than ever before, this intelligence does not simultaneously create an enhanced ability to

distinguish general content from sponsored content[8]. Sponsored content has become so firmly entrenched in the various mediums of American entertainment that it is often difficult to notice for adults, let alone children. Building on this point, whereas adults are relatively aware of the risks and causes of identity theft, inherently naïve children are not equipped with this same caution and they routinely divulge precious information like their name, date of birth, address, etc. It may seem hard to believe how "aggressive, all-too-clever techniques enable corporations to capture personal information from millions of children," but the real issue lies in the fact that "legal and regulatory protections have failed to keep pace with ever-changing technology and the methods used to target and expose children to corporate persuasion." (Boghosian 2013, 180).

The main safeguard for protecting the digital privacy rights of children is the Children's Online Privacy Protection Act of 1998 (COPPA) which deals most specifically in protections for children under age 13 (Federal Trade Commission). While this act was specifically designed to keep pace with the dynamic nature of the internet and amend itself accordingly, it has proven time and time again to be ineffective in the sense that it intervenes long after the psychological damage has been done. COPPA has been at the heart of many successful lawsuits claiming illegal corporate persuasion, but the penalties levied against wealthy corporate defendants are negligible whereas the persuasive effects on the children are irreversible. One of the most noteworthy examples of this problem can be found in a marketing scheme created by the McDonald's Corporation.

McDonald's tactics for successfully marketing to children have frankly been nothing short of pure genius in the past. They built playgrounds in their restaurants with the *PlayPlace*,

[8] Sponsored content is essentially "material in an online publication which resembles the publication's editorial content but is paid for by an advertiser and intended to promote the advertiser's product." This form of advertising has increasingly appeared in all mediums of entertainment.

their mascot is a clown and they are technically the largest distributor of toys in the world, by far. These ideas have brought untold amounts of business to the fast-food chain, as well as massive increases in American childhood obesity. In any event, one of the corporation's recent golden ideas to attract young consumers was through a game available on happymeal.com called 'McWorld'. The McDonald's Corporation allocated a large sum of money to create sophisticated 'advergames'—essentially online video games that attract children in various ways and incorporate McDonald's products throughout the game itself. The largest, most successful advergame was McWorld, McDonald's own virtual world geared towards children where one collects codes from happy meal boxes that, per the website[9], "unlock all kinds of cool stuff like exclusive accessories for your avatar or treehouse, interactive pets, or even events where your favorite movie, TV, or comic book characters may appear and play with you!" (Federal Trade Commission (FTC) 2012, 3). McWorld's success was largely due to the way in which it enabled children to create their own unique avatar which could play multiple games before the user had to enter personal information or purchase a Happy Meal. In this way, the addictive site hooked a large numbers of users before even gaining anything of real value to the corporation. Yet, soon after this stage of McWorld, the clever game reminds all non-members—kids that had created a free account that requires no input of personal information—that:

> "'[o]nly members can use Happy Meal codes to get special stuff!' The website not only encourages children to spend time playing in the McDonald's branded environment, but it also encourages them to purchase (or ask their parents to purchase) Happy Meals, create user accounts, and develop positive associations with Happy Meals. As McWorld loads on a child's computer, a Happy Meal box appears with the caption "Happiness." At

[9] The website and the game itself have since been taken down from the internet by McDonalds. However, the FTC report has a number of direct quotes from the former McWorld game, such as the one being referred to here.

least two games on the site—"Great Space Rescue" and "Suzi Van Zoom"—reward kids for collecting Happy Meals during gameplay." (FTC 2012, 3).

While the entire concept of McWorld may seem silly, it is disturbingly clever at its core, and in the eyes of the FTC it undoubtedly constitutes unfair and deceptive marketing practices. Making matters worse, these duplicitous marketing techniques that preyed on young, healthy and impressionable children were not even the reason the FTC ultimately investigated McWorld and quickly decided it was in violation of COPPA. Rather, it was the games "refer-a-friend" feature that finally brought about its demise. The "refer-a-friend" function of the game is actually an extremely common function among all digital games and apps. It basically asks the user to input one or more of his or her friend's email addresses or Facebook profiles in exchange for in-game rewards. The reward for the company that owns the game is far more valuable. It now has the ability to not only reach out to more prospective users, but to do so in a personalized way that makes it seem as if the offer is being conducted by the friend—this greatly increases the likelihood of the offer being accepted, and indeed they were. Thus, the number of children using the game proliferated to such a point that parents eventually took notice, nearly all of whom hated the idea of their children playing McDonald's-sponsored videogames and never consented to having their children's emails or social media profiles accessible by the McDonalds Corporation. From there, the FTC conducted a report deeming the entire McWorld site unlawful based most specifically on the lack of "verifiable parental consent for the collection, use or disclosure of personal information from children" (FTC 2012, 4).

The example provided by McWorld is a compelling one for several reasons, and it is important to mention that it is just one of many similarly deceptive corporate marketing schemes aimed at children. In fact, along with McDonald's website geared towards children, four other

major corporations' websites— "General Mills, Inc. and its TrixWorld.com and ReesesPuffs.com sites; Turner Broadcasting System's CartoonNetwork.com; Viacom Inc.'s Nick.com site; and Doctor's Associates Inc. and its SubwayKids.com site—were charged with circumventing the Children's Online Privacy Protection Act of 1998" (Boghosian 2013, 184). Despite this charge by the FTC, these corporate giants suffered no real consequences beyond being forced to change their websites to legally align with COPPA or risk financial punishments. What is more, whereas most businesses stand to suffer greatly if they are forced to pay legal recompense, for corporations like McDonald's, TBS (owned by Time Warner) and Viacom, such punishments are not even taken seriously. In fact, it is likely that the officials in charge of the FTC considered the immense costs they themselves would have been forced to spend if they attempted to take these corporations to court, all of whom have the most expensive legal teams money can buy on retainer year-round. In the end, these corporate giants who lie at the core of the American economy gained a major victory, especially when one considers the invaluable amount of influence they gained over young, future consumers before being 'forced' to change their ways. As a whole, the data collection and deceptive marketing exhibited by these corporations provides a strong example of the way in which digital privacy laws struggle to keep pace with technological advances, and how when this gap is created, it is greatly exploited for profit at the expense of consumers long before judicial oversight can investigate and ultimately put a stop to it.

One can quite easily imagine the various ways in which internet advertisements influence children. However, bearing in mind kids' preoccupation with smartphone and tablet games, many people, including parents, fail to realize that apps "are also insidious trackers able to pinpoint and store a child's physical location, the telephone numbers of their friends, and more"

(Boghosian 2013, 192). Geo-location tracking is a surprisingly common feature for mobile Apps geared towards children, and these same children, as well as their parents, typically have no idea that they have enabled it when they choose to download and play the newest "free" game available in the App Store. This is not a minor occurrence; in fact, Angry Birds, an App that has been downloaded over 2 billion times, discretely mentions in its privacy policy that it has the right to not only track users' location, but also store the aggregated data for independent use (Ball 2014, 1). Dragnets of personal data such as this are of great value to many businesses, and thus it is not surprising that only a minute fraction of popular children's apps disclose their data collection polices at all.[10] Unlike the corporate examples mentioned above, the tablet and mobile app "industry's growth is fueled largely by small businesses, first-time developers, and even high school students without access to either legal counsel or privacy experts" (Boghosian 2013, 190-1). Whereas large corporations bend digital privacy laws knowing they stand to gain more than they could ultimately lose, Silicon Valley tech startups often break these same rules without even knowing they exist.

These small, poorly regulated companies routinely vend users' personal data to "third parties, such as advertising networks or analytics companies," and this is typically done simply to stay in business—despite the media attention and massive success some tech startups have had, some reports estimate upwards of 90% fail[11] (Boghosian 2012, 191). With this in mind, it is not hard to believe how the people in charge of these small companies would act recklessly with

[10] According to a 2012 study of 400 popular children's apps (200 Apple, 200 Android) conducted by the Federal Trade Commission: "the Apple app promotion pages…provided almost no information on individual developers' data collection and sharing practices. Similarly, the Android app promotion pages that staff examined provided little information other than the mandatory "permissions." Only three (1.5%) of the 200 Android apps even attempted to convey information about the purpose for the "permissions" (Federal Trade Commission 2012).

[11] According to the article "Silicon Valley's culture of failure … and 'the walking dead' it leaves behind" written by Rory Carroll of *The Guardian*, some statistically based estimates put the rate of startup failure as high as 90%. More conservative estimates report between 75-85% of all Silicon Valley startups fail, with the typical trend for companies being bankruptcy approximately 20 months after their last financing round.

users' personal information in exchange for profit, especially if it extended the amount of time their business could survive or opened the door for new investments. What is more, this same carelessness reveals itself in these companies' firewalls and basic security systems, or lack thereof. Large droves of users' personal information represent a goldmine for professional hackers who can then sell this information on the black market. This is quickly becoming one of the leading causes of identity theft, and it happens to tech startups far more often than one might think. For example, one of the more well-known game designer companies, *RockYou Inc.*, began enjoying considerable amounts of success after a handful of its apps gained immense popularity. However, this same company never decided to update its firewall, and eventually RockYou's "inadequate security resulted in hackers gaining access to the personal data of 32 million users," ultimately leading to an investigation by the FTC that subsequently revealed they were in violation of "COPPA by knowingly gathering the email addresses and passwords of approximately 179,000 children without first obtaining their parents' consent." (Boghosian 2012, 292). This specific breach in privacy was severe, but similar examples happen all the time.

All of these cases, both corporate and startup, suggest that there is a dire need to reform policies governing data collection and digital surveillance—especially as it relates to children—yet efforts to do so by advocacy groups have proven to be ineffective. That is not to say that reforms have not been made to pieces of legislation such as COPPA. Rather, these reforms are often minor and they take far too much time to be established. Corporations, on the other hand, are constantly on the forefront of using new technologies to continue collecting personal data in increasingly effective ways. By the time these tactics are identified and possibly deemed illegal, these same companies will be ten steps ahead, already looking forward to even more advanced ways to achieve their goal. Until this is fully understood and radical changes are brought about,

preventing these continued breaches in privacy that put both adult and children at risk will inevitably continue to occur. This truth lies not in some nefarious corporate plot, but rather in the basic principles of Moore's Law. The exponential advancement of technology is an unstoppable force. Pieces of legislation similar to COPPA need to stop trying to work in opposition to this fact and instead be theorized with its principles shaping every aspect. Despite all the evidence suggesting how imperative these changes are becoming, attempts for reform have been thwarted by a suppressive political environment bolstered by the power of corporate-government collaboration.

However, while there are undoubtedly points to be made about the way in which corporate-government collaboration stymies vital reforms, is there not anything that can be done by the citizens themselves to prevent the pervasive surveillance, collection and vending of their own personal data? The American people elect their representatives with the hope that these officials will then carry out the collective will of their respective constituencies, yet does this subsequently mean that the will of the actual constituent no longer matters? In other words, are we as American citizens helpless in the protection of our own personal data—is there nothing that we can do, as individuals, to defend ourselves?

Opting Out: The Futility of Trying to Protect Your Personal Data Without Immense Sacrifice

One of the greatest obstacles average citizens face in in trying to prevent the collection of their personal data is the fact that so many of the government agencies and corporations that collect this data also provide vital services that nearly every American has used at one point in his or her life. This basic insight ties into one of the larger observations of this entire thesis, essentially the idea that the enticing technological advances created by government-corporate collaboration make our lives far easier and more manageable, yet simultaneously force us to

develop immense dependence on these same technologies. This dependence is unquestionably irreversible, and thus the valuable information we routinely disclose to use these ‘free’ services is the price we pay—but does it have to be this way? Is there no way to enjoy the comforts brought about by technology without subsequently eroding our privacy and basic freedoms? Unfortunately, while there are people and companies in the United States attempting to offer this service, the reality of the situation is that our dependence on corporate-government technological services has become so great that opting out of this relationship is inconvenient and troublesome to a point that largely renders the option unrealistic.

While there are thousands of companies and government agencies that have profited from civilians’ overwhelming reliance on their services, the best examples to be analyzed can be found in the handful of corporate giants who essentially laid the framework for this entire relationship—corporations that, if they were to hypothetically disappear tomorrow, would throw the entire American economy into utter disarray. Of all the examples of major companies that play a role in data collection and vending, there is perhaps none greater than Google—a company with a market cap hovering just below $600 billion whose name has essentially been converted into a verb known the world over. The advertising services offered by Google account for the vast majority of its income, and all of these advertisements are specifically catered to individual web users based on their compiled search queries and web history. The specific way in which this process works is highly elaborate, essentially using peoples’ IP addresses as a tracking module that links them to every search query and actual webpage they visit via google.com. For the sake of remaining clear and to the point, an actual explanation of the science behind Google’s tracking-advertisement technology is unnecessary. That being said, it is highly likely you have noticed the peculiar way in which advertisements on non-Google websites

sometimes appear to be offering products that you recently investigated while using Google. To make this more clear, I will offer a brief personal example that actually relates to my construction of this thesis.

After doing a considerable amount of research on Maptitude via Google searches to bolster my chapter on political data mining, I noticed just one day later that a European sports website I routinely visit—http://www.fullmatchesandshows.com—now appeared to be advertising Caliper Corporation's Maptitude services on the front page. Based solely on two days of considerable research I conducted regarding Maptitude, Google's algorithms predicted I would be a likely candidate to purchase Maptitude's services, and thus one of my most frequented websites that happens to be contracted by Google's advertising services is now providing me with a poignant example of how my web searches shape the products being advertised to me online. An even more peculiar example can be identified through the fact that I passionately watch European soccer year-round, a sport that is watched online in this country primarily by Spanish-speaking people. Thanks to Google's ad-tracking services, I now routinely find myself watching video advertisements completely in Spanish before any video I watch on YouTube, ESPN, Facebook, etc. Google tracks countless terabytes of data every day to algorithmically identify trends that can help companies advertise their products more effectively online. Yet, according to Google's data, the large majority of people who love to watch soccer in this country speak Spanish—despite the fact that I do not speak Spanish, my digital footprint tells a different story, and thus I have no choice but to either stop using Google, or simply get used to advertisements in Spanish. This illustrates one of the largest faults of the data collection industry—essentially the idea that much of the data collected from people is routinely

misinterpreted, and even when these false assumptions are identified by the user, the same user has no ability to correct these errors.

As stated before, the only other legitimate option a user has in this situation is to refrain from using Google's highly convenient web services—the same goes for the services offered by Bing, Yahoo, Ask, etc.—and instead try and use a search engine that does not collect the data of everyone who uses it. For those few people who are genuinely trying to break their dependence on Google because of issues with data collection, the best search engine that can still satisfy their search needs is a small search engine called DuckDuckGo. DuckDuckGo has an extensive policy regarding data collection on the privacy section of their website, but their homepage accurately sums it up with three basic statements: "1) We don't store your personal information. 2) We don't follow you around with ads. 3) We don't track you, including private browsing mode[12]" (DuckDuckGo.com). Having established the basic way in which DuckDuckGo protects user privacy, one will now see all the subtle sacrifices that come with this decision, essentially the multitude of convenient services provided by Google that often are not even recognized by users until they are no longer functioning.

Of all the sacrifices that come with a departure from Google, the largest and most readily apparent is the loss of Google's flawless memory and search suggestions, all of which are based on the stored information from every previous search a user has made. In other words, when you Google something basic, such as 'good food near me,' Google will provide you with a complex list of quality restaurants based on all available online reviews, simultaneously listing the

[12] Many people have an incorrect understanding about how common web browsers' private browsing or incognito mode works. They believe that once the function is turned on, their data is no longer tracked or collected. Julia Angwin does well in summing up the reality of these privacy modes, stating: "Not to put too fine a point on it, but Incognito mode [or Private Browsing mode] is built for one thing: browsing porn. It removes the cookies with porn names from your computer so your spouse won't see. The website and its advertisers on those sites still know you were there" (Angwin 2014, 254).

specific distance each restaurant is relative to you down to a tenth of a mile. If you put this same search into DuckDuckGo—assuming you have not allowed DuckDuckGo to track your location, one of the most invasive functions people concerned about data collection take issue with—then the search engine will simply give you a list of websites specifically designed to find good restaurants near your location, all of which collect and store your data, thereby defeating the purpose of using DuckDuckGo in the first place.

What is more, people often fail to realize just how helpful Google's stored memory is in terms of eliminating the need for the user to remember or bookmark websites that they frequently visit. Once a user makes the transition to DuckDuckGo, he or she must consider the fact that their stored web memory and basic web history no longer exist. Once again relating the argument to my personal experiences creating this thesis, if I was not able to check my web history and easily revisit sites I previously used to learn about a given topic, I would have literally been forced to bookmark hundreds of websites, coordinating all of them with precise tags that would enable me to remember what specific information I gleaned from them. This would be tedious to say the least, causing me more than enough of an inconvenience to ultimately abandon any valiant effort to stand up to data collection at the individual level. Building on this point of basic convenience, identical searches are far more helpful and thorough when done through Google rather than DuckDuckGo. While this is a relatively obvious statement considering Google is the largest search engine in the world, it is important to mention that the comparative difference in search results is massive. For example, a basic search of 'Union College' yielded just over 100 results in DuckDuckGo, the same search yields approximately 22,300,000 when done through Google. Clearly this does not mean a user cannot find what he or she is looking for when using DuckDuckGo, but it does reveal the profound

difference in scope between search engines that store user data, and search engines that do not. In the end, DuckDuckGo is a legitimate alternative to search engines like Google that store your personal data, but it is far less easy to use, and it still represents just one piece of the puzzle. To genuinely achieve freedom from Google data collection, one must delete his or her Gmail—something not even feasible for college students and employees[13]—one must no longer use Google Maps, or Google Docs, or Google Drive, etc. Remember, despite Google being the biggest company routinely profiting from the collection of personal data, they are still just one of the thousands of businesses that perpetuate this issue, ultimately making the idea of individually opting out less and less feasible.

Another corporate giant that vends user data in countless ways often unbeknownst to the user is Facebook, the most popular social media website that boasts over 1.23 billion active users to date. Facebook is an intriguing example because its services are completely free, yet it still tries to convey to users the idea that they have complete control over their information, especially when it comes to who can and cannot see this information. Just to be clear from the outset, this is simply not true anymore. While this may have been the case way back when the company first began—these were the days when having a Facebook meant the user was associated with an elite university via his or her .edu email—Facebook itself has greatly evolved since it was founded in 2004, and in many ways it is an entirely new entity when compared to its original format. Since the time in which the company began pushing the former social media giant, MySpace, into relative obscurity, "Facebook has… repeatedly abused users' trust," changing its privacy policies hundreds of times each year to a point in which users had "to dig

[13] According to Time Inc.'s article, "Google and Microsoft: The Battle Over College E-Mail," nearly every single college and university not just in the United States, but the entire world, uses the email services of either Google or Microsoft Outlook, both of which legally collect all emails for independent use, i.e. data mining.

deep in its menus to reclaim control of [their] data" (Angwin 2014, 328). What is more, there have been actual lawsuits brought against Facebook when their abuse of user data led to serious issues such as when they created a program called Beacon in 2007 that shared people's online purchases with everyone they were connected to despite not actually informing the purchaser. This led to countless incidents, such as when a man bought a diamond ring for his wife on overstock.com without being notified "that his purchase was automatically posted to all 720 of his friends, including his wife. In 2009, Facebook agreed to pay $9.5 million to settle a class action lawsuit over Beacon and to shut down the service" (Angwin 2014, 328). One would have hoped this would be the end of the corporation's efforts to convert its users into literal advertisements, yet all it really did was send the people in charge of concept back to the drawing board. Lo and behold:

> Instead of dropping the idea of turning its users into free product advertisements… Facebook revived it in 2011 with a product called Sponsored Stories that allowed advertisers to buy the rights to republish a user's post and display it to that user's friends as an advertisement. In 2013, Facebook agreed to pay $20 million to settle a class action lawsuit over Sponsored Stories. But rather than do away with the product, Facebook simply added new language to its privacy policy to make it clear to users that Facebook has the right to use its customers' images and posts in advertisements. In other words, Facebook has been waging a six-year war to be able to turn its users' conversations into ads that it can sell. (Google has since joined the fray, launching a similar program called "shared endorsements" that will turn users' reviews, ratings, and comments into advertisements.) (Angwin 2014, 327-329)

Corporations like Facebook and Google offer some of the most widely used web services in the world, and as this information shows, despite their attempts to lead users into believing their data is not routinely sold at a profit, these statements cannot be further from the truth. Yet, in the end, while it is highly inconvenient to abstain from using the services provided by these companies, that does not mean it is impossible. But what options do individuals have if they want to opt out of having their information collected by data brokers? This is arguably an even more insidious way by which user data is collected, stored, sold, and often misinterpreted. While there are several ways in which an individual can safeguard his or her online data, the most effective strategy is through purchasing and installing comprehensive software that blocks the equally comprehensive software used by companies to track one's digital footprint. Of all the different types of software available today, the two most effective examples are Adblock Plus and NoScript. Adblock Plus is most commonly—though not exclusively—used with the web browser, FireFox, and it essentially does exactly what it sounds like it would, block advertisements from appearing. However, its true brilliance lies in the fact that, unlike other ad blockers that merely put the advertisement out of sight, Adblock Plus disallows advertisers from dropping any HTTP tracking cookies on a user's computer, essentially rendering all online advertisements useless while also preventing data brokers from spying on a user's future web activity. Adblock Plus is actually an excellent tool for people interested in heightening the security of their personal information on the internet. That being said, it essentially equates to a nuclear option in that it opts out of online advertisement data collection by completely opting out of online advertising itself, something that plenty of people consider a very helpful, convenient resource that they would not want to give up for just a minor victory in the overall war against

data mining. NoScript, on the other hand, represents a more interesting example in that it fundamentally transforms the way in which one uses the internet after being installed.

NoScript is an even more comprehensive piece of software than Adblock Plus, and thus its effects on a user's web experience are far more profound. After installation, NoScript essentially disallows executable web content from sources like JavaScript, Java, Silverlight, Flash and many other application frameworks that essentially function as the fuel with which any given website can run. The issue with NoScript is similar to the issue with Adblock Plus in that its effectiveness lies in its almost nuclear approach to preventing data collection. For example, this software prevents the functioning of JavaScript, a technology at the very foundation of the World Wide Web that "can be used to load all sorts of tracking technology, including cookies, and can even be used to monitor how you move your mouse on the page. But it also has a lot of legitimate uses" (Angwin 2014, 355).

In truth, saying that JavaScript 'also has a lot of legitimate uses' is quite an understatement for people who have no prior familiarity with this technology—JavaScript having legitimate uses in relation to the internet is the equivalent of saying gasoline has legitimate uses in relation to automobiles—the latter relies on the former to function. JavaScript has been a fundamental building block of websites since the nascent stages of the internet, and today internet statistics report that 94.4% of all websites use JavaScript.[14] Not surprisingly, within this 94.4% is essentially every website you have ever visited—the most popular include sites like Google.com, Youtube.com, Twitter.com, Facebook.com, Linkedin.com, Yahoo.com, Wikipedia.com, Amazon.com, Baidu.com, etc. To make matters simpler, one would have a substantially harder time finding a website that does not use JavaScript as compared to finding

[14] According to W3Techs.com reliable internet usage statistics on Client-side Languages, Usage of JavaScript for websites is approximately 94.4%. https://w3techs.com/technologies/details/cp-javascript/all/all

one that does. With this point established, one can more fully appreciate the nuclear aspect of what implementing NoScript entails—in a sense, it is protecting a user's personal data by closing him or her off from 94.4% of the entire internet. It would be misleading not to mention that NoScript enables users to allow the functioning of JavaScript and other codes on a website to website basis, but the entire point of preventing data vending from third-parties is subsequently defeated in that nearly every single website in existence today cannot function without these scripts. Thus, to truly opt out from the pervasive online collection and vending of personal data is virtually impossible unless one chooses to opt out from the internet entirely, something most people in the United States cannot even seriously consider.

While it may seem unfair to claim abstention from the internet is unrealistic in American society, especially if you pose this question to senior citizens, for people of my generation the internet has undoubtedly become a societal imperative growing in importance every year. Clay Shirkey, a philosopher whose recent works analyze the effects of the internet on Western Civilization, summed it up best when he wrote:

> The Internet has so permeated our lives that its influence is becoming impossible to see. Imagining today minus the Net is as content-free an exercise as imagining London in the 1840s with no steam power, New York in the 1930s with no elevators, or L.A. in the 1970s with no cars. After a while, the trellis so shapes the vine that you can't separate the two. (Snow 2016, 3)

This insightful point ties well into the basic argument made above regarding just how problematic it has become for someone to protect his or her personal data at an individual level. To successfully do so would ultimately eliminate the practicality of using the internet in the first place, and as Shirkey suggests, in this day and age, completely opting out of the internet is the

equivalent of marginalizing oneself to the periphery of American society. The way in which corporate America profits through treating civilians as both the product and the consumer simply cannot be stopped by the civilians themselves. One of the greatest concerns surrounding this issue is the fact that millions of Americans are still unaware any of this is even taking place. These people stand to suffer the most in that they are unwittingly perpetuating the problem because nobody has ever explained to them the countless ways in which corporate-government collaboration exploits their personal information. This is not to place blame on uninformed citizens or claim widespread negligence; after all, the only real way in which data collection is required to be disclosed to its subjects is via privacy policies and 'Do you Accept' updates. We have all encountered these absurdly long disclaimers carefully crafted by lawyers to include subtle clauses with immense implications amid countless pages of drawn out legal jargon—all of which is generally there to give readers a headache, thereby leading them to click agree so they can get on with their lives. In the end, we as individuals are simply not equipped with enough resources to protect ourselves from corporate-government surveillance, and just as we rely on government for protection in other aspects of society, we may need to rely on it now more than ever when it comes to maintaining our right to privacy in an increasingly digital world.

Yet, as has been shown through countless examples of corporate success, digital privacy laws as they currently stand are more or less an anachronism when one truly considers the rate at which technology is advancing. Legitimate resolutions to this problem need to come through legislation, and this legislation needs to be shaped with an acceptance that the rate of technological advancement is unpredictable and in need of regular examination in relation to the way in which it can be unleashed at the expense of American citizens. However, while these theories are viable options to resolve this growing dilemma, they are rarely mentioned by U. S.

elected officials save for a select few who do not care if they are in the unpopular minority. At first blush, it may seem odd that more men and women in Congress are not advocating for increased digital privacy laws to protect American citizens. However, when faced with the risk of being labeled "unpatriotic" for damaging our efforts in the war against terror, and perhaps more importantly at risk of biting the corporate hand that feeds significant election campaign and lobbying dollars into the coffers of these same officials, the reticence to tackle this issue on behalf of a constituent population that is largely unaware of the threat to its privacy rights may not seem so odd after all. One suspects that it may take a large-scale catastrophic event affecting a significant percent of the electorate to spur meaningful action in this area. Perhaps the spying files of the Central Intelligence Agency recently disclosed by WikiLeaks will be the catalyst; however, given the entrenched nature of the symbiotic relationship between the government and corporate America in this regard, one should not be too optimistic.

The Unchecked Power of Corporate-Government Collaboration: How the Enhanced Surveillance State Perpetuates Itself

The deep-rooted, mutually beneficial relationship between corporations and government not only functions to advance the interests of both groups, it creates a political landscape where political reform is discouraged and repressed in numerous aspects of American society. While appearing conspiratorial and collusive on the surface, the actual logic behind this arrangement is rather simple. With the growth in corporate power over the past few decades, it would be rational to believe that the federal government should curb the amount of civilian data being collected by these entities. Yet, when this same data is of vital importance to the government as well, and corporations have better technology and access to the data, the original logic becomes flawed—why would the government push for policies that limit its ability to pursue its anti-terrorism agenda, which it believes is of vital importance? Conversely, with a shared interest in an

intangible commodity for different reasons, it is only practical that the two entities have used each other to advance their respective personal agendas. What is more, those in elected positions to defend civil liberties within the government are often bolstered by corporate lobbying in their path towards winning the position in the first place (Schneier 2013). A primary concern of people in office is gaining reelection—thus, to push for reform on the issue of data collection would almost certainly weaken one's chances for reelection, thereby representing an illogical political decision.

The combination of all these factors creates an environment in which powerful, well-funded lobbyists disseminate misleading and inaccurate ideas to weaken reform movements. Of all the flawed ideas repeatedly forced upon American society by the heads of business and government, one of the most damaging of all has been the basic principle that surveillance makes us safer. In fact, the inundation of advanced surveillance technology has actually endangered the populace in a number of ways. First and foremost, the prevailing assumption that more cameras correlates to less crime is statistically incorrect. In fact, while "cities invest hundreds of millions of dollars in surveillance cameras" without "evidence…that they deter crime," the subsequent waste of resources actually opens the door for even more detrimental crime (Boghosian 2013, 403). This underlies the inherently flawed logic behind our nation's prioritization of crime. While millions of Americans detest those involved in urban violence fueled by years of racial tension and institutional impoverishment, people have already seemed to stop caring that not one single banker was arrested for defrauding millions of investors, and repossessing the homes of millions of American families in a financial crisis that cost the U.S. over 10 trillion dollars (The Cost of the Crisis 2012). As "the war on terror" sank enormous capital into ineffective domestic surveillance, "[t]he investigation and prosecution of white-collar crime plummeted, a boon to the

Wall Street plunderings [sic] that helped create the greatest economic crisis in America since the 1930s" (Boghosian 2013, 402). Thus, while most people seem to ignore this fact, the political environment created by corporate and political elites has conversely functioned to silence anyone critical of the "war on terror" and its damaging, long-term implications. Despite all the evidence suggesting increased investment in surveillance technology fails to demonstrably increase national security while benefiting the wealthy and powerful, the corporate controlled media created "the linkage of national identity to national security… to create a climate in which dissent and opposition became equated with anti-Americanism" (Hutcheson 2004, 47). In the end, corporate and government interests in data collection are not the sole causes for the enhanced American surveillance state—we as a population must also bear some measure of responsibility for failing to protect against policies and activities which threatened our fundamental rights and freedoms.

European Data Protection: A World of Difference

Whereas the American surveillance state's growth has been enabled through a legislative disregard for digital privacy, the European model offers an intriguing counterexample in that both the views of the people and the role of the state are fundamentally different than our own. Although American legislation has been put in place to protect digital privacy, its enforcement lacks coordination and its overall scope does not share the European view that citizens deserve total control over their personal data at an individual level, regardless of the implications. American privacy laws have historically been strong and similar to those of the European Union in that all citizens have an implicit right to privacy. However, unlike the European Council, the American government has not effectively extended these protections of

individual privacy into the rapidly expanding digital world, nor has it seemingly taken the position that such protections are even warranted.

Despite the fact that we all now live in this digital world to varying degrees, it is the apparent belief of the federal government that this digital world is not explicitly within its jurisdiction, and thus undeserving of the same regulation. This same logic applies itself conversely to what federal agencies like the NSA and the CIA feel they are permitted to do through this unregulated medium. In other words, the federal government routinely uses this digital realm to achieve certain goals that would otherwise be illegal, or impossible, if carried out by conventional means. As the research shows, this general perspective has been embraced and capitalized upon by countless players in corporate America as well, subsequently expanding the scope of the internet along with our global dependence on it. This has led to countless breaches of innocent people's privacy, and it seems that only when these breaches involve very public matters or significant criminal acts that the government sees no choice but to intervene. This is the fatal flaw in the American model—legislative efforts…[are] mounted in response to specific and egregious harms," yet [a]dvancing privacy as a matter of individual rights across the corporate sector generally has little legislative or regulatory traction" (Bamberger & Mulligan 2015, 444). Whereas the American model takes a shortsighted, reactionary approach to digital privacy, the European model takes a completely different approach, instead opting to be the primary guardian for digital privacy rights, most specifically at the individual level. Unlike its American counterpart, the European Union's basic model seems to embrace the notion that effective legislation cannot keep pace with the dynamic expansion of technology unless the two are inextricably linked.

This European approach to the protection of digital privacy and surveillance has been exhibited since the dragnet collection of online data began to take shape, most notably through the EU's approval of the Data Protection Directive in 1995. This comprehensive piece of legislation displayed a wholehearted embrace of the rights of individuals, essentially granting European citizens the right to correct or simply delete any personal information they find online, as well as block companies from transferring their data to a third-party, even if this entity is outside their borders. This ambitious bill crafted over twenty years ago says a lot about the profound way in which the European approach to privacy differs from that of America. Whereas the U.S. government has run into trouble by enabling unregulated corporate interests to encroach upon civil liberties, the European approach was so preemptive and thorough that it ran into similar difficulties enforcing these laws as transnationals—primarily based in the United States—began dominating the digital landscape (Bamberger & Mulligan 2015, 141). Large aggregates of personal data collected from people living in the European Union were arguably of even greater value to these companies because they opened the door for untapped markets. Thus, data brokers and large internet based corporations began utilizing the full extent of their technology and influence to circumvent European data protections just as they have in the United States.

However, demonstrating its dedication to the continued protection of European individuals' privacy, the EU passed the General Data Protection Regulation (GDPR) in April of 2016, the single most comprehensive initiative to combat unwarranted surveillance and data mining to date. While technically an update to the 1995 Data Protection Directive, the GDPR can more accurately be described as a complete overhaul, tightly binding data protection policy and enforcement between all member states and eliminating any room for substantive national

deviations (Bamberger & Mulligan 2015, 31). The GDPR was first proposed before the European Parliament back in late 2011, and after lengthy deliberations among representatives from all 28 member states, it has officially been approved with plans to take effect on May 25, 2018 following a two-year transition period. The GDPR is a comprehensive piece of legislation that uses all available resources at the disposal of the EU to protect citizens' personal data, specifically facilitating free circulation of data within the union while barring external collection and exploitation abroad. Unlike the United States government, the EU has been clear and expansive in regard to what it considers personal data protected by the state—Viviane Reding, European Commissioner for Justice, Fundamental Rights and Citizenship, explains:

> Personal data is any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a photo, an email address, bank details, your posts on social networking websites, your medical information, or your computer's IP address… everyone has the right to personal data protection in all aspects of life: at home, at work, whilst shopping, when receiving medical treatment, at a police station or on the Internet… In a globalized[sic] world, the transfer of data to third countries has become an important factor in daily life… and there are no borders online… (Reding 2012, 2)

This comprehensive perspective held by the EU regarding digital privacy laws and enforcement differs meaningfully from that of the United States, and as of May 25, 2018, American corporations stand to suffer significantly. These American transnationals have historically been in control of the digital world, and much of their success has come as a direct result. If these same corporations refuse to accept the vast transformations the European digital landscape is primed to undergo, serious conflicts may arise that set the two entities against each

other. Yet, unlike the United States, the European Union has no allegiance or critical dependence on these same corporations, and it has chosen to place the rights of its citizens above their interests. This is where the final divergence between the American model and the European model can be identified—the rights afforded to corporations are fundamentally different.

The United States has a much more lenient view on corporations in general, essentially viewing them as a number of persons united in one body for one purpose, thereby deserving of the same rights and protections as the people themselves. This generalized definition has evolved over the course of American history, and the process of its evolution has been significantly influenced through various decisions made by the Supreme Court. The most recent ruling of this sort was Citizens United v. Federal Election Commission, and in it the Supreme Court voted 5-4 in favor of corporations' right to make unrestricted political expenditures. This ruling has significantly altered the political landscape and corporate influence therein, and the perpetuation of digital surveillance and data collection has come as a direct result. Citizens United has allowed immeasurable sums of corporate dark money to flood the political world, essentially making one's chances of winning a seat in Congress nearly impossible without it in some form. As a result, the true allegiance of our elected officials has been thrown into question—why vie for comprehensive digital privacy legislation on behalf of the people if it will threaten your relationship with corporate backers? While American corporations are afforded rights similar to the American people, the two groups are widely dissimilar. Corporate interests belonging to a wealthy, powerful few are being placed above the rights of millions of Americans lacking these same resources. Unlike representatives in Europe who have committed to individual privacy rights through the implementation of the GDPR, the majority of Americans in Congress have shown they lack the courage to defy corporate America and stand up for the individual citizens.

Unfortunately, until rulings such as Citizens United are repealed, this transformation is unlikely to occur, thereby making the opportunity for comprehensive surveillance and data protection unrealistic. History has shown that substantial legislation in favor of disenfranchised people is often opposed until sudden, catastrophic events catalyze intervention—abolition required the Civil War, the Great Depression led to the New Deal, and September 11, 2001 triggered two wars costing over $2 trillion. While these examples are extreme, the basic principle remains the same—monumental changes to American society are often brought about by catastrophic circumstances. As the cycle of mass surveillance and dragnet data collection continue to spiral out of control, one can only speculate as to the inconceivable disasters that may finally force us—all of us—to accept this as a problem in need of legitimate resolution.

Chapter Six: Conclusion

All political thinking for years past has been vitiated in the same way. People can foresee the future only when it coincides with their own wishes, and the most grossly obvious facts can be ignored when they are unwelcome. (George Orwell)

The evolution of American surveillance and data collection was not an undetectable development. Rather, we allowed ourselves to remain ignorant, placing too much faith in institutions as to which we would be wise to always maintain a healthy skepticism. As mentioned above, the development and abuses in data collection between corporate-government collaboration were not unforeseeable, but in fact a result of logical processes. The "war on terror" gave the government the opportunity to expand its surveillance activities, and as it had in the 1970s, the government seized this opportunity. As these activities expanded and data collection became a growing and profitable industry, it was to be expected that corporations would similarly seize the opportunity to exploit the government's willingness to spend significant sums of money in these endeavors. It was in many ways almost inevitable that the two groups would be true to their natures—while perhaps "strange bedfellows," the arrangement was mutually beneficial and thus its development and growth are not surprising.

Our fault lies in the fact that we failed to heed the warnings of people such as Edward Snowden, those brave enough to stand up as the unpopular minority in an attempt to defend the rights afforded to us by the Constitution. Many citizens chose to ignore what they simply did not want to believe. Yet, history has shown that this is one of the worst things we as citizens can do. As Americans, we are not merely given the right to come together and create political change, we are tasked with a responsibility to participate politically in defense of civil liberties people

before us fought to guarantee. One of these most basic liberties is privacy and it has arguably never faced a greater challenge in American society than that posed by mass digitalization. The final chapters of the story of domestic surveillance and mass data collection have not yet been written. It would be naïve to suggest that all surveillance and data collection activities are detrimental to society, and even more naïve to expect that they will cease, especially as technological advances further enable their expansion. However, we cannot allow the positive elements of these activities, as well as our seemingly insatiable appetite for and dependency on technology, to weaken our commitment to the protection of our fundamental rights. These rights were established as a means to create limits on the power of the government. As data increasingly becomes a commodity, we must remember that it is our commodity, and it is indelibly linked to our privacy. We must be vigilant in ensuring that it is used in a responsible, ethical and legal manner.

References

18 US Code. Sec. 2703(d) and 3122, 2012, Online, wired.com, 10 October 2016

28 CFR 23.20 - Operating Principles. LII / Legal Information Institute. N.p., 2017. Web. 10 Mar. 2017.

Angel Jennings, Richard Winton and James Rainey. "Sheriff's Secret Air Surveillance Of Compton Sparks Outrage". latimes.com. N.p., 2014. Web. 10 Mar. 2017.

Angwin, Julia. “Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance.” 1st ed. New York: Henry Holt, 2014. Print.

Atkins, S. (2011). National security agency. In *The 9/11 Encyclopedia*. Santa Barbara, CA: ABC-CLIO.

Bachman, Katy. "Senate Commerce Report Says Data Brokers 'Operate Behind A Veil Of Secrecy' [Updated]". Adweek.com. N.p., 2013. Web. 10 Mar. 2017.

Ball, James. "Angry Birds And 'Leaky' Phone Apps Targeted By NSA And GCHQ For User Data". the Guardian. N.p., 2014. Web. 10 Mar. 2017.

Bamberger, Kenneth A and Deirdre K Mulligan. Privacy On The Ground: Driving Corporate Behavior In The United States And Europe. 1st ed. Cambride, MA: The MIT Press, 2016. Print.

Binney, William. "The Frontline Interview: William Binney." Interview by Jim Gilmore. *Pbs.org*. N.p., 2 Jan. 2015. Web. 11 September. 2016. <http://www.pbs.org/wgbh/pages/frontline/government-elections-politics/united-states-of-secrets/the-frontline-interview-william-binney/>.

Boghosian, Heidi. Spying on Democracy: Government Surveillance, Corporate Power, and Public Resistance. City Lights, 2013. Print.

Braun, Stephen. "US Officials Long Denied Massive Data Trawling." *The Big Story- Associated Press*. Associated Press, 7 June 2013. Web. 16 October. 2016. <http://bigstory.ap.org/article/us-officials-long-denied-massive-data-trawling>.

Burns, Thomas L. "The Early History of the NSA." *The Quest for Cryptologic Centralization and the Establishment of NSA 1940-1952*. Fort Meade: Center for Cryptologic History, National Security Agency, 2005. Print.

Carroll, Rory. "Silicon Valley's Culture Of Failure … And 'The Walking Dead' It Leaves Behind." The Guardian. N.p., 2014. Web. 10 Mar. 2017.

Citizenfour. Dir. Laura Poitras. Prod. Mathilde Bonnefoy and Dirk Wilutzky. Perf. Edward Snowden, Glenn Greenwald and Ewan Macaskill. Praxis Films, Participant Media & HBO Films, 2014. DVD.

Daley, David. Ratf**Ked: The True Story Behind The Secret Plan To Steal America's Democracy. 1st ed. London: Liveright Publishing Corporation, 2016. Print.

Dart, Tom. "Eye In The Sky: The Billionaires Funding A Surveillance Project Above Baltimore". the Guardian. N.p., 2016. Web. 10 Mar. 2017.

DNI Releases Budget Figure for 2008 National Intelligence Program. *DNI Releases Budget Figure for 2008 National Intelligence Program*. Web. 15 Sep. 2016. <http://fas.org/irp/news/2008/10/odni102808.html>.

Farzad, Roben. "Google at $400 Billion: A New No. 2 in Market Cap." Bloomberg.com. Bloomberg, 12 Feb. 2014. Web. 10 Nov. 2016.

Federal Trade Commission,. Complaint And Request For Investigation Of Mcdonald's Corporation's Violation Of The Children's Online Privacy Protection Act In Connection With Happymeal.Com. Washington, D.C.: N.p., 2012. Print.

Federal Trade Commission. (2012, February). Mobile Apps for Kids: Current Privacy Disclosures are Dis*app*ointing [Staff Report]. Retrieved from https://www.ftc.gov/sites/default/files/documents/reports/mobile-apps-kids-current-privacy-disclosures-are-disappointing/120216mobile_apps_kids.pdf

Greenwald, Glenn. "Fisa Court Oversight: A Look inside a Secret and Empty Process." *Theguardian.com*. Guardian News, 18 June 2013.

Grinberg, Emanuella. "Baltimore Police Have Racial Bias, DOJ Says". CNN. N.p., 2016. Web. 10 Mar. 2017.

Harress, Christopher. "The FBI Faces Scrutiny Over Its Surveillance Airplanes Flying Over US Cities". International Business Times. N.p., 2014. Web. 10 Jan. 2017.

Hayden, Michael, Mike Wiser, and Jim Gilmore. "Transcript of C-SPAN Interview with CIA Director." *PBS*. PBS, 2 Jan. 2014. <http://www.pbs.org/wgbh/pages/frontline/government-elections-politics/united-states-of-secrets/the-frontline-interview-michael-hayden/>.

Huhne, Chris. "Prism and Tempora: The Cabinet Was Told Nothing of the Surveillance State's Excesses." *Theguardian.com*. Guardian News, 6 Oct. 2013. Web.

Hutcheson, John, David Domke, Andre Billeaudeaux, and Phillip Garland. "National Identity, Elites, and a Patriotic Press." *Political Elites, News Media, and the Rhetoric of U.S. National Identity Since September 11*. Taylor & Francis Group, 2004. 27-50. Print.

Isikoff, Michael. "Homeland Security 'Fusion' Centers Spy On Citizens, Produce 'Shoddy' Work, Report Says". NBC Investigations. N.p., 2017. Web. 10 Mar. 2017.

Johnson, Luke. "Obama Defends NSA Programs, Says Congress Knew About Surveillance." *The Huffington Post*. TheHuffingtonPost.com, 7 June 2013. Web. <http://www.huffingtonpost.com/2013/06/07/obama-nsa_n_3403389.html>.

Kroft, Steve. "The Data Brokers: Selling Your Personal Information". Cbsnews.com. N.p., 2014. Web. 10 Mar. 2017.

Lee, Timothy B. "Here's Everything We Know about PRISM to Date." The Washington Post. N.p., 13 June 2013. Web. 11 May. 2016.

Lipowicz, Alice. "Trailblazer Loses Its Way -- Washington Technology." *Http://washingtontechnology.com*. 1105 Media Inc., 10 Sept. 2005. Web. 18 October 2016.

MacAskill, Ewan. "NSA Paid Millions to Cover Prism Compliance Costs for Tech Companies." The Guardian. 23 Aug. 2013. Web. 18 Sep. 2016.

McAvoy, Nelson. Coded Messages: How the CIA and NSA Hoodwink Congress and the People. New York, NY, USA: Algora Publishing, 2010.

Monahan, Torin and Neal A. Palmer. "The Emerging Politics Of DHS Fusion Centers". Security Dialogue 40.6 (2009): 617-636. Web. 10 Mar. 2017.

Monte, Reel. "Secret Cameras Record Baltimore’S Every Move From Above". Bloomberg.com. N.p., 2016. Web. 10 Mar. 2017.

Morris, Jason, and Ed Lavendera. "Why Big Companies Buy, Sell Your Data - CNN.com." *CNN*. Cable News Network, 23 Aug. 2012.

Pagliery, Jose. "FBI Lets Suspects Go to Protect 'Stingray' Secrets." CNNMoney. Cable News Network, 18 Mar. 2015. Web. 9 Nov. 2016.

PBS. Frontline Interviews: Edward Loomis. 13 May. 2008 Web. 15 Oct. 2016. <http://www.pbs.org/wgbh/pages/frontline/government-elections-politics/united-states-of-secrets/the-frontline-interview-edward-loomis/>.

Price, David H. 2014. "The New Surveillance Normal: NSA and Corporate Surveillance in the Age of Global Capitalism." *Monthly Review* 66 (3): 43-53.

Reding, Vivane. "European Commission - PRESS RELEASES - Press Release - Commission Proposes A Comprehensive Reform Of Data Protection Rules To Increase Users' Control Of Their Data And To Cut Costs For Businesses". Europa.eu. N.p., 2012. Web. 10 Mar. 2017.

Sarno, David. "Hacking of Data Firm Epsilon Exposes Customers of 50 Firms." *LAtimes.com*. Los Angeles Times, 05 Apr. 2011. Web. 19 Sep 2016.

Schneier, Bruce. "Schneier on Security." *Bloomberg.com*. Resilient Systems Inc., 31 July 2013. Web. 15 October 2016.

Schulz, G.W. and Amanda Pike. "Hollywood-Style Surveillance Technology Inches Closer to Reality | The Center For Investigative Reporting". Cironline.org. N.p., 2017. Web. 10 Mar. 2017.

Singer, Natasha. "Mapping, and Sharing, the Consumer Genome." *The New York Times*. The New York Times, 16 June 2012.

Snow, Blake. "What Would A World Without Internet Look Like?". The Atlantic. N.p., 2016. Web. 10 Mar. 2017.

Stanley, Jay. "Baltimore Police Secretly Running Aerial Mass-Surveillance Eye In The Sky". American Civil Liberties Union. N.p., 2016. Web. 10 Mar. 2017.

Stingray Tracking Devices: Who's Got Them? American Civil Liberties Union. ACLU, 24 Feb. 2015. Web. 14 September 2016.

United States of Secrets: Part One & Two. Dir. Will Lyman Prod. Michael Kirk and Martin Smith. FRONTLINE, Public Broadcasting Service. 2014. DVD.

United States. Congress. Senate. *The Final Report of the Select Committee on Presidential Campaign Activities, United States Senate, Pursuant to S. Res. 60, February 7, 1973: A Resolution to Establish a Select Committee of the Senate to Investigate and Study Illegal or Improper Campaign Activities in the Presidential Election of 1972.* Washington: U.S. Govt. Print. Off., 1974. Print.

United States. U.S. Department of Justice. Office of Legal Affairs. *Legal Authority for the Recently Disclosed NSA Activities*. William E. Moschella. Washington D.C.: Department of Justice, 2005. Print.

Verble, Joseph. "The NSA and Edward Snowden: Surveillance in the 21st Century." *Computers and Society - Special Issue on Whistleblowing* 23 Sept. 2014: 14-20. Print.

Wagner, Alex. "When Republicans Draw District Boundaries, They Can't Lose. Literally." Nytimes.com. N.p., 2016. Web. 10 Mar. 2017.

Walker, Clarence. "New Hi-Tech Police Surveillance: The "StingRay" Cell Phone Spying Device." Global Research. The Centre for Research on Globalization, 13 Apr. 2013. Web. 18 October 2016.

Whitehead, John. "The Corporate Surveillance State: How the Thought Police Use Your Cell Phone to Track Your Every Move." The Huffington Post. TheHuffingtonPost.com, 8 Aug. 2012. Web. 18 October 2016.