BRAVE NEW WORLD RELOADED: ADVOCATING FOR BASIC CONSTITUTIONAL SEARCH PROTECTIONS TO APPLY TO CELL PHONES FROM EAVESDROPPING AND TRACKING BY THE GOVERNMENT AND CORPORATE ENTITIES

by

MARK KENNETH BERRIOS-AYALA

A thesis submitted in partial fulfillment of the requirements
for the Honors in the Major Program in Legal Studies
in the College of Health and Public Affairs
and in The Burnett Honors College
at the University of Central Florida
Orlando, Florida

Fall Term 2013

Thesis Chair: Dr. Abby Milon

ABSTRACT

Imagine a world where someone's personal information is constantly compromised, where federal government entities AKA Big Brother always knows what anyone is Googling, who an individual is texting, and their emoticons on Twitter. Government entities have been doing this for years; they never cared if they were breaking the law or their moral compass of human dignity. Every day the Federal government blatantly siphons data with programs from the original ECHELON to the new series like PRISM and Xkeyscore so they can keep their tabs on issues that are none of their business; namely, the personal lives of millions. Our allies are taking note; some are learning our bad habits, from Government Communications Headquarters' (GCHQ) mass shadowing sharing plan to America's Russian inspiration, SORM. Some countries are following the United States' poster child pose of a Brave New World like order of global events. Others like Germany are showing their resolve in their disdain for the rise of tyranny.

Soon, these new found surveillance troubles will test the resolve of the American Constitution and its nation's strong love and tradition of liberty. Courts are currently at work to resolve how current concepts of liberty and privacy apply to the current conditions facing the privacy of society. It remains to be determined how liberty will be affected as well; liberty for the United States of America, for the European Union, the Russian Federation and for the people of the World in regards to the extent of privacy in today's blurred privacy expectations.

DEDICATION

This thesis is hereby dedicated to the late Mark Edward Tourigny, a good friend, person and poster child for the positive mindset. His time here on Earth proved the cold, hard truth that life can be an unforgiving mistress; however, you never let your problems get the best of you. Looking back, when we were in middle school I always remembered the times we laughed together, the times you would play my Scorpion King game on GameCube. Those times were great; but, as you know, situations change and best friends can become strangers with lack of communication and contact acting as the wedge in our lives. I wish I could have gone to your funeral but I simply did not know that you passed away until many years later and for that I am sorry. I have always found it eerie that you left Earth on my eighteenth birthday; nevertheless, with great happiness and greater resolve I write this thesis with your memory in mind as the guiding light of even-temper and good heartedness in a time of turbulent confusion and growing oppression. With that, I dedicate this thesis to your life and memory.

Mark Edward Tourigny-

Passed away November 14th, 2009

ACKNOWLEDGMENTS

I take the time here to acknowledge all those who helped make this thesis possible. I would like to thank my Thesis Committee Chair Dr. Abby Milon for planting the seed in my brain about this opportunity and being a good mentor. I would like to thank Dr. Fromang for joining my committee and giving me the thoughtful critiques on my proposal and thesis. I give much thanks to Dr. Parrish for his supportive wisdom and belief in me throughout the time I have known him; I also thank Dr. Cory Watkins of the Criminal Justice Department for the forgoing reasons.

I wish to acknowledge my Mother and Father for making me the man I am today for without them I would be lost. I would like to thank and acknowledge my eighth grade math teacher Mr. Embry for his wise and thoughtful words on growing up and life; his words greatly made me more aware of the trials that would come in life. I recognize my good friend Mathew Goodison-Orr for opening my mind to the possibilities of the world and for motivating me to reach out and get what I truly want.

Next, I wish to recognize the University of Central Florida (UCF) for its impression on me during my time here. UCF has given me the opportunities of a lifetime and a new perspective on how far I have come and the road I must travel ahead.

Finally, I recognize the United States of America as the nation to which this thesis would be meaningless without. Only here can I write or speak about anything I want without fear of government persecution; I know this thesis will help put my nation back on the right track.

TABLE OF CONTENTS

BACKGROUND 1

ECHELON 4

Timeline of Tyranny 5

Legal but not Constitutional 11

Initial Safeguards 12

MAC Address 13

Street View "Wi-Spy" 15

Android Spying 17

Opt-Out Options 19

"Magneto" 19

Cooking up Trouble with the NSA 22

Leaked Documents on NSA Searches 24

Capabilities 27

Benefits and Issues 29

ISSUE 30

Congressional Audits 30

Dangers of Using the Same Comments Twice 31

We Can lie about It, Just Not Talk about It 33

PRISM and its Counterparts 35

SORM 37

INDECT 40

French Big Brother 42

Allied Spying 43

Corporate Espionage 44

Retail Tracking 46

Corporate Double Agents 48

Password Demand Letters 50

Questions of Law 53

Litigation 55

Al-Haramain v. Obama 57

Fifth Circuit Upholds Mass Surveillance 58

Partisan Divide 60

International Front 61

Merkel's Election Woes 62

European Union's (EU) Drone Fleet 64

Ireland 66

Long Term Goals and Global Hegemony 66

Internet of Things 68

RESOLUTION 70

Laboratories of Democracy 70

Supremes of New Jersey 71

Bill against Big Brother 71

Amending § 215 72

Substantial Revamping 73

Global Policy Implications of Government Surveillance 75

The World has Taken Note 76

Katz Test and Relevant Case Law 76

Concluding Remarks 84

WORKS CITED 86

LIST OF ABBREVIATIONS

ACLU – American Civil Liberties Union

AOA – Angle of Arrival

CALEA – Communications Assistance for Law Enforcement Act

CFAA – Computer Fraud and Abuse Act

CIA – Central Intelligence Agency

DARPA – Defense Advanced Research Projects Agency

DOJ – Department of Justice

ECPA – Electronic Communications Privacy Act of 1986

EU – European Union

FBI – Federal Bureau of Investigation

FISA – Foreign Intelligence and Surveillance Act of 1978

FISC – Foreign Intelligence and Surveillance Court

GCHQ – Government Communications Headquarters

GPS – Global Positioning System

IMSI – International Mobile Subscriber Identity

LEO – Law Enforcement Officer

MAC address – Media Access Control Address

NSA – National Security Agency

OUI – Organizationally Unique Identifier

PRISM – Planning Tool for Resource Integration, Synchronization, and Management

SORM – System for Operational-Investigative Activities

SSID – Service Set Identifier

TDOA – Time Difference of Arrival

TIA – Total Information Awareness

UAA – Universally Administered Address

UK – United Kingdom

US – United States of America

XKS – Xkeyscore

BACKGROUND

Technology like cell phones, the Internet and computers are a staple of our lives in the United States and the world, their size induces mobility. This technological interface helps people connect with friends and family on a consistent basis. The GPS applications make sure that we will never get lost.[1] Technology progresses at light speed, yet the laws that govern it strive to catch up and are moving at a snail's pace. This technology impacts our culture. This technology has grown to affect our lives in unexpected ways; police misconduct has been documented via video by bystanders who happen to see the misconduct and film the event with their cell phones, exposing the problem to the world.[2]

Cell phone applications like Foursquare and Facebook allow users to broadcast their location when they deem appropriate.[3] Corporate giants like Google use this location feature to display advertisements by the inbox after it is done searching the messages for location content.[4] This begs to question just who else is watching innocent location broadcast as well as their purposes. This shows that this new technology can prove to be a double-bladed sword; the same technology that enables greater mobility, heightened vigilance and superior navigation can also deprive people of their privacy.[5] Each cell phone communicates through a nationwide complex of over 300,000 cell phone towers and 600,000 "micro sites." These perform the same function

[1] Koppel, Adam. "Warranting a Warrant: Fourth Amendment Concerns Raised by Law Enforcement's Warrantless Use of GPS." *University of Miami Law Review* 64 (2010). 1061. At 1062
[2] Van Tassel, Rebecca G. "Walking A Thin Blue Line: Balancing The Citizen's Right To Record Police Officers Against Officer Privacy." *Brigham Young University Law Review* (2013). Et al
[3] Plourde-Cole, Haley. "Back To Katz: Reasonable Expectation Of Privacy In The Facebook Age." *Fordham Urban Law Journal* 38.2 (2010): 571-628
[4] *Id.*
[5] Bailey, Ronald. Your Cell Phone is Spying on You (2013)

as a cell phone tower, each of which gets a location "ping" from your cell phone every seven seconds.[6] It is possible for the government to trace your location with an accuracy of up to six feet.[7] It is even possible for law enforcement to gain access to your phone calls and text messages as well.[8]

This can all be done without a warrant and usually without a person ever knowing that the surveillance was commenced in the first place.[9] Law enforcement agencies across the United States have made 1.5 million requests for user data to cell phone companies in 2011 alone. Virtually none of the people who were investigated ever learned the request happened.[10] Law enforcement has also grown to favor the use of International Mobile Subscriber Identity (IMSI) in order to do their eavesdropping; even using make-shift cell towers that allow them to triangulate a cell phone's signal and location.[11]

Triangulation, as this process is known uses the same location signal a cell phone gives to the cellular towers as a means to make sure its phone calls are received in the highest quality and speed can be used to locate inhabitants as well.[12] The triangulation process uses two forms of cell phone/cell tower interface in order to find a human being's location: Time Difference of Arrival (TDOA) and Angle of Arrival (AOA) to triangulate the position.[13] TDOA measures the travel time it takes for a cell phone's location ping to travel to the cellular tower; the AOA measures

[6] *Id.*
[7] *Id.*
[8] *Id.*
[9] *Id.*
[10] *Id.*
[11] *Id.*
[12] Koppel 1067-68
[13] Koppel 1067

the strength of the signal.[14] Combined, these two methods of cell phone calling logistics can prove to be an accurate means to track someone's location in real time.[15]

Few people appreciate the gravity of the problem at hand.[16] They do not think it matters if the government can locate their favorite restaurant or preferred house of worship just by tracking their location.[17] "However, this line of thinking misses a larger point. If someone has the ability to know the real-time location of an individual around the clock, then one is able to create a full picture of that person's life."[18] This is an ever growing problem that needs to come to an end with greater public and societal scrutiny!

The discussion of the background facts will begin with an explanation of former government campaigns for espionage like ECHELON before transitioning into a timeline, giving an illustrative play-by-play of the relevant facts and how they interrelate to each other. There will be in-depth cataloging of past problems with Government and its surveillance desires. There will be mentions of new technological feats that will be used to shadow unsuspecting people and illustrations of how this happened. Details on how these new surveillance techniques impact real life situations are shown; international counterparts to the United States's spy agencies are discussed in detail. Questions of law will be presented with appropriate examples as well as examples of how the states are taking the initiative to solve these issues at their level of governance. Relevant case law is conferred and played in the form of a hypothetical appellate

[14] *Id.*
[15] Koppel, et al
[16] Koppel 1062
[17] *Id.*
[18] *Id.*

case, acknowledging the merits of each precedent's value towards a fictional (but soon to be real) petitioner and how it relates to the issues at hand.

ECHELON

After the fall of the Soviet Union the American intelligence community made a major shift in its information siphoning from spying on the Eastern Bloc to using their resources for terrorism, narcotics trafficking, technological development, economic intelligence, and organized crime.[19] It was not until after the 1998 Embassy bombings in Africa did the United States government realize that the new enemy would be Al-Qaeda, rising front and center as the primary threat to American values.[20] The major challenge to the NSA and the intelligence community as a whole was not the lack of adequate technology but the lack of personnel to help decipher the mountains of information fed by their spy satellites into a practical usable form.[21]

With the support and infrastructure of the UKUSA, the NSA created ECHELON, a massive global shadowing system.[22] Some have claimed that the NSA has used ECHELON to conduct corporate espionage on rival international firms on their behalf. The goal is to help them win international contracts and dominate the industry, solidifying American dominance.[23] "The Echelon interception system connects supercomputers throughout the world to "automatically search through the millions of intercepted messages for ones containing pre-programmed keywords or fax, telex and e-mail addresses."[24] ECHELON's twenty interception stations are

[19] Lawner , Kevin J. (2002). Post-Sept. 11th International Surveillance Activity—a Failure of Intelligence: the Echelon Interception System & the Fundamental Right to Privacy in Europe
[20] *Id.*
[21] *Id.*
[22] *Id.*
[23] *Id.*
[24] *Id.*

spread across the globe and are directly connected to the main office of the NSA in Fort Meade, Maryland; "where intercepted data can be analyzed, retained and disseminated."[25]

Since 1978, ECHELON is capable of tracking the communications of a single person via satellite.[26] In fact, it has been alleged that it was used to spy on the late Senator Strom Thurmond's conversations at one point.[27] "The testimony of a former Canadian Secret Service ('CSE') employee affirmed that Echelon monitored civilian communications."[28] He claims that they entered a woman into the database of suspected terrorists because she used an ambiguous phrase in a conversation.[29] Non-profits are not immune to the expansion of Government information interests; former NSA employees stated that Greenpeace and Amnesty International have been regularly eavesdropped for many years.[30]

Timeline of Tyranny

This timeline discloses how both the STELLARWIND program and ECHELON came into being from the ashes of the September 11th attacks to its (official) end in 2011.[31]

- 1948: United Kingdom-United States Security Agreement (UKUSA) is formalized; it creates the first clandestine international cooperative spy alliance between two nation's

[25] *Id.*
[26] *Id.*
[27] *Id.*
[28] *Id.*
[29] *Id.*
[30] *Id.*
[31] Bump, Philp. NSA's Massive Email Collection Started with Cheney and Ended With Obama

intelligence communities.[32] Though the UK parliament acknowledged the existence of the agreement the United States still will not follow suit.[33]

- August 1998: an American Intelligence agency reported that they had evidence "unidentified Arabs" planning on flying an "explosive-laden" plane into the Twin Towers in New York; the community felt that the evidence was exaggerated to great lengths and downplayed the risks.[34]
- December 1998: "the DCI [Director of Central Intelligence] George Tenet provided written guidance to his deputies at the CIA, declaring, in effect, 'war' with Bin Laden."[35]
- 1999: the NSA filed a patent for a software elucidation for creating a catalog of subject-matter from computer-generated content.[36]
- May-June 2001: NSA reports that there are around 33 different communications received indicating an imminent terrorist attack in the United States, courtesy of Al-Qaeda.[37]
- July 2001: the "Phoenix Memo" was sent; this memo was sent from the FBI field office in Phoenix, Arizona to a FBI unit in Washington stating that "several Arabs were seeking flight training and other courses involving airport security and airport operations at least one U.S. flight school."[38] The memo further suggested that the FBI look into all flight

[32] Lawner , Kevin J. (2002). Post-Sept. 11th International Surveillance Activity—a Failure of Intelligence: the Echelon Interception System & the Fundamental Right to Privacy in Europe
[33] *Id.*
[34] *Id.*
[35] *Id.*
[36] Markoff, John. (2006).Taking Spying to Higher Level, Agencies Look for More Ways to Mine Data
[37] Lawner
[38] *Id.*

schools to find Al-Qaeda operatives; still, the FBI never shared this information with other intelligence agencies.[39]

  - The EU parliament formally discloses the existence of the ECHELON program the NSA owns and maintains.[40]

- August 6th, 2001: President Bush received a briefing titled "Bin Laden Determined to Strike in U.S[;]" the briefing indicates that Al-Qaeda plans to hijack planes as part of their attack and that the buildings of Manhattan are their primary target.[41]
- August 16th, 2001: Al-Qaeda operative Zacarias Moussaoui was arrested in Minnesota after he was reported by a suspicious flight instructor who found it perplexing that a flight student did not wish to learn how to take off and land.[42] After an initial delay, the FBI obtained a warrant to search Moussaoui's computer and found cockpit blueprints for jet liners and a cell phone number of Muhammad Atta, one of the September 11th, hijackers.[43]
- August 23rd, 2001: "the Intelligence Community requested that two Al Qaeda suspects (wanted in connection with the August 2000 attack on the U.S.S. Cole, and later determined to be participants in the September 11th attacks) 'be added to the U.S. Department of State's 'watch list' for denying visas" for entry into the United States."[44] The New York FBI field office began to search for them, to no avail.[45] The Los Angeles

[39] *Id.*
[40] *Id.*
[41] *Id.*
[42] *Id.*
[43] *Id.*
[44] *Id.*
[45] *Id.*

office never received the memo, despite the fact that the two suspects lived openly in San Diego and were listed in the phone book and had credit cards in their name.[46]

- September 2001: the NSA is at the drawing board stage as it ponders how to expand its reach to gather more information from electronic communications.[47]
- September 11th, 2001: the World Trade Center in New York City and the Pentagon in Virginia are attacked when three planes are flown into them; one for each building. A fourth plane crashes in rural Pennsylvania.
- October 2001: the NSA informs the House Intelligence Committee and the CIA director about the intelligence gathered from predetermined phone numbers; the CIA director goes to the White House for a briefing regarding their findings and it is reported that the Vice President has interest in expanding the program further.[48] On October 4th, President Bush signs the order allowing the NSA to expand its shadowing.[49] During this time the NSA decided that they would hold themselves to their Chief Michael Hayden's "personal standard" which meant that the NSA would not intentionally spy on Americans domestically even though the act could be construed as allowing it.[50] "On October 26, 2001, President George W. Bush signed the USA Patriot Act into law."[51]
    - The NSA never considered obtaining the approval for their expansion under the flag of the Foreign Intelligence and Surveillance Act (FISA;) "Getting FISA approval would have curtailed the agency's flexibility and the number of targets it

[46] *Id.*
[47] Bump, NSA's Massive Email Collection Started with Cheney and Ended With Obama
[48] *Id.*
[49] *Id.*
[50] *Id.*
[51] Lawner

could surveil".[52] They decided instead to go the route of self-regulation; looking towards their internal legal review boards to help with the NSA's compliance with the law; the NSA general counsel signed approved the plan on October 5th.[53] "Approval of data analysis involving domestic targets was tasked to the Chief of Counterterrorism — or the program manager if the Chief was absent[;] [h]ow their "personal standards" [referring to the aforementioned standards of NSA Chief Michael Hayden] applied is not clear."[54]

- Sometime in 2002: the President finally allowed the Inspector General (IG) to be briefed about the surveillance program; the IG is the person tasked with oversight of the NSA.[55]
- 2004: the NSA is now sharing information with its sister agencies, the FBI and the CIA; this decision was made by the Department of Justice's (DOJ) Office of Legal Counsel;[56] this came as a surprise to the NSA. This may possibly be attributed to the increasing lawful dubiousness of the agenda.[57]
    - Later, the Bush Administration had to postpone the spying crusade amid concerns raised by high ranking officials of the DOJ and the FBI.[58]
    - 'The D[O]J quickly convinced the Fisa court to authorize ongoing bulk collection of email metadata records. On 14 July 2004, barely two months after Bush stopped the collection, Fisa court [C]hief [J]udge Collen Kollar-Kotelly legally blessed it under a new order – the first time the surveillance court exercised its authority over a two-and-a-half-year-old surveillance program.'[59]

[52] Bump, NSA's Massive Email Collection Started with Cheney and Ended With Obama
[53] *Id.*
[54] *Id.*
[55] *Id.*
[56] *Id.*
[57] *Id.*
[58] *Id.*
[59] *Id.*

    - Under the Vice President's blessing, the NSA began to work hand in hand with LEO's which is later approved by the FISC.[60]

- February 2006: NSA officials meet with a few venture capitalists regarding "computerized systems that reveal connections between seemingly innocuous and unrelated pieces of information."[61] The technology the NSA was looking for amounted to finding a new way to eavesdrop for data and find a new, better way to "us[e] mathematical and statistical techniques to scan for hidden relationships in streams of digital data or large databases."[62] "Supercomputer companies looking for commercial markets have used the practice for decades. Now intelligence agencies, hardly newcomers to data mining, are using new technologies to take the practice to another level."[63]
- May 2006: former NSA employee Russell Tice attends the Senate Armed Services Committee to tell them that the work that they are doing is both illegal and only a small fraction of the real picture of what is going on.[64] He also stated that the former NSA chief Michael Hayden oversaw all of this.[65] Some at the hearing also speculated that he additionally alluded to the use of spy satellites used to participate in the mass surveillance crusade.[66]

[60] *Id.*
[61] Markoff, John. (2006).Taking Spying to Higher Level, Agencies Look for More Ways to Mine Data
[62] *Id.*
[63] *Id.*
[64] Shakir, Faiz. (2006). NSA whistleblower To Expose More Unlawful Activity: 'People…Are Going To Be Shocked'
[65] *Id.*
[66] *Id.*

- 2007: the government gives the program its biggest revamp in over six years. The NSA moves to sifting through the emails of Americans.[67]
- 2008: the Congress (who is well versed in STELLARWIND) passes an amendment to FISA; hereby legalizing the conduct of the NSA.[68]
- 2011: the official termination of the program is recognized by the Obama Administration.[69]
    - The grand issue here is that the NSA has on a consistent basis cried for deregulation so that it may better "protect and defend" the United States of America from its foreign and domestic enemies when it clearly is not worried about them.[70] But this is not the first time the NSA has gone on a Brave New World style rampage over our privacy.

Legal but not Constitutional

In the 1970s there was reason to believe that the NSA was in the midst of a major eavesdropping campaign when it was found to be actively collecting telegraphic data from companies and while doing so, spied on millions of Americans that sent them regardless of whether they affiliated themselves with a foreign foe.[71] Other espionage agencies like the CIA and FBI ran an operation where they opened mail illegally in order to obtain information; they even went so far as to authorize break-ins to suspect's households in order to obtain intelligence

[67] Bump, NSA's Massive Email Collection Started with Cheney and Ended With Obama
[68] *Id.*
[69] *Id.*
[70] *Id.*
[71] Donohue, Laura. (2013). NSA Snooping is Legal: It Isn't Constitutional

data.[72] Even Congress was not immune to the Surveillance State as the Army Security Agency ran a program known as CONUS where many lawmakers, major political and civil rights leaders were the intended targets.[73] It is estimated that over 100,000 people were victims of the CONUS program.[74]

Initial Safeguards

In response to the perceived Big Brother that was growing in their midst, Congress passed FISA in 1978 in order to safeguard our civil liberties while allowing the Counter-Intelligence Community to do its work.[75] Over the past two generations however, FISA's purpose has eroded away with passages of its subsequent amendments that have turned it into the vehicle used to justify the Big Brother style governance that it was meant to prevent.[76] "Under the traditional FISA, if the government wants to conduct electronic surveillance, it must make a classified application to a special court, identi[f]ing or describing the target[;] [i]t must demonstrate probable cause that the target is a foreign power or an agent thereof, and that the facilities to be monitored will be used by the target."[77] Congress added § 702 to FISA in 2008 to make it easier to conduct espionage on foreigners; they do not need a court order so long as Americans were not targeted.[78] After the Oklahoma City Bombings and the September 11th Attacks the Government was allowed to expand their shadowing to company and personal data.[79] The United States Supreme Court has found that the Fourth Amendment does not shield

[72] *Id.*
[73] *Id.*
[74] *Id.*
[75] *Id.*
[76] *Id.*
[77] *Id.*
[78] *Id.*
[79] *Id.*

foreigners from searches conducted outside of the US; however, it has not recognized an overseas intelligence warrant prerequisite when foreign-targeted searches end result in the gathering of immeasurable stores of citizens' interactions.[80]

MAC Address

Whether a person is abroad or in the domestic sphere, in the current state of world affairs, the government has many new ways of keeping tabs on the population's electronic devices. Tablets, smartphones and some computers have a unique code that allows wireless internet to identify your electronic device.[81] With the advent of servers that are used to locate and track these devices; it has been used to track shoppers at malls so corporations can learn more about their shopping habits.[82] Some of these services have an "opt out" option but that requires that the consumer actually knows about it before they can go about opting out.[83] Media Access Control addresses (herein referred to as "MAC addresses)" give each electronic device a specific serial number so they can recognize them; some Wi-Fi hotspots are secure and only allow devices with very specific media access control or MAC addresses to log in.[84] There are smartphone "apps" that are used to change the MAC address in order to mitigate the effects of spying.[85]

Tragically, changing your MAC address could inevitably cause you to violate the Computer Fraud and Abuse Act (CFAA.)[86] The main aim of the CFAA is to deter the ability to

[80] *Id.*
[81] Solanti, Ashkan. (2013). How Protecting Your Privacy Could Make You the Bad Guy
[82] *Id.*
[83] *Id.*
[84] *Id.*
[85] *Id.*
[86] *Id.*

gain access to a network without authorization.[87] It is possible that in the process of changing your MAC address you could therefore gain access to forbidden networks, violating the CFAA.[88] MAC addresses help websites know how many times a person has used their website, used a form of free service or product, and exclude them once they have exceeded their limit for use.[89] "The New York Times, for example, imposes a 10 articles-a-month limit for non-subscribers, allowing users to browse 10 articles for free but then requiring payment for subsequent use… the method the New York Times and other publications use to identify users is unreliable and easy to circumvent, even inadvertently [users could use cell phone applications to change their MAC address or clear their cookies to avoid the New York Times' security measures]."[90]

Tracking is getting much more difficult to detect and evade.[91] There is an estimated 300+ tracking mechanisms actively keeping tabs on you if you browse onto a fairly popular website.[92] Some of the companies involved in these eavesdropping techniques have refused to honor user preferences and made it harder to evade their tracking.[93] Even simple acts such as clearing cookies off your browser can be construed to be in violation of the CFAA.[94]

> However, many websites rely on cookies to enforce paywalls. These companies do this so their freemium [colloquial term for a web based business model centered around giving something or providing a service free of charge] business models can work transparently, without initially requiring the user to be aware (i.e., log in) until they hit the limit. The *New York Times*, for example, imposes a 10 articles-a-month limit for non-subscribers, allowing users to browse 10 articles for free but then requiring payment for subsequent use. But the method the *New York Times* and other publications use to

[87] *Id.*
[88] *Id.*
[89] *Id.*
[90] *Id.*
[91] *Id.*
[92] *Id.*
[93] *Id.*
[94] *Id.*

> identify users is unreliable and easy to circumvent, even inadvertently. Clearing one's cookies periodically — or even using a browser's private browsing mode — bypasses the flimsy paywalls and allows users to continue reading stories. Under an unsophisticated judge's take, this act could be interpreted as exceeding "authorized access" (of 10 free articles a month) — and is therefore a potential, prosecutable violation of the CFAA.[95]

Street View "Wi-Spy"

In 2010, the internet company Google was revealed to have been involved in the "Wi-Spy" incident.[96] The incident dealt with Google's use of MAC addresses during their creation of the Google Maps Street View application (herein referred to as "Street View)."[97] Wi-Fi MAC address mapping functions by submitting the user's address to a database, which then returns the user's triangulated location.[98] Devices such as this will first query the Wi-Fi hotspot for the GPS locations of the connected devices; if that does not work then the device will next try to use a device's MAC address to find the location.[99] Once the MAC address is obtained the tracker begins to obtain the GPS location of the MAC address' device.[100]

MAC addresses have several different components and types.[101] The most common type is the Universally Administered Address (UAA) which is a MAC address that is intended to never be changed.[102] The first component of the MAC address is the Organizationally Unique

[95] *Id.*
[96] Chow, Raymond. (2013). Why Spy? An Analysis of Privacy and Geolocation in the Wake of the 2010 Google "Wi-Spy" Controversy. 57-93. Et al
[97] *Id.* at 69
[98] *Id.*
[99] *Id.*
[100] *Id.*
[101] *Id.*
[102] *Id.* at 63

Identifier (OUI) which is used to indicate the device's manufacturer.[103] MAC addresses also have a SSID which stands for Service Set Identifier which is used to aid in triangulation.[104]

Since MAC addresses are unique and presumably unchangeable they are usually associated with a person (the device's owner) much like a vehicle identification number is associated with a car owner.[105] Currently, the courts have has been reluctant to accept the argument that MAC addresses and other identifying locators used to track and brand technology can be used as an avenue to track and associate with a person.[106]

In 2006 a Google computer engineer developed a code for a tracker to autonomously locate and capture all wireless communications within the tracker's range for an unrelated purpose.[107] Later, in 2007 Google began creating the Street View imagery and in the process used the old 2006 code to help collect location data for their database.[108] The seriousness of the problem depends on the wireless routers' security settings.[109] If there is some security protocol, the data will be encrypted and therefore useless to the observer. On the other hand, if no security protocol exists then the data will be available in a plain text form;[110] meaning that the data will be viewable to anyone who receives it as a readable file, loaded with personal information.[111]

Chances are low that a person's data has been picked up. Unless a user was transmitting data at the moment that the Google Maps truck drove by; they probably did not obtain any

[103] *Id.*
[104] *Id.* at 61
[105] *Id.*
[106] *Id.*
[107] *Id.* at 69
[108] *Id.* at 69
[109] *Id.* at 69
[110] *Id.* at 69
[111] *Id.* at 69

information.[112] Still, there are those who believe that the last sentence is a matter of wishful thinking rather than a matter of truth.[113] Google has been accused of unwittingly collecting private information such as credit card information, passwords and other unencrypted data without anyone's consent or knowledge.[114] German authorities initially accused Google of its mass gathering endeavors in April of 2010, Google vehemently denied the accusations.[115] Faced with the threat of German government audits, Google reversed its deny-all-accusations stance and admitted to the mass gathering accusations.[116] They went a step further and grounded its Street View trucks until the issue could be resolved.

Android Spying

In the aftermath of the Street View fiasco, Google next turned to its Android smartphone operating system in order to continue its mass collection campaign.[117] With its default privacy settings, Android phones send their GPS coordinates to regional data collection centers; other phones that request data from a Google GPS application will come under Google's "all seeing eye" of mass surveillance.[118] There is no option to discontinue the constant reporting of your geolocation information to Google; the only way to accomplish this goal is to shut off the Android's Wi-Fi hotspot and GPS applications.[119]

This is causing massive new legal problems for Google and the rest of Silicon Valley. Violations of contractual abilities are almost certainly not the best road to travel for plaintiffs in a

[112] *Id.* at 69
[113] *Id.* at 69-70
[114] *Id.* at 70
[115] *Id.* at 70
[116] *Id.* at 70
[117] *Id.* at 71
[118] *Id.* at 71
[119] *Id.* at 71

hypothetical suit against Google's eavesdropping crusade.[120] As far as public knowledge is concerned, there has not been any harm between the parties but there are the concerns of our society as a whole.[121] "Is our society concerned about being bound by adhesion contract to consent to constant surveillance and contribution of our location data to an unregulated database?"[122] Do users understand the full picture of constant location reporting even if they do read the terms of agreement?[123] States have the power to legislate and adjudicate over contractual matters like this; although, with the advent of smartphones, there seems to be a call for a federal response to this quagmire.[124]

If a state court or legislature moved to prohibit Google's shadowing goals then the consumer could be held as cohorts in illicit activity.[125] If a hypothetical state managed to ban Google's data collection, how would that play out in a practical sense?[126] Would it be possible to code their Android products to systematically not spy on their customer's GPS position if they are within a man-made line drawn in the ground?[127] Framed broadly, this could apply to shadowing restrictions on any electronic device that has been imposed at the state or federal level.[128]

[120] *Id.* at 71-72
[121] *Id.* at 72
[122] *Id. at 72*
[123] *Id. at 72*
[124] *Id. at 72*
[125] *Id. at 72*
[126] *Id. at 72*
[127] *Id.*
[128] *Id.*

Opt-Out Options

Now comes the quagmire of the data Google already has. Amid pressures from a plethora of EU agencies, on September 13th, 2011 Google stated their intentions on developing an "opt-out" option for their patrons.[129] By adding "_nomap" to the wireless routers' SSID, Google will delete the user's information off their data base and only have access of the user's location if the user decides to actively use their GPS application.[130] Google claims this is the wisest move since it allows only the owner of the wireless router to disable the tracking.[131]

The critics opine on the so called "solution" to the problem. Critics say that the technological illiterate will not be able to utilize this tool; they cite that few people outside of Silicon Valley know what a SSID is, let alone know how to use it to their advantage.[132] Even if they do manage a miracle and update their wireless router, they will doubtlessly be unaware of the last segment of the task; updating the security settings of their internet-capable gadgets.[133]

"Magneto"

On the morning of August 4th, 2013 malware showed up on numerous websites owned and maintained by the anonymous movement sympathizer, the Freedom Hosting firm; at first, the FBI is (allegedly) to blame, but in time the attack was traced to the Science Applications International Corporation (SAIC) headquarters.[134] SAIC is a major technology and defense contractor for the government.[135] Malware's reverse-engineer Vlad Tsyrklevich who was on site

[129] *Id.*
[130] *Id.*
[131] *Id.*
[132] *Id.*
[133] *Id.*
[134] Poulsen, Kevin. (2013). Feds Are Suspects in New Malware That Attacks Tor Anonymity
[135] *Id.*

to help with damage control said "[i]t just sends identifying information to some IP in Reston, Virginia… [i]t's pretty clear that it's FBI or it's some other law enforcement agency that's U.S.-based [now known to be SAIC.]"[136] This may be the first instance of a live CIPAV (computer and internet protocol address verifier) in the field; CIPAV is a form of spyware used by Law Enforcement Officers (LEO), thought to have existed since 2002 to gather evidence for criminal prosecutions against pedophiles.[137] "The code [in reference to CIPAV] has been used sparingly in the past, which kept it from leaking out and being analyzed or added to anti-virus databases".[138]

In Ireland, roughly the week before the incident, Erin Marques was arrested on charges of disseminating child pornography via an extradition request from the United States. His case is pending in a Maryland federal court and he is believed to be one of the largest distributors of child pornography on the Earth.[139] Freedom Host has a shadowy reputation of encrypting child pornography in its servers as well as extremely sensitive information from human rights groups to journalists in its Tor anonymous servers [a firm that provides a server people may use as a proxy to keep their online actions private].[140] The servers hide the location information of sites with the ".onion" domain under massive layers of routing; creating an "onion" of sorts for encryption purposes.[141]

[136] *Id.*
[137] *Id.*
[138] *Id.*
[139] *Id.*
[140] *Id.*
[141] *Id.*

Surveillance of alleged pedophiles is not the scope of this thesis. What is at stake is the content of the websites owned by groups not accused of aiding child molestation. The Tor anonymous hosting sites experienced a shutdown of their operations; users accessing the website saw a "down for maintenance" message across their screens.[142] The FBI would have been hard pressed to find anything provocative on these sites, let alone child pornography.[143] "Some visitors looking at the source code of the maintenance page realized that it included a hidden 'iframe' tag that loaded a mysterious clump of Javascript code from a Verizon Business internet address located in Virginia."[144] This code was circulated over the internet until internet service provider Mozilla identified the code; they claimed that it attacks a specific code in a now outdated Firefox internet browser vulnerable to the spyware.[145] This version of Firefox is used by the Tor anonymous server sites.[146] "The malware payload could be trying to exploit potential bugs in Firefox 17 ESR, on which our Tor Browser is based… '[w]e're investigating these bugs and will fix them if we can."[147]

"The strongest clue that the culprit is the FBI, beyond the circumstantial timing of Marques' arrest, is that the malware does nothing but identify the target."[148] The culprit, the Magneto virus, is unique in that it is used to determine the MAC address from the target and report it back to its creator.[149] It is subsequently sent to a server in Virginia where it reveals the

[142] *Id.*
[143] *Id.*
[144] *Id.*
[145] *Id.*
[146] *Id.*
[147] *Id.*
[148] *Id.*
[149] *Id.*

real IP (internet provider) address.[150] "The attackers spent a reasonable amount of time writing a reliable exploit, and a fairly customized payload, and it doesn't allow them to download a backdoor or conduct any secondary activity."[151] Magneto furthermore makes a serial number used to tie a user's specific visit to the Freedom Host server; thus drawing a timeline of an individual's usage.[152] It remains unresolved if anti-virus companies will be able to code a defense to Magneto with this new source sample.[153]

Cooking up Trouble with the NSA

Not even simple internet queries are immune from government intrusion and retaliation. In New York, the Catalano couple was busy "googling" the words pressure cookers and backpacks on their respective work computer; a few days later the "Joint Terrorism Task Force" (JTTF) came to pay them a visit in the form of a raid of their property.[154] "The Suffolk County Criminal Intelligence Detectives received a tip from a Bay Shore based computer company regarding suspicious computer searches conducted by a recently released employee."[155] The Google search was deemed to be noncriminal in nature by the Suffolk County Criminal Intelligence detectives.[156] The members of the task force were probably part of the FBI or Homeland Security; but, it is not unheard of to see local, state and federal LEOs working together as members of a JTTF squad.[157]

---

[150] *Id.*
[151] *Id.*
[152] *Id.*
[153] *Id.*
[154] Bump, Philp. (2013). Update: Now We Know Why Googling 'Pressure Cookers' Gets a Visit from Cops
[155] *Id.*
[156] *Id.*
[157] *Id.*

The FBI claims that the raid was carried out by the Suffolk County police department while that same department points the finger of blame at the FBI.[158] The FBI spokesperson could not comment on whether the FBI had any role in the dissimilation of intelligence of the search to the local LEO agency.[159] "Both Suffolk and Nassau County's police departments are members of the FBI's Joint Terrorism Task Force…[;] Suffolk County is also home to a 'fusion center,' a regionally located epicenter for terror investigations associated with the Department of Homeland Security."[160] The FBI contends that they did not participate in the raid.[161]

The Government contends that it only spies on Americans that are separated from the terrorists by "at least two" people.[162] This two person test could mean that the government has the ability to shadow up to two million people when eavesdropping one suspect.[163] Perhaps one is flagged for a search because they were among the two million people who knew someone who knew someone that was a terrorist? Others say that the real reason that the green light was given for a raid was because the NSA has been systematically collecting data for Google searches that contain "suspicious" words like "pressure cooker" or "backpack" so they can be passed on to the appropriate organization.[164]

There may be a third reason. "The Guardian [refers to the major newspaper based in London] reported on XKeyscore, a program eerily similar to a Facebook search that could clearly allow an analyst to run a search, pick out people who have done searches for [certain]

[158] *Id.*
[159] *Id.*
[160] *Id.*
[161] *Id.*
[162] *Id.*
[163] *Id.*
[164] *Id.*

items from the same location."[165] The real question is how those searches ended up in the government's surveillance data hub?[166] Other factors that may have contributed to the raid may have been the fact that Mr. Catalano traveled to Asia in the past; still no one knows why the Catalanos were targeted for this raid.[167]

During the raid, the Catalanos were told by the members of the JTTF that they participate in these kinds of raids about a hundred times per week.[168] "And that 99% of those visits turn out to be nothing[;] I don't know what happens on the other 1% of visits and I'm not sure I want to know what my neighbors are up to."[169] All this can reportedly happen from a simple Google search.

Leaked Documents on NSA Searches

The classified documents whistleblower Edward Snowden released shows that Xkeyscore is a force of reckoning.[170] Snowden released some training slides that depicted "screenshots showing what analysts would see as they viewed the intercepted conversations and include sample search queries such as '[s]how me all encrypted word documents from Iran' or '[s]how me all the word documents that reference Osama Bin Laden."[171] If a suspected terrorist cell is not associated with a specific search term then, the slides refer them to "anomalous events;" defined as a person "whose language is out of place for the region they are in" otherwise, more

[165] *Id.*
[166] *Id.*
[167] *Id.*
[168] *Id.*
[169] *Id.*
[170] Satter, Raphael. (2013). Leaked docs Give New Insight into NSA's Searches
[171] *Id.*

hazily, "someone searching the web for suspicious stuff."[172] One slide has suggested that the Xkeyscore (herein referred to as "XKS)" has led to the capture of around 300 suspected terrorists since 2008.[173]

The question of XKS's value in regards to its efficiency to intrusiveness ratio is largely philosophical. Would a person willingly put their faith in an employee of the NSA or other intelligence agency the expectation that this employee will have the power to sift through their private information as well as millions of others without abusing this power for political or personal gain? Would the arrest of 300 terrorists justify the mass data mining of millions of people's electronic information on a constant basis? The line must be drawn so that the rights of millions will be protected while still allowing LEOs the ability to track criminals and capture them and allowing potentially unlimited use is not the answer.

In the Supreme Court case, *Youngstown Sheet and Tube Co. v. Sawyer*, the Court said that the "absence of authority in the President to deal with a crisis does not imply want of power… the need for new legislation does not enact it[;] [n]or does it repeal or amend existing law."[174] This is analogous to the present issue; the need for intelligence gathering does not mean that the Government has the vested power to do what it wants with its population's private information. The people have that power and government must heed to their rule. In Justice Frankfurter's concurring opinion in *Youngstown*, he stated that "the separation of powers was adopted by the [Constitutional] Convention of 1787 not to promote efficiency but to preclude

[172] *Id.*
[173] *Id.*
[174] *Youngstown Sheet and Tube Co. v. Sawyer*, 343 U.S. 579., 604 (1952) (Frankfurter. Concurring)

exercise of arbitrary power."[175] This is on point with the current situation of warrantless tracking and espionage, using technology as the vehicle to achieve this goal may give the eavesdropping parties a sense of efficiency and dominance but it is nonetheless a grave defiance of the Constitution and a dishonor to the United States' Founding Fathers belief that government efficiency should be limited to "save the people from autocracy."[176]

The NSA justified the use of XKS by asserting that it helps lead to the capture of people in "defense of our nation."[177] How and where the program harvests its intelligence is not totally understandable; it is not palpable what XKS's place is with other recently revealed NSA surveillance programs.[178] Another slide in the training lecture shows that Xkeyscore has 700 servers supporting it in over 150 locations across the planet.[179] The media has gone on to state that XKS can reap up to 42 billion independent bits of records in a month-long period; in fact, it reaped information at such an exponential rate that the intelligence could only be stored in its servers for a few days before forcibly deleting it to prevent a server crash.[180] In some places, up to 20 terabytes can be collected in a day.[181]

The documents that Snowden released showed that the NSA has some in-house restrictions against trigger-happy spying on innocent Americans; however, they appear to be flimsy and vague at best.[182] "On the one hand, it appears that NSA analysts were required to fill out forms asserting that their target was a foreigner before they could pore over the intercepted

[175] *Id*. at 613 (Frankfurter. Concurring)
[176] *Id*. at 614 (Frankfurter. Concurring)
[177] Satter, Raphael. (2013). Leaked docs Give New Insight into NSA's Searches
[178] *Id*.
[179] *Id*.
[180] *Id*.
[181] *Id*.
[182] *Id*.

data."[183] The forms that were unconfirmed were scant of any meaningful detail.[184] The form contained a checklist that asked why a target was foreign (an example would be checking the box next to "the number had a foreign area code.)"[185] An example of a properly completed one illustrates a "justification" text box where a NSA operative can write in more information justifying the eavesdrop; but, the case in point only had vague one-word responses that did not give detailed (or informative) information on the interested subject.[186] It is now clear that the NSA is not totally honest about its recent intelligence leak but it (ironically) is not completely dubious about it either.

Capabilities

Metadata's applications are vast. Here are some of the ways that the NSA's spying apparatus affects the populous. If one uses Twitter, their metadata will indicate that person's location, language, profile biography information and that person's account web address.[187] They will know when your account was created, who you follow and your followers as well as the device used to tweet; they know your location and time zone the tweet was sent in.[188] They also know your unique identifier too![189]

For Facebook, the methodology is the same. Your location is recorded if you check in or update a life event.[190] Like Twitter, they know your biographical information and subscriptions,

[183] *Id.*
[184] *Id.*
[185] *Id.*
[186] *Id.*
[187] Team, Guardian US interactive. A Guardian Guide to Your Metadata
[188] *Id.*
[189] *Id.*
[190] *Id.*

activities as well as your device (like a smartphone.)[191] If you use Google, then your queries will be seen by the NSA as well as the results and the pages you visited from the results.[192] Even simple emails are not safe from the NSA's scrutiny; they get your IP address, recipient's name and email address, and of course the date, time and time zone you were in.[193] They also know the email's subject and its status (whether or not it was read yet.)[194]

Digital cameras are not immune either. The camera gives the authorities the camera's manufacturer and model, camera settings like shutter speed, f-stop, focal length, not to mention the flash type.[195] The picture's resolution and dimensions are known as well.[196] The location of the camera at the time a picture is taken is displayed to the NSA akin to a pop up advertisements online.[197]

Finally, your web browser, the pages you visit and the activity within comes under scrutiny.[198] "[U]ser data and possibly user login details with auto-fill features" are some other key ingredients the NSA espionage network is looking for in their quest for total information awareness (TIA.)[199] The NSA collects cookies stored in your computer too.[200]

---

[191] *Id.*
[192] *Id.*
[193] *Id.*
[194] *Id.*
[195] *Id.*
[196] *Id.*
[197] *Id.*
[198] *Id.*
[199] *Id.*
[200] *Id.*

Benefits and Issues

The reality is that this new technology offers a cornucopia of benefits for law enforcement and the populace at large. Cell phone technology like IMSI and MAC addresses can be used to validly track the location and conversations of a suspected criminal with relative accuracy and ease; it can help the government locate suspected terrorists with great precision. Still, with great power comes the need for even greater accountability as these new inventions have the capability to infringe on our constitutional freedoms and our human dignity. This activity is without any of the appropriate safe guards that is expected by our society and guaranteed by the Constitution.

ISSUE

The issue is simple: there are just not enough safeguards to protect the public's privacy and intimate information when the public is using technology such as cell phones and computers. The use of these tactics by intrusive government and corporate entities in order to maintain national security or law and order has gone too far in the eyes of many.

Recently, the NSA has been found collecting data from millions of Verizon customers on a daily basis.[201] Under the direction of the Obama administration, the NSA has continued his predecessor's policy of actively obtaining information from Verizon customers' phone calls since at least October 4th, 2001.[202] As stated previously this is when the original order was signed under the direction of President George Bush in the abrupt repercussion of the September 11th attacks.[203] The data-mining does not stop at Verizon customers rather, in 2006 USA Today article touched on the NSA's collection of information on subscribers of AT&T and Bell South.[204]

> "These recent events reflect how profoundly the NSA's mission has transformed from an agency exclusively devoted to foreign intelligence gathering, into one that focuses increasingly on domestic communications. A 30-year employee of the NSA, William Binney, resigned from the agency shortly after 9/11 in protest at the agency's focus on domestic activities."[205]

Congressional Audits

In fact, the government's last audit concerning domestic surveillance was in the 1970's when Congress audited the NSA for domestic surveillance capabilities.[206] "At the conclusion of

[201] Greenwald, Glenn. (2013). NSA Collecting Phone Records of Millions of Verizon Customers Daily
[202] *Id.*
[203] *Id.*
[204] *Id.*
[205] *Id.*
[206] *Id.*

that investigation, Frank Church, the Democratic senator from Idaho who chaired the investigative committee, warned: 'The NSA's capability at any time could be turned around on the American people, and no American would have any privacy left, such is the capability to monitor everything: telephone conversations, telegrams, it doesn't matter."[207]

In classified briefings, the NSA has admitted that it does not need a warrant to listen to domestic phone calls to Congress.[208] Congressman Jerrold Nadler disclosed that he was told this at a secret briefing to Congress.[209] In direct violation of American jurisprudence, the only hurtle the NSA needs to overcome in order to eavesdrop on a call is for one of their lower level analysts to make the decision.[210] This sheds more light on how the NSA's surveillance infrastructure works and how the Justice Department interprets the law.[211] Current law allows the NSA to access email, text, phone and instant message without any court approval since the standard used by the DOJ to determine whether phone call eavesdropping demands a warrant applies to this other modes of communication.[212] These mortifying facts eerily resembles George Orwell's classic novel, 1984.

Dangers of Using the Same Comments Twice

The House of Representatives Intelligence Committee (herein referred to as the "House)" hearing went well for the administration officials; it was reported that both Republicans and Democrats treated them well.[213] Fortunately for the American people, the House Judiciary

[207] *Id.*
[208] McCullagh, Declan. (2013). NSA Spying Flap Extends to Contents of U.S. Phone Calls
[209] *Id.*
[210] *Id.*
[211] *Id.*
[212] *Id.*
[213] Yost, Pete. (2013). Hostile Hill Territory on NSA Surveillance Issue

Committee was less than merciful.[214] James Cole, the second in command of the DOJ said, "[w]e are constantly seeking to achieve the right balance between the protection of national security and the protection of privacy and civil liberties," at the House Judiciary Committee.[215] "You've already violated the law as far as I am concerned," rebutted Congressman John Conyers, a ranking member of the committee.[216] "Given the magnitude of this program, I'm frankly surprised it has remained secret,' said Goodlatte [refers to Congressman Bob Goodlatte, the House Judiciary Committee Chairman] 'Why not simply have told the American people that we're engaging in this type of activity in terms of gathering information[;] [i]t doesn't give away any national security secrets in terms of the particular information gathered ... but it might have engendered greater confidence in the public."[217]

Robert Litt, (General Counsel of the Office of the Director of National Intelligence) replied back by saying that making this program public would send everyone they were monitoring a red flag.[218] Representative James Sensenbrenner, sponsor of the PATRIOT Act said that nowhere in the act is there any explicit or implied authorization to actively gather metadata from everyone's cell phones.[219] The third administrative official, John Inglis, Deputy Director of the NSA disclosed a tactic of the NSA known as the three-hop analysis; allowing the NSA to spy on its target, the target's known associates and the associate's known associates (as defined by

[214] *Id.*
[215] *Id.*
[216] *Id.*
[217] *Id.*
[218] *Id.*
[219] *Id.*

his cell phone contacts.)[220] He cites that if the suspect has 40 contacts (the average for a person) then that could lead the NSA into mining two million people's cell phones.[221]

This is one of the few issues in which Republicans and Democrats agree despite their partisan differences.[222] Past investigations were theoretical and had a higher legal emphasis than now.[223] Just imagine what would happen if Congress could muster bipartisan support against, or for the program.

We Can lie about It, Just Not Talk about It

The intelligence community is showing signs that they are becoming more sincere about their dealings with Congress. They released some documents on July 31st, 2013 that were originally given to lawmakers in Washington in 2011 and 2009.[224] The documents confirm what many who are aware already knew; that Congress did know and even consent to the pandemic data mining program.[225] It is reported that the Congress voted to extend the program at least twice.[226]

But why would the NSA commit a treasonous act (in the eyes of the intelligence community) and make public these serious revelations?[227] "The release of the documents is intended to allay concerns that the Obama administration was overstepping its legal authority in carrying out the spy program, which is now under attack in courtrooms from San Francisco to

[220] *Id.*
[221] *Id.*
[222] *Id.*
[223] *Id.*
[224] Kravats, David. (2013). Declassified Memos Confirm Dragnet Phone Surveillance Program was No Secret to Congress
[225] *Id.*
[226] *Id.*
[227] *Id.*

the District of Columbia."[228] An alternate theory is that the NSA does not like the situation it is currently in; they wish to share the blame just as they have been sharing information with the three branches of government.[229]

At the Senate Judiciary Committee hearing on July 31st, 2013 the Deputy Attorney General of the DOJ attended to rail in the fact that "although kept from the American public — was no secret on Capitol Hill."[230] The Deputy Attorney General went further to state that all three branches of government were represented in the data mining agenda.[231] The Judiciary branch was represented by FISC while the Executive branch was the leader of making sure the program went according to their guidelines; let's not forget Congress for its role in passing the laws, oversees their execution, and concluding whether or not the contemporary laws ought to be reauthorized or amended.[232] "The released documents, one dated February 2, 2011[…], and the other December 14, 2009[…], were made 'available to all Members of Congress' to 'inform the legislative debate' as the Obama [A]dministration privately lobbied Congress to reauthorize the programs under Section 215 of the Patriot Act."[233]

Even members of Congress are hopping on the whistleblowing bandwagon as Vermont Senator Patrick Leahy admitted on the day of the previously mentioned Judiciary hearing that the whole program was never a secret among Congress, but also that they cannot discuss it

[228] *Id.*
[229] *Id.*
[230] *Id.*
[231] *Id.*
[232] *Id.*
[233] *Id.*

publically.[234] This goes to show that the massive intelligence fiasco is only widening in scope and blame.

PRISM and its Counterparts

This time the NSA is using 21st century equipment to do its electronic eavesdropping. The NSA has a program called PRISM that was created in 2007 to search the servers of major internet corporations akin to Google, Facebook, and America Online (AOL) to name a few.[235] PRISM stands for "Planning Tool for Resource Integration, Synchronization, and Management," and is the most notorious of the NSA's data mining programs.[236] The heavily used program looks into photo, video, audio, and connection data.[237] Google denies aiding the government in any way.[238] Recent news articles have illustrated that this problem is not unique to the United States, but other countries are cut from the same cloth. The United Kingdom's equivalent is known as GCHQ. Both organizations circumvent the constitutional legal processes used to obtain this sensitive information from unknowing civilians.[239]

> Britain's GCHQ is to file a report to the parliament's Intelligence and Security Committee (ISC) over its alleged links with the covert US spy programme, Prism. The committee's chairman, Sir Malcolm Rifkind, said the eavesdropping agency will give the report "very soon". The GCHQ has been forced to take the step following revelations that it used data gathered from top US internet companies through a secret spy programme by Washington. The Guardian has reported that Britain's intelligence officials had access to the information collected by America's secret surveillance programme. 'The ISC is aware of the allegations surrounding data obtained by GCHQ [through] the US Prism programme. The ISC will be receiving a full report from GCHQ very shortly and will decide what further action needs to be taken as soon as it

[234] *Id.*
[235] Gallagher, Dan. (2013). NSA Snooping Reportedly Includes Google, Facebook, Apple, Others
[236] Dreyfuss, Laura. (2013). What is the NSA's PRISM Program? (FAQ)
[237] Gallagher, Dan. (2013). NSA Snooping Reportedly Includes Google, Facebook, Apple, Others
[238] *Id.*
[239] Gellman, Barton. (2013). U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program

> receives that information,' said Sir Malcolm. The programme was set up by the National Security Agency (NSA) in the US as part of boosting its defence capabilities. Its presence was exposed earlier this week much to the embarrassment of authorities in Washington and London. According to the report, GCHQ had access to the Prism system since June 2010. The agency, however, defended its links saying it is legitimate.[240]

On occasion, the federal government taps the wrong phone numbers.[241] The advocates for a group called the Electronic Privacy Information Center opine that "technological advances have made it harder, not easier, to 'conduct wiretapping in a surgical way' because digital communications often carry many conversations…."[242] In fact, the Federal Bureau of Investigation (FBI) has admitted that over 39,000 hours of recorded information was obtained from the wrong source.[243]

Innocent mistakes add fuel to the flame, there was an instance where the Government tapped the wrong phone number due to a clerical mistake on the part of the telephone company; the difference between typing an "O" and a "0" can have momentous consequences.[244]

In fact, when the FBI first started eavesdropping on their target's emails they not only received their emails but also inadvertently collected emails from other non-targets; their actions were violative of the rights of these non-targeted people.[245] The equipment used was faulty from the get go; it appears that the DOJ intentionally gave them experimental technology for their surveillance practice.[246]

---

[240] GCHQ to File Report over US Prism Spy Programme links
[241] Adler, Andrew. (2013). The Notice Problem, Unlawful Electronic Surveillance, and Civil Liability Under the Foreign Intelligence. 415
[242] *Id.* at 415
[243] *Id.* at 415
[244] *Id.* at 415
[245] *Id.* at 414
[246] *Id.* at 414

SORM

The Russians are beginning to learn that they are not the only ones who spy on their citizens in real time. In Volgograd a man named Nail Murzakhanov, owner of an internet provider in Russia received a request from the Federal Security Service on the subject of access of his subscribers email traffic, to which he refused.[247] In response to his defiance, the Communications Ministry revoked his business license for failure to cooperate with an intelligence agency; a move he countered by filing a lawsuit.[248] Then, to his delight, in August of 2000, he received his license back.[249] The big surprise in this event was that the Russian government balked at his legal counter; giving him his license in a rare fashion.[250]

"Typically, Internet providers in Russia say they do all they can to satisfy the state security services, even if it means turning over the password of every client."[251] Technically, both the Russian and American constitutions give the same rights and protections regarding right to privacy and freedom from LEO's spying on "phone calls, pager communications, radio transmissions, emails or Internet traffic without a court order."[252] However, do to typical enforcement policies and new laws; it is rare for the Russian government to appear before a judge to do their espionage work.[253] "The regulations that allow Russian officials to partake in

[247] LaFraniere, Sharon. (2002). Russian Spies, They've Got Mail Regulations Allow Security Services to Top Into Systems of Internet Providers
[248] *Id.*
[249] *Id.*
[250] *Id.*
[251] *Id.*
[252] *Id.*
[253] *Id.*

these shadowing operations are known as SORM, the Russian acronym for System for Operational-Investigative Activities."[254]

In the US, it is in our jurisprudence to create legal constraints to keep LEO's in check while in Russian jurisprudence the LEO's are fully capable of self-regulation.[255] Despite perestroika taking place in the Russian Federation's birth it has had little impact in helping internet companies fend off the Big Brother like sacking of their contractual obligations or confidentiality to their customers.[256] Many of these firms feel no impetus to challenge the Kremlin on its Brave New World polices; "[t]hey see no sense in putting up resistance[,] [s]o they work out a deal with the FSB [Russian equivalent of the FBI.]"[257] To add insult to injury, Russia has poor troop strength in terms of civil rights attorneys; the little they have are overstretched on fronts from military reform to juvenile justice.[258] In fact, before a 2000 ruling by the Russian court of last resort, the Russian intelligence community did not even have to inform the internet providers that they were eavesdropping on them.[259]

Murzakhanov's stance on the issue raised plenty of hell for him and his family (LaFraniere). His business was audited over 15 times for a plethora of offenses, ranging from tax code compliance to fire code safety.[260] The FSB shut off his main transmission line, forcing him to use undependable and low-quality dial up alternatives.[261] Only after failing to show up to four

[254] *Id.*
[255] *Id.*
[256] *Id.*
[257] *Id.*
[258] *Id.*
[259] *Id.*
[260] *Id.*
[261] *Id.*

court hearings did the Kremlin then reinstate Murzakhanov's license and back down.[262] The Kremlin just felt it was better to lose legitimately than expose the reality of the situation.[263] Nail Murzakhanov is a prime example of what happens when you challenge the belligerent apparatus of government.[264]

SORM's regulations run far and wide; according to SORM "[i]nternet service providers themselves are required to foot the bill for the expensive technology and even train FSB officers to use the equipment to spy on their clients."[265] SORM further regulates that all internet firms place a black box like device on their server and "build a high-speed communications line, which would hot-wire the provider -- and necessarily, all Internet users."[266] Since all this data is streamed right to the FSB headquarters, there is no need for them to get a warrant; in clear violation of Russian law but nonetheless a common practice.[267] Five days into President Vladimir Putin's first term he signed into law a bill that gave the same surveillance power of the FSB to tax police and the interior ministry LEO's, Duma (Russian parliament) and presidential security guards, border patrol and customs agents.[268]

The FSB has even been known to sell data obtained through the program to fill its coffers so it can stay solvent in the post-Soviet economy.[269] "The crisis in Russia has redefined some of the priorities and the Anti-SORM movement is one of the victims of this process, […] [p]eople

[262] *Id.*
[263] *Id.*
[264] *Id.*
[265] Tracy, Jen. (2000). New KGB Takes Internet by SORM The Russian Government has Just Authorized Itself to Spy on Everything its Citizens do on the Net – and to Punish ISPs That Won't Help
[266] *Id.*
[267] *Id.*
[268] *Id.*
[269] *Id.*

are thinking about how to stay alive and they forget the value of freedom."[270] SORM's financial impact can cost providers around $30,000 in compliance costs; more than enough to defunct the small internet providers in Russia.[271] With Russia's long history of authoritarianism, it is not the only European power to engage in mass surveillance.

INDECT

The EU has pondered its own purported 1984-esq surveillance machine. "A five-year research programme, called Project I[NDECT], aims to develop computer programmes which act as 'agents' to monitor and process information from web sites, discussion forums, file servers, peer-to-peer networks and even individual computers."[272] INDECT is built with the aim of detecting violent acts and abnormal behavior.[273] This project gains 10 million in British pounds a year and has some of the UK's top computer scientists nurturing the program till it reaches its goals.[274] "The Indect research, which began this year, comes as the EU is pressing ahead with an expansion of its role in fighting crime, terrorism and managing migration, increasing its budget in these areas by 13.5% to nearly £900 million."[275]

The EU is leading the way in a wider European police force and has asked for the UK to turn in over a third of its member states' LEO's to be trained in continental affairs within five years.[276] This move to a united continental front in law enforcement means that the UK may need to divulge sensitive documents to the rest of the EU LEO's on a more common basis; these

[270] *Id.*
[271] *Id.*
[272] Johnston, Ian. (2009). EU Funding 'Orwellian' Artificial Intelligence Plan to Monitor Public for "Abnormal Behavior"
[273] *Id.*
[274] *Id.*
[275] *Id.*
[276] *Id.*

disclosures include DNA samples and enforcement of transnational warrants.[277] Critiques do not like this one bit; "[t[he EU lacks sufficient checks and balances and there is no evidence that anyone has ever asked 'is this actually in the best interests of our citizens?"'[278] Some feel this is a move to profile entire populations instead of just shadowing on individual; however, these allegations lack any substance beyond their imagination.[279] Agents will continuously monitor websites, forums, servers, and personal computer systems akin to their Russian and American counterparts.[280]

Similar EU programs like "[ADABTS] – the Automatic Detection of Abnormal Behaviour and Threats in crowded Spaces – has received nearly £3 million[;] [i]ts is based in Sweden but partners include the UK Home Office and BAE Systems."[281] The ADABTS program will be equipped with an algorithm that allows it to seek and find (via CCTV) people who it perceives to act violently.[282] EU programs like ADABTS are said to eventually come under the sphere of influence of the EU Joint Situation Centre (SitCen), this organization has been described as the EU version of the CIA.[283] Critics contend that SitCen's involvement should come under serious scrutiny since it is a very secret agency.[284] "The expansion of what is effectively the beginning of an EU 'secret service' raises fundamental questions of political oversight in the member states."[285]

[277] *Id.*
[278] *Id.*
[279] *Id.*
[280] *Id.*
[281] *Id.*
[282] *Id.*
[283] *Id.*
[284] *Id.*
[285] *Id.*

French Big Brother

Just like the US, Russia and the UK, France runs a network of vast intelligence gathering much like the NSA's PRISM program; this is purportedly run by the French DGSE.[286] They have followed in the footsteps of the NSA as they seek to spy on phone calls and internet activity, especially those of international calls.[287] It is thought that they do this with the intent of looking "not so much at content[,] but to create a map of 'who is talking to whom."[288] The French keep these records in massive servers under the DGSE headquarters in Paris.[289] In fact a technical supervisor for the DGSE said that the server was "probably the biggest information centre in Europe after the English."[290]

France was among the quietest of Europe when the revelation of the NSA PRISM scandal came out.[291] Even though the French were spied on by the United States, they probably did not complain simply because they had the same end game too![292] Later however, the French president condemned the US for its acts of secrecy; even going as far as advocating postponing talks for the US-EU free trade treaty.[293] France further asserted that they did not spy on the American embassy because they did not think that's something acceptable to do to an ally.[294]

[286] Chrisafis, Angelique. (2013). France 'Runs Vast Electronic Spying Operation Using NSA-Style Methods' Intelligence Agency has Spied On French Public's Phone Calls, Emails and Internet Activity
[287] *Id.*
[288] *Id.*
[289] *Id.*
[290] *Id.*
[291] *Id.*
[292] *Id.*
[293] *Id.*
[294] *Id.*

Allied Spying

It is one thing to spy on so called "enemies" it's another thing to spy on your allies. One of the documents by Edward Snowden has shown that the US has actively spied on its allies' embassies and mission in the US.[295] "One document lists 38 embassies and missions, describing them as 'targets[;]' [i]t details an extraordinary range of spying methods used against each target, from bugs implanted in electronic communications gear to taps into cables to the collection of transmissions with [specialized] antennae."[296] Some of those embassies include EU missions and the allied embassies of South Korea, Greece, Japan, Mexico, India and Turkey.[297] The bugging method was codenamed Dropmire, a surveillance device planted on a secure fax machine at the EU mission in Washington; the fax machine is used to transmit sensitive cables across the ocean to Europe.[298] It is suggested that the US does this "to gather inside knowledge of policy disagreements on global issues and other rifts between member states."[299] "Germany's justice minister, Sabine Leutheusser-Schnarrenberger, demanded an explanation from Washington, saying that if confirmed, US behaviour 'was reminiscent of the actions of enemies during the cold war."[300] Other intelligence operations have gone as far as to set up antennas near the mission to investigate the EU-American disagreements; the operation even gained a (supposedly) complete copy of a computer hard drive content from the EU.[301] The codename for the French

[295] MacAskill, Ewen. (2013). New NSA Leaks Show How US is Bugging its European Allies Exclusive: Edward Snowden Papers Reveal 38 Targets Including EU, France and Italy
[296] *Id.*
[297] *Id.*
[298] *Id.*
[299] *Id.*
[300] *Id.*
[301] *Id.*

embassy information gathering was named Wabash, while the Italian equivalent was known as Hemlock.[302]

Corporate Espionage

The threat does not stop with the government. Electronic surveillance on employees has been a staple of companies for many years.[303] "Some companies routinely check phone records of employees, monitor what websites they visit, and read emails and instant messages [of their employees.]"[304] Experts say that all phone calls on their work phone, text, as well as social media activity are fair game for employer espionage.[305] Some companies like Goldman Sachs have tailored their email records in a searchable format; using email-scanning applications akin to Websense and Spector Pro that can scan for profane language or other keywords in addition to searching for spam.[306]

Some companies do not bother to hide their snooping from their employees. For years, employees of the media company Bloomberg would get a pop up page on their computer if they tried to send an email containing profanity with the profane word, other times the program simply would not allow them to send the email.[307]

Technology firm Google has stated that it will issue a transparency report of all the instances in which the U.S. government has requested information about their programs.[308] Google's chief Legal Officer made a public letter to the federal government asking them for their

[302] *Id.*
[303] Fottrell, Quentin. (2013). Who's a Bigger Snoop: the NSA or Your Boss?
[304] *Id.*
[305] *Id.*
[306] *Id.*
[307] *Id.*
[308] Perez, Evan. (2013). Tech Firms Push Back Over NSA Secrecy

permission in releasing this data.[309] Twitter and Microsoft have supported Google's move.[310] Facebook is reluctant to release this information on technical grounds.[311] Google's legal counsel formally asked the FISA court to lift their gag order, so they may give the promised detailed transparency report on the Government's surveillance requests to the public, citing their First Amendment rights apply to this case.[312] So far the Federal government has yet to respond.

The recent NSA mass surveillance has its economic effect.[313] Both Google and Facebook have denied any participation in the surveillance of the American populace; but the idea of them talking the same story in court- as sworn testimony is fanciful at best.[314] Unfortunately, due to current law, it is impossible for Google (or any other company) to give a complete disclosure of the information requested by the federal government.[315] Time will tell if the request for a full and transparent report is heeded.[316]

Sometimes the Corporate World works with the Government. Interview with NSA analyst: there are over 50 companies that have received court orders to comply with the NSA's eavesdropping program.[317] This is an issue because court orders do not receive the same scrutiny as a warrant. There are fewer safeguards and when court orders are utilized they are used as a means of legitimizing the unconscionable behavior of the Government's methods to feed its bottomless appetite for raw data. No form of digital communication is safe.[318] Textual material is

[309] *Id.*
[310] *Id.*
[311] *Id.*
[312] Flaherty, Anne. (2013). Google Asks FISA Court to Lift Gag Order
[313] Pimmentel, Benjamin. (2013). Why Google, Facebook, Must Nip Spy Tag Analyst Warns of Fears of a 'U.S. Version of the Chinese Internet'
[314] *Id.*
[315] *Id.*
[316] *Id.*
[317] Cavanaugh, Tim. (2013). What Do They Know About You? An Interview With NSA Analyst William Binney
[318] *Id.*

the easiest to get; phone call volumes are too large in dimension to record outside of their target list.[319] The NSA does not have the technical capacity to transcribe the data they have; this is a long term goal for them.[320] Developing algorithms to locate useful information is a key area the NSA lacks in.[321]

Retail Tracking

Some retail stores are tracking their customer's smartphones while they shop.[322] Retail company Nordstrom partook in an experiment in one of their stores; they began to use technology to track their customers in the store.[323] Though the store notified their customers of their surveillance via a sign that they posted in the store, there were many unnerved customers.[324] This is an example of the larger movement of retailers striving to learn more about their patrons while they are actively looking through the store.[325] The information the retailer is looking for varies from customer's gender to how long they spend at a particular isle.[326]

Some stores have installed cameras that can tell the retailers your mood and how long you look at something before you choose to buy it (or walk away.)[327] Other retail firms like Family Dollar and Warby Parker are following Nordstrom's lead.[328] The aims of these companies endeavors is to improve the way they interact with their customer base; this technology will give them the opportunity to tally everything from how many people come in to

[319] *Id.*
[320] *Id.*
[321] *Id.*
[322] Clifford, Stephanie. (2013). Attention, Shoppers: Store Is Tracking Your Cell
[323] *Id.*
[324] *Id.*
[325] *Id.*
[326] *Id.*
[327] *Id.*
[328] *Id.*

the store during peak times to data that will show them how to specifically place the products in their aisles.[329] Many customers find this alarming that their moves are mapped by the retailers without their knowledge.[330] Retailers defend by citing that their actions are no different than what websites do to consumers by the use of cookies.[331]

Studying consumers while they search for items to purchase may prove to be a highly technical field. "One [such company], RetailNext, uses video footage to study how shoppers navigate, determining, say, that men spend only one minute in the coat department, which may help a store streamline its men's outerwear layout."[332] RetailNext collects data from shoppers' phones in order to obtain more precise information about them.[333] If the store offers Wi-Fi then the store can then access the data from the shoppers' cell phones if they are set to search for Wi-Fi signals, regardless of whether the phone connects to the Wi-Fi.[334] RetailNext's system can recognize return customers so retail companies can time average visits and the time span in between visits.[335] This retail tracking could become burdensome on the customer as it could be used to determine potentially sensitive shopping habits of the customer plus there is no penalty on the company to share this information with other companies or third parties for a price.

Another retail spy company, Brickstream is an Atlanta based company that specializes in video surveillance.[336] Their $1,500 stereoscopic cameras can count the number of people in a

[329] *Id.*
[330] *Id.*
[331] *Id.*
[332] *Id.*
[333] *Id.*
[334] *Id.*
[335] *Id.*
[336] *Id.*

certain area of the store and can differentiate the facial expressions of their customers.[337] London based, Realeyes and St. Petersburg based Synqera, have systems that are similar to Brickstream but uses the facial expressions, age and gender recovered to make personalized advertisements and coupons.[338] "Nomi, of New York, uses Wi-Fi to track customers' behavior in a store, but goes one step further by matching a phone with an individual."[339] If a patron offers up some personal information, the Nomi program creates a profile of that customer; retailers can use this information to give customers personal recommendations and send personal coupons.[340] Nomi combines this with its Wi-Fi cell phone tracking to accomplish this goal.[341]

Corporate Double Agents

Sometimes the government is the corporation's adversary. A recent document has surfaced that could implicate the CIA in a major economic sabotage ring.[342] The document is a manual that instructs its agents on how to deliberately work in an inefficient, slow or moral killing manner in order to undermine the company they are employed.[343] There are roughly ten tell-tale signs that your supervisor or co-worker could be a government crony with the goal of disruption.[344] The manual encourages its disciples to deliberately make decision making at the firm as time consuming as possible.[345] They are prone to being extremely talkative; "Make

[337] *Id.*
[338] *Id.*
[339] *Id.*
[340] *Id.*
[341] *Id.*
[342] Arends, Brett. (2013). 10 Signs Your Co-Worker is a Spy Commentary: Why Colleagues Might be Making it Harder to do Your Job
[343] *Id.*
[344] *Id.*
[345] *Id.*

speeches,' the government advises agents. 'Talk as frequently as possible and at great length[,] [i]llustrate your 'points' by long anecdotes and accounts of personal experiences."[346]

These operatives are trained to take issue with minor flaws in otherwise perfect work.[347] They take issue with specific words or phrases used in office communications, final work products and meeting minutes.[348] These agents are not big fans of res judicata (accepting things as they are and moving on,) they have been known to try to open up and undermine past decisions made in the company that they work.[349] They delay major decisions with accusations that the employee hasn't the proper authority to implement the decision; like a judge inquiring about whether the plaintiff's counsel has filed his complaint in the proper venue the corporate double agent can be counted on to question employees decisions for lack of proper jurisdiction.[350] They make life more difficult with heightened "red tape" as they try to expand on the current bureaucratic infrastructure.[351] "They 'multiply the procedures and clearances involved in issuing instructions, pay checks, and so on' and 'see that three people have to approve everything where one would do[].'"[352]

Lastly, they have crafted the fine art of corporate mismanagement and rumor spreading.[353] The double agents will give preference to the inefficient workers, even going as far as to giving them priority status when it comes time to promotions or raises.[354] Efficient workers are to be treated as second class citizens; their work is unjustly discriminated against for the most

[346] *Id.*
[347] *Id.*
[348] *Id.*
[349] *Id.*
[350] *Id.*
[351] *Id.*
[352] *Id.*
[353] *Id.*
[354] *Id.*

rudimentary of flaws or at the very least overlooked in favor of lesser work.[355] The reasoning behind this sinister activity is fanciful.

These recently revealed problems show that there are parallels in the government's and company's use of technology to circumvent long standing legal due process principles to obtain sensitive information crucial to our privacy. Sometimes the law is inadequate to be effectively applied to the predicament; other times there is a complete lack of relevant law to begin with.[356] Major communications corporations have to design their communications products and services with eavesdropping in mind as required in CALEA.[357] Passed in 1994, CALEA was originally deemed necessary for the continuity of enforcing the law; the digital revolution at the time had overwhelmed law enforcement.[358] Due to the sheer nature of wireless communications, it was no longer possible for law enforcement officials to obtain all needed surveillance from one provider.[359] With CALEA, government has made it cheaper, fast and easier to eavesdrop on the populace than ever before.[360] So regardless of one's political views the need for greater protection and accountability is paramount.[361]

Password Demand Letters

The Government sometimes asks companies for access to their users passwords in order to avoid having to go to the courts and the possible issue of whether or not a warrant is needed in order to obtain the password as well as use it to log on to a user's website account and shadow it

[355] *Id.*
[356] Fottrell, Quentin. Who's a Bigger Snoop: The NSA or Your Boss?
[357] Gidari, P Coie. (2006). Designing the Right Wiretap solution: Setting standards Under CALEA IEEE Security & Privacy. 29
[358] *Id. at 29*
[359] *Id. at 30*
[360] *Id. at 30*
[361] *Id. at 30*

or use it.[362] "If the government is able to determine a person's password, which is typically stored in encrypted form, the credential could be used to log in to an account to peruse confidential correspondence or even impersonate the user."[363] Thankfully, companies have been reluctant to give out their user's passwords to a government entity; these companies heavily scrutinize these demands.[364] Internet companies have even received requests for algorithms and "salts" to the requested passwords.[365]

"A salt is a random string of letters or numbers used to make it more difficult to reverse the encryption process and determine the original password."[366] There are companies that have chosen to come out in the open and publicly deny that they would ever comply with the government's request; Microsoft is one of them, when one of its representatives was asked whether they would participate in a government's request for salts or password algorithms they said, "[n]o, we don't, and we can't see a circumstance in which we would provide it."[367] Google has stated that it has a legal team on standby ready to defend the company against any government legal action against their moratorium on password divulgence.[368]

The clarity regarding these demands is not clear.[369] It is not public knowledge whether these requests are for individual passwords or for the entire database.[370] The PATRIOT Act has been used to obtain whole databases of phone records so it could be conceivable that they would

[362] McCullagh, Declan. (2013). Feds Tell Web Firms to Turn Over Users account Passwords
[363] *Id.*
[364] *Id.*
[365] *Id.*
[366] *Id.*
[367] *Id.*
[368] *Id.*
[369] *Id.*
[370] *Id.*

apply this provision to password information as well as passwords are arguably similar to phone record databases.[371]

Assuming that a LEO or surveillance operative obtained a salt or algorithm there is no guarantee that they would be able to crack the encryption codes used to hide it from the unauthorized eyes of the outside world.[372] The password's complexity and the type of algorithm will determine if Big Brother will be able to access the password; algorithms are made to scramble the password into an unreadable string of letters and numbers to evade the chance of it falling into the wrong hands.[373] "One popular hash function called MD5, for instance, transforms the phrase 'National Security Agency' into this string of seemingly random characters: 84bd1c27b26f7be85b2742817bb8d43b."[374]

Any computer that contains a video card has the capability to test the different "hashes" (possible random characters hidden in MD5's password transformation) at a rate of billions per second.[375] To combat this, most tech firms have chosen to develop an algorithm to design a password encryption in such a way as to deliberately ratchet the cost of decoding it sky high.[376] Bcrypt, an encryption algorithm used by Twitter can be decoded in a year for a cost of $4 if the password is only eight characters long (composed only of letters.)[377]

[371] *Id.*
[372] *Id.*
[373] *Id.*
[374] *Id.*
[375] *Id.*
[376] *Id.*
[377] *Id.*

If the government wanted to crack a Bcrypt password of eight letters on a daily basis then it would cost them an average of $1,500.[378] If you add asterisks, numbers and other special characters then the cost will skyrocket to a whopping $130,000 per code (that is, assuming they wish to decrypt a code a year.)[379] It is very likely that the NSA or FBI may choose to use application-specific integrated circuits (ASIC) in order to do their mass decrypting because it is the most cost effective on a large scale.[380]

Questions of Law

Does the government have the legal authority to command internet companies to deliver encrypted passwords, salts and algorithms? This is a very (legally speaking) debatable question.[381] Are there circumstances where the populous could see their passwords taken by the government for their own purposes?[382] There is no known precedent for such a demand to have any legal force.[383] If the government were to use a password to log into its corresponding account; it would amount to a prospective surveillance which would need a FISC order.[384] This could also raise issues under the CFAA too.[385]

All the on point cases controlling this situation deal with the defendant having to unilaterally give the government the password so the Government may use the information it unlocks against them.[386] In 2011, a United States Attorney from the Northern District of Florida

[378] *Id.*
[379] *Id.*
[380] *Id.*
[381] *Id.*
[382] *Id.*
[383] *Id.*
[384] *Id.*
[385] *Id.*
[386] *Id.*

subpoenaed a man named John Doe who they attempted to gain access to the password of his encrypted information from his laptop for evidence of child pornography.[387] In this case the grand jury issued a subpoena demanding John Doe to appear before the court since the forensics lab could not decrypt John's laptop device and portable hard drive.[388] John Doe informed the United States Attorney before appearing at a grand jury hearing that he would assert his Fifth Amendment right against self-incrimination, thereby denying the prosecutor's demands.[389]

The forensic examiner in the case, Timothy McCorhan testified both that the laptop and portable hard drive had been encrypted with TrueCrypt, a device aimed at encrypting software to hide its contents from intruders but also that there was a possibility that there was nothing illegal encrypted by it.[390] Despite this turn of events, John Doe was held in contempt and he was turned over to the custody of a federal LEO.[391] In 2012, on appeal, the United States Circuit Court for the Eleventh Circuit upheld John's use of his Fifth Amendment protection against self-incrimination to refuse to release the codes needed to decrypt his laptop and hard drive data.[392]

But, "[i]n January 2012, a federal district judge in Colorado reached the opposite conclusion, ruling that a criminal defendant could be compelled under the All Writs Act[393] to type in the password that would unlock a Toshiba Satellite laptop."[394] In the case, defendant

[387] *United States v. Doe*, 670 F.3d 1337 (11th Cir. 2012)
[388] *Id*. at 1339
[389] *Id.* at 1340
[390] *Id*.
[391] *Id*.
[392] *Id*. at 1341
[393] Referring to 28 U.S.C. § 1651
[394] McCullagh, Declan. (2013). Feds Tell Web Firms to Turn Over Users Account Passwords

Ramona Fricosu's home was searched under the guise of a warrant and the LEOs seized three computers, one of which was the Toshiba laptop which was password encrypted.[395]

Still, the issue presented is not addressed. The above mentioned cases only deal with passwords that belong to the subject of an investigation; not of someone's encoded password saved in the server of a third party company.[396] In trial, a recorded conversation Ramona had with another person where she discussed having something on her laptop that (she alluded) was password encrypted.[397] The District Court went on to "conclude that the government has met its burden to show by a preponderance of the evidence that the Toshiba Satellite M305 laptop computer belongs to Ms. [Ramona] Fricosu, or, in the alternative, that she was its sole or primary user, who, in any event, can access the encrypted contents of that laptop computer… and conclude that the Fifth Amendment is not implicated by requiring production of the unencrypted contents of the Toshiba Satellite M305 laptop computer."[398] The District Court went on to hold that the All Writs Act was the decisive factor in this decision.[399]

Litigation

In 2006, AT&T, Verizon and BellSouth filed a complaint that alleged the NSA compelled them to give the NSA access to their phone records up to a few months before September 11th, 2001 attacks.[400] The pleading spurned the Bush Administration and the NSA for their violative actions; a clear disobedience, the pleading held, to the Constitution and the

[395] *United States v. Fricosu*, 841 F. Supp. 2d 1232 (D. Colo. 2012)
[396] *Id*.
[397] *Id*. at 1235
[398] *Id*. at 1237
[399] *Id*. at 1238
[400] Harris, Andrew. (2006). Spy Agency Sought U.S. Call Records Before 9/11, Lawyers Say

Communications Act of 1934.[401] This is amid more "than 30 suits have been filed over claims that the carriers, the three biggest U.S. telephone companies, violated the privacy rights of their customers by cooperating with the NSA in an effort to track alleged terrorists."[402] The DOJ has retreated to its standard policy of neither confirming nor denying AT&T's involvement in NSA telecommunications crusade; divulgences like this would present "exceptionally grave harm to national security,' and would violate both civil and criminal statutes."[403]

The NSA asked the telecom firms to build a server center for their exclusive access; this was called the "Pioneer Groundbreaker" initiative.[404] The NSA ultimately decided that it would be more feasible and more efficient to just have direct access to their servers.[405] In June 2000, the NSA publically announced that they were in quest of bids for a venture to ``modernize and improve its information technology infrastructure."[406] This was said to be a part of Pioneer Groundbreaker.[407] "On June 9 [2006], U.S. District Court Judge P. Kevin Castel in New York stopped the lawsuit from moving forward while the Federal Judicial Panel on Multidistrict Litigation in Washington rules on a U.S. request to assign all related telephone records lawsuits to a single judge."[408] Verizon's representatives have tried to debunk allegations that they willingly allowed the NSA access to their stored information but simultaneously refused to comment on Verizon's involvement with Pioneer Groundbreaker.[409]

---

[401] *Id.*
[402] *Id.*
[403] *Id.*
[404] *Id.*
[405] *Id.*
[406] *Id.*
[407] *Id.*
[408] *Id.*
[409] *Id.*

Al-Haramain v. Obama

Under § 1810 of FISA, it is possible to find the government civilly liable for eavesdropping on people or corporate non-profits if it can be found that this happened without a warrant.[410] The case does raise some Sovereign Immunity concerns; previous courts have ruled that vague laws in civil cases against the Government are construed to favor the sovereign.[411] Al-Haramain Islamic Foundation was recently embroiled in a suit against the FBI for warrantless wiretapping and lost in trial, holding that § 1810 of FISA waives Sovereign Immunity.[412] The issue in the case was "whether the government waived sovereign immunity under FISA's civil liability provision…."[413] On appeal, the Ninth Circuit Court of Appeal vacated the lower court's ruling by citing that there was no explicit waiver of Sovereign Immunity.[414] Ruling that "Al Haramain's suit for damages against the United States may not proceed under [FISA's] § 1810."[415]

This same decision however, affirmed the lack of personal responsibility of FBI Director Mueller to Al- Haramain for any loss in the dispute.[416] The Court stated in their reasoning that the argument of holding the Director personally liable for his official conduct is nothing more than a "sideshow."[417] The Court goes on to say that Al-Haramain never took their claim against Mueller seriously; it was mentioned that at a trial hearing they referred to their claim against

[410] *Al-Haramain Islamic Foundation v. Obama*, 705 F.3d 845 (9th Cir. 2012)
[411] *Id.* at 850
[412] *Al-Haramain Islamic Foundation v. Obama. Et al*
[413] *Id.*
[414] *Id.* at 855
[415] *Id.*
[416] *Al-Haramain Islamic Foundation v. Obama. Et al*
[417] *Id.*

Mueller as "a corollary we needn't get to."[418] Al-Haramain's claims against Mueller were based on statements to facilitate "Mueller 'threatened to resign because of concerns about the legality of the warrantless surveillance program;' and 'Mueller testified before the House Judiciary Committee [] that in 2004 the FBI, under his direction, undertook activity using information produced by the NSA through the warrantless surveillance program."[419] According to the Court, this is not a proper claim under FISA.[420]

Fifth Circuit Upholds Mass Surveillance

The United States Fifth Circuit Court of Appeals just reversed a lower court's ruling regarding the wireless wiretapping; they ruled that the federal government does not need a warrant to access mobile-phone subscribers' cell-site information.[421] In this case the Court was asked to determine whether the District Court's ruling that the Stored Communications Act[422] (SCA) violates "the Fourth Amendment because the Act allows the United States to obtain a court order compelling a cell phone company to disclose historical cell site records."[423] The major point of contention regarding the statute was the phrase "only if"[424] in its clause detailing when a court order is justified to allow the shadowing of cell phone data.[425] The Court reasoned that the prior precedent has viewed the phrase, "only if" as a "necessary condition, not a sufficient condition."[426] On this question, the Court upheld the lower court's court order; when it comes to locational information given off by cell phones, the Court conceptualized the cell

[418] *Id.* at 855
[419] *Id.*
[420] *Id.*
[421] Kravets, David. (2013). Cops Can Track Cellphones Without Warrants, Appeals Court Rules
[422] Referring to 18 U.S.C. §§ 2701-2712
[423] *In Re. Application of the United States for Historical Cell Site Data*, 724 F.3d 600, 605 (5th Cir. 2013)
[424] see 18 U.S.C. § 2703(d)
[425] *In Re. Application of the United States for Historical Cell Site Data*, 724 F.3d at 606
[426] *Id.*

phones vulnerability to tracking as a form of business record used by the service provider and acknowledged by the phone user.[427]

The decision was split 2-1, they are the second court to rule in favor of the government since the NSA surveillance scandal began; a third judge ruled that the federal government needed a warrant in order to use the tools of electronic surveillance.[428] The United States Supreme Court has remained mute on the issue but did reject an appeal from a narcotic courier sentenced to 20 years after being arrested with a half a ton of marijuana.[429] He was found in a motor home, the authorities tracked via his cell phone pinging cell towers for days across many states.[430]

"In the end, the Fifth Circuit, which sets law in Louisiana, Mississippi and Texas, concluded today that the locational history of a mobile phone does not enjoy constitutional protections because the government has not performed the tracking, and that the data is simply a business record owned by carriers".[431] The Court cited that the cell phone providers record and store the information for their own business purposes.[432] The Court further stated that the government does not require the mobile providers to give them or even record such data and it is the companies that control how much data can be recorded.[433] The Government's argument was that a cell phone provider may unveil chronological cell-site reports fashioned by the company in its commonplace route of business; as long as such an order is based on a showing of "specific

[427] *Id*. at 606-612
[428] Kravets, David. (2013). Cops Can Track Cellphones Without Warrants, Appeals Court Rules
[429] *Id*.
[430] *Id*.
[431] *Id*.
[432] *Id*.
[433] *Id*.

and articulable facts."[434] Specific and articulable facts are sensible proof to support that the records wanted are pertinent and material to an enduring criminal investigation.[435]

There is an estimated 326 million wireless subscriber accounts in the US; this is actually higher than the population.[436] An ACLU representative said in reference to the case "This ruling fails to recognize that Americans do in fact have a reasonable expectation of privacy in their cell phone location information[;] [w]here you go can reveal a great deal about your life, and people don't think that carrying a cell phone around means that someone can get a detailed record of their movement for days or even months on end."[437] Now they feel, the Fifth Circuit has created a legal precedent that does just that.

Partisan Divide

The recent revelation of the NSA's surveillance has Americans split on partisan lines; about 64% of Democrats find it acceptable that the NSA is monitoring their calls while only 37% did during the Bush administration years.[438] Three-fourths of Republicans liked when the Bush administration monitored their calls; now only a bare majority does.[439] President Obama will not lose much from this fiasco.[440] Overall, there is a declining number of Americans who think NSA mass surveillance is a good thing; only 45% of "young" Americans are okay with the NSA's mass surveillance.[441]

---

[434] *Id.*
[435] *Id.*
[436] *Id.*
[437] *Id.*
[438] Bartash, Jeffrey. (2013). Democrats, Republicans Switch Views on NSA Surveillance
[439] *Id.*
[440] *Id.*
[441] *Id.*

International Front

This section delves into the reactions of the European populous to the revelations of Edward Snowden's leak of documents related to the United States mass data reaping campaign (Germany,) and similar eavesdropping crusades in other nations (Russia.) Relevant statutory law is also mentioned concerning how it impacts privacy issues and how it relates to EU law on issues of control and precedent of the situation.

In Moscow, the officials of the city's metro system are thinking of establishing a cell tracking system to deter people from stealing cell phones.[442] The purpose of this is debatable, advocates claim that it will be used as a crime fighting method while privacy supporters find it extremely intrusive and that its' true nature is more nefarious.[443] "According to Mokhov [referring to the police operations chief of the Moscow metro, Andrey Mokhov], the action radius of each reading device is five meters. For the system to be successful, he said the devices would have to be installed into every CCTV camera inside stations, lobbies, and metro cars."[444] As the passengers near the sensor, it automatically identifies their phone number; if the phone's SIM card is on the "missing" list then the phone is flagged for the police to respond.[445]

The critics of Moscow's fledgling surveillance state are united in asserting that this is a flagrant violation of privacy and Russian law.[446] The critics cite the lack of a meaningful way to profile those who they should keep their attention on versus the innocent populous.[447] Moscow

[442] Police to Track Moscow Metro Passengers' SIM Cards. (2013)
[443] *Id.*
[444] *Id.*
[445] *Id.*
[446] *Id.*
[447] *Id.*

officials argue that the system is legal because they are not tracking people, but rather property of different companies (the phone is considered property of the company;) critics stressed that the mobile device is the property of the passenger – not the phone company.[448] This legal loop-hole has not waived the flare of the critic's passion for the halt of the installation; "Many surveillance technologies are created and deployed with legitimate aims in mind, however the deploying of IMSI… catchers sniffing mobile phones en masse is neither proportionate nor necessary for the stated aims of identifying stolen phones."[449]

While mobile phone robberies run like a pandemic in the Moscow metro system, critics contend that the system will be a waste of tax payer money.[450] They affirm that in the US, when a cell phone is stolen the victim calls their provider who then disables their phone; regardless of whether their SIM card is still in it.[451] Russian lawyers say that thieves normally get rid of the SIM card after they steal the phone.[452] With that logic in mind, an LEO can still trace the phone by its own International Mobile Station Equipment Identy (IMEI) number.[453] Some believe that the real aim for this system is to protect the metro from a terrorist attack.[454] The Moscow metro has been the victim of three attacks in the last ten years.[455]

Merkel's Election Woes

In contrast to the dilemma in Russia, Germany's problems deal with public reaction to the surveillance state of its primary ally, the United States, impact on their self determination.

[448] *Id.*
[449] *Id.*
[450] *Id.*
[451] *Id.*
[452] *Id.*
[453] *Id.*
[454] *Id.*
[455] *Id.*

German Chancellor Angela Merkel has been recently pummeled by questions regarding the surveillance program the NSA has orchestrated here in the US.[456] "Merkel's opponents in the Sept[ember] 22 parliamentary elections have seized on the issue, asserting that she has not done enough to protect [the] Germans' privacy[;] [a]lthough polls show Merkel with a comfortable lead, the issue has created turbulence in what had looked like a smooth glide to a third term as chancellor."[457] There were allegations that the US was spying on its European allies.[458] With memories of the Nazi Gestapo and the East German Stasi fresh in the nation's mind the recent news of the NSA's eavesdropping campaign had an eerie historical relevance in today's Germany.[459]

Chancellor Merkel has denied that she is stalling till the election before giving the German people the rightful answers regarding the full details of PRISM.[460] "I have to take note that our American partners need time for the examination ... [;] [i]t wouldn't help to have an answer that would later turn out not to be truthful,' she said[,] 'So I prefer to wait."[461] Chancellor Merkel sent the Interior Minister, Hans-Peter Friedrich to the United States to inquire on the dilemma that has befouled the American government.[462] When he came back, he came away pointing to the significance of intelligence in preventing attacks; prompting Chancellor Merkel's liberal opponents to deepen their criticism over what they describe as an lacking effort to look after Germans' personal data.[463] The German government has been inundated with questions over

[456] Baetz, Juergen. (2013). Germany's Merkel Urges Patience on NSA Answers
[457] *Id*.
[458] *Id*.
[459] *Id*.
[460] *Id*.
[461] *Id*.
[462] *Id*.
[463] *Id*.

the niceties of those programs, with NSA whistleblower Snowden's allegations overshadowing such issues as Europe's economic depression.[464] The Chancellor's center-left challenger, Peer Steinbrueck has called some of her comments regarding the fiasco "alarming" and a sign of "cluelessness and helplessness."[465]

To make matters worse for Chancellor Merkel, there have been several protests regarding the recent revelations about the NSA mass surveillance scandal.[466] "Protesters, responding to calls by a loose network calling itself #stopwatchingus, braved searing summer temperatures… to demonstrate in Hamburg, Munich, Berlin and up to 35 other German cities and towns."[467] Many showed their support to NSA whistleblower Edward Snowden by showing billboards made to chastise the NSA for its role in the information reaping front.[468] In the opposite side of the spectrum, the revelation that the US is actively violating European privacy services as a catalyst for the EU to accelerate its own surveillance programs.

European Union's (EU) Drone Fleet

The intelligence reaping front the NSA has operated has coaxed the EU to create a fleet of drones, satellites and planes to stimulate their defense industry.[469] The European Commission has created a multi-page report on how the EU could strengthen its defenses.[470] The report boasts

[464] *Id.*
[465] *Id.*
[466] Press, Associated. (2013). Thousands Take to Streets in Germany to Protest US Surveillance of Internet
[467] *Id.*
[468] *Id.*
[469] EU's Response to NSA? Drones, Spy Satellites Could Fly Over Europe
[470] *Id.*

a full deployment of developing technologies for its use, including drones, and "equipment to detect chemical, biological, radiological, nuclear and explosives threats (CBRNE.")[471]

This technology, coupled with the use of satellites and aircraft will prove to be a major step in the move to become more like the US.[472] "Lamenting the absence of a structural link between civil and military space activities in the EU and saying that Europe 'can no longer afford' the economic and political cost of such a divide, the Commission focused on several technologies that are said to be able to serve both civilian and defense objectives."[473] There is a space surveillance and tracking (SST) system being put into place which paves the way for a supranational spying apparatus that is not seen anywhere else.[474]

This is seen by some as the beginning of an EU-breed defense and intelligence bureau.[475] Its critics think that this new bureau will just be an EU-spawned NSA bent on spying on the EU masses.[476] In fact, "Open Europe… [think tank based in Europe] has already warned that the EU 'has absolutely no democratic mandate for actively controlling and operating military and security capabilities."[477] Open Europe has opined that the nations of the EU are best served by an inter-country defense projects; they view the EU Commission's recommendations as advocating nation building in Europe.[478]

---

[471] *Id.*
[472] *Id.*
[473] *Id.*
[474] *Id.*
[475] *Id.*
[476] *Id.*
[477] *Id.*
[478] *Id.*

Ireland

In Ireland, the authorities will not pursue any coercive legal action against Facebook or Apple over their compliance with the NSA collection of personal data.[479] Due to an agreement signed between the NSA and the corporations their one-way data torrent practice is a perfectly legitimate covenant.[480] The Irish government has stated that it cannot bring sanctions against Apple or Facebook because they signed a "safe harbor" agreement; this accord means that they acted under the full umbrella of EU law; the safe harbor agreement is an approved contractual agreement by the European Commission, depriving the Irish LEOs and of jurisdiction.[481] The Irish government cites, ironically, that the safe harbor accord is a mechanism for the safeguard of the Irish people's digital data.[482] This revelation has caused uproar over whether the safe harbor agreements are still providing the safety that is in its namesake or if they are safe at all.[483]

Long Term Goals and Global Hegemony

The safe harbor issue in Ireland is only a staple of things to come; the American government's long term goals for its data reaping program is stunningly ambitious at in view or their goals while simultaneously disturbing in regards to its reach and impact. The Government's ambitions amount to a seed of dreams and direction that, given a few decades will grow into a sequoia of dominance and turmoil.

[479] 'It's Legal: Probe Into Facebook and Apple Spying Rejected by Ireland (2013)
[480] *Id.*
[481] *Id.*
[482] *Id.*
[483] *Id.*

In the desolate town of Bluffdale, Utah the NSA is creating a place to house a super computer of god-like processing power.[484] The base is decidedly fortified with outer defenses capable of stopping a 15,000 lb truck from ramming the wall by stopping it cold.[485] This base, known as the "Utah Data Center" (herein referred to as "The Center)" will be the vital heart of the NSA's countrywide infrastructure of mass espionage.[486] The Center is part of the Stellarwind program.[487] Its information centers are in the vicinity of the location fiber optic cables meet the continental US; this is done to enhance their ability to eavesdrop on communications coming from abroad.[488] "Inside sources show that Stellarwind's surveillance programs recorded 320 million calls a day."[489] Coding for Stellarwind's purposes was completed by a business known as Narus, now owned by Boeing; they created the algorithm to allow the computer applications to screen all email and phone communications for key phrases and if found they would download the communication to a server.[490]

Before, the NSA was said to only collect data "closest" to the suspect (text made and phone calls to associates, etc) and the shadowing fades the farther one is from the suspect.[491] "Now it is suspected that they eavesdrop on everything."[492] The NSA has the means to siphon

[484] Bamford, James. (2013). The NSA is Building the Country's Biggest Spy Center (Watch What You Say)
[485] *Id.*
[486] *Id.*
[487] *Id.*
[488] *Id.*
[489] *Id.*
[490] *Id.*
[491] *Id.*
[492] *Id.*

information from phone calls in real time.[493] Their supercomputers will have the capability to break all level of encryption within a few years.[494]

Internet of Things

More and more household appliances are now capable of being connected to the internet.[495] Then CIA Director David Petraeus called this phenomenon "transformational" at a summit hosted by the CIA venture capital firm In-Q-Tel.[496] The same 'apps' that you would use on your smart phone to adjust the temperature can easily turn into a tool for surveillance for the CIA.[497]

In earlier times spies would have to physically place espionage tools on the device's control or premises it is now much easier for them to use the household apps across your home to do their bidding.[498] "Items of interest will be located, identified, monitored, and remotely controlled through technologies such as radio-frequency identification, sensor networks, tiny embedded servers, and energy harvesters — all connected to the next-generation internet using abundant, low-cost, and high-power computing."[499] Petraeus has considered making an online identity for his spies so that it may be changed and erased at will.[500] "Proud parents document the arrival and growth of their future CIA officer in all forms of social media that the world can access for decades to come[…] [m]oreover, we have to figure out how to create the digital

[493] *Id.*
[494] *Id.*
[495] Ackerman, Spencer. (2013). CIA Chief: We'll Spy on You Through Your Dishwasher
[496] *Id.*
[497] *Id.*
[498] *Id.*
[499] *Id.*
[500] *Id.*

footprint for new identities for some officers."[501] It has never been easier to recreate the life that a person never had.

[501] *Id.*

RESOLUTION

The issue addressed is whether there are enough safeguards to protect the public's privacy and intimate information when the public is using technology such as cell phones and computers from corporate or government entities. The answer to the forgoing issue is not a question of more or less safeguards but how to create and implement better and timeless safeguards to address this dilemma as well as the quality of their enforcement and implementation.

Laboratories of Democracy

There are some signs that this country is already heading that way. In 2012, Maryland joined North Carolina to become one of the first few states to ban employers access to their subordinates' Facebook profiles[502]; this was in response to corrections officer Robert Collins outreach to the ACLU after he was appalled that he was required to give his Facebook login email and password to the Maryland Division of Corrections during a recertification interview so they could screen him for possible gang affiliations.[503] At the federal level, there has been some recent legislation on the issue; Congressmen Ed Perlutter of Colorado and Peter Welch of Vermont sponsored the Password Protection Act of 2013 in May, which is intended to prevent employers from gaining access to online passwords of their subordinate employees.[504]

[502] Referring to Maryland State Government Code § 10-624 (4)
[503] Fottrell, Quentin. (2013). Who's a Bigger Snoop: the NSA or Your Boss?
[504] *Id.*

Supremes of New Jersey

Unfortunately, in New Jersey, the government's powers to track suspect's cell phones without a warrant have grown.[505] LEOs will not need a warrant to track someone by cell phone.[506] The Court cited in the facts of the case that the Respondent's girlfriend allowed local LEOs to search a storage facility in her name; there, they found a cornucopia of stolen good to which they seized.[507] In order to find the Respondent, the LEOs in the case contacted his cell phone provider, T-Mobile to inquire about locating him using his phone; T-Mobile agreed.[508] The Respondent contested the use of his cell phone locational data as the catalyst to his arrest.[509] The Court rejected this argument holding that the Respondent had no expectation of privacy while he was on the public streets during the commission of his crimes.[510]

The New Jersey Supreme Court ruling only serves as a proverbial bump in the road on the journey splendid privacy safeguards. In contrast, the Federal Government has shown an interest in moving to end the surveillance-industrial complex through codified statute.

Bill against Big Brother

In Washington, two representatives of the 111th Congress have conceived a bill that has been hailed as a major step in the right direction.[511] Co-sponsors Senator Ron Wyden and Representative Jason Chaffetz sit on opposite sides of the aisle but have managed to create a bill

[505] *State v. Earls* 22 A.3d 114 (N.J. 2011)
[506] *Id*. at 117
[507] *Id.*
[508] *Id.*
[509] *Id.* at 119
[510] *Id*. at 122
[511] Ackerman, Spencer. (2013). Bill Would Keep Big Brother's Mitts Off Your GPS Data

with a simple purpose: no warrant, no geolocation information.[512] "GPS devices are everywhere and that's a good thing[…] [w]e just don't want nefarious characters tracking people without someone knowing, nor do I want law enforcement to be able to just follow everyone all the time."[513]

If passed the bill will protect the public from GPS tracking via their cell phones, or other device; the proposed law will also contain a provision protecting the public from tracking via a "successor devise" one which has not been invented yet.[514] The bill is widely regarded to be all encompassing and very thorough by its supporters.[515] Some of the critics are afraid that the bill fails to address undisclosed surveillance tactics that have yet to see the light of day.[516]

Amending § 215

Currently, Congress is considering a different but equally important bill. The Amash-Conyers Amendment has been introduced with the purpose of amending section 215 of the PATRIOT Act which gives FISC the power to deliver warrants for phone, medical, financial or business records.[517] Under current law, as long as the government can prove that the information is "relevant" then that is all they need in order to legally obtain the records and information.[518] A major challenge is to demand Congress' representatives to pass the Amash-Conyers Amendment since the likelihood of it passing is slim to none.[519]

---

[512] *Id.*
[513] *Id.*
[514] *Id.*
[515] *Id.*
[516] *Id.*
[517] Kravats, David. (2013). House to Vote on Repealing NSA Dragnet Phone Surveillance
[518] *Id.*
[519] *Id.*

FISC ruled that its 2008 court order for tech firm Yahoo!'s data on its customers should be revealed to the world.[520] This may help it prove to the world that they fought the NSA instead of allowing them to dictate their actions; let alone shown the world that it is possible to fight the Government when the Government chose to stomp on others' constitutional rights.[521] "Yahoo! takes users' privacy very seriously[;] [w]e do not provide the government with direct access to our servers, systems, or network," a Yahoo! Representative said regarding the NSA surveillance disclosure.[522] The firm formally asked FISC to release the 2008 case to the public; this is all to help keep people in the know about the scandal and the gravity of the situation.[523] Aside from requesting two weeks to look into the case before it was released, the US government has not made any comments about the release.[524] "It remains to be seen how forthcoming (the government) will be[;] [t]he administration has said they want a debate about the propriety of the surveillance, but they haven't really provided information to inform that debate. So declassifying these opinions is a very important place to start."[525]

Substantial Revamping

However, other laws are in need of a substantial revamping. LEOs are more than ever interested in this information; so they can use it to establish a suspect's precise location and to track their movements.[526] The main concern is that cell phone companies have possession of the

[520] Yahoo Wins Lawsuit to Declassify Docs Proving Resistance to PRISM
[521] *Id.*
[522] *Id.*
[523] *Id.*
[524] *Id.*
[525] *Id.*
[526] Koppel, Adam. (2010). Warranting a Warrant: Fourth Amendment Concerns Raised by Law Enforcement's Warrantless Use of GPS. University of Miami Law Review. At 1068

cell towers, and these companies have control of the pertinent information.[527] This brand of electronic surveillance is normally governed by the ECPA.[528] Generally, they must be granted a court order obliging the cellular service provider to give law enforcement access to this data.[529] "The current debate is centered on the legal standard required for obtaining these orders."[530] There are courts that specify that law enforcement solely has the burden of proving "specific and articulable facts," for these orders to be granted; other times they can prove less to obtain them.[531] Other courts necessitate the government to endow them with a showing of probable cause in order to be granted the order.[532] The debate over the proper procedure for granting these orders has not been resolved.

Now and again, a law enforcement agency may ask the cellular service provider for the suspect's stored records of their previous locations in order to get an idea of where they were and what they were doing previously.[533] This information, dubbed "historical data" has a low profile form even [to] the most hard-lined privacy rights' advocates.[534] It follows, that a law enforcement agency may request for a "prospective order" in aims to obtain the right to collect data of the suspect's future locations via their cellular phone provider due to the fact that this information does not exist yet.[535] This greatly impacts the populace's expectation of a nation free from government intrusion.

---

[527] *Id.*
[528] *Id.*
[529] *Id.*
[530] *Id.*
[531] *Id.*
[532] *Id.*
[533] *Id.*et al
[534] *Id.*at 1068-69
[535] *Id.* at 1069

Global Policy Implications of Government Surveillance

European firms are already retreating from their business contracts with American internet service providers.[536] Cloud service providers will suffer immensely if their customers cannot trust that their secret information will not fall into government hands.[537] This issue has affected the free trade discussions between the US and the EU as they see this incident as a market issue just as much as a civil liberties issue.[538] "'It is often American providers that will miss out, because they are often the leaders in cloud services[;] [i]f European cloud customers cannot trust the United States government, then maybe they won't trust US cloud providers either."[539]

If this proves to be true, this could be a multi-billion euro disaster for the American internet service providers; the EU suggest that these companies should quit cooperating with the government and concentrate on regaining their patrons' trust.[540] Many EU member states came together in a conference on how to engage the US over this issue.[541] However, they seem to wish to separate the two subjects into respective summits.[542] "Concerns about cloud security can easily push European policy-makers into putting security guarantees ahead of open markets, with

[536] Traynor, Ian. (2013). European Firms 'Could Quit US Internet by SORM The Russian Government has just Authorized Itself to Spy on Everything its Citizens do on the Net – and to Punish ISPs that Won't Help
[537] *Id.*
[538] *Id.*
[539] *Id.*
[540] *Id.*
[541] *Id.*
[542] *Id.*

consequences for American companies."[543] American internet companies have potential for expansion in the EU; but promise for profit runs hollow in an environment of deceit.[544]

The World has Taken Note

The EU has taken steps to prevent the emerging police state that is America from happening there.[545] Calling it a "wake-up call," the EU's Minister of Justice referred to the US shadowing program as the EU's leaders Germany and France promise to sketch up new laws to protect EU citizens' privacy rights from the state.[546] "Justice Commissioner Viviane Reding says that Europe needs to 'act swiftly' in response to PRISM […] and adopt measures to protect data and tough sanctions for violators."[547] The Justice Ministers of Germany and France executed a joint pronouncement in which they approved to establish "adequate safeguards" for the citizens of the EU so their data can only be used in a way that balances their self-determination and the need for safety measures.[548] The US should follow their example as soon as possible.

Katz Test and Relevant Case Law

Next, the realm of fundamental precedent regarding the United States' right to privacy is entered. From the time of the ruling of *Katz v. United States*[549], the reasonable expectation of privacy from intrusion by the state has been the norm as the Fourth Amendment of the Constitution applies to people, not places; at the time this was allowed in reluctance of the new

[543] *Id.*
[544] *Id.*
[545] Press, The Associated. (2013). EU Justice Chief: US Surveillance a 'Wake-Up Call'
[546] *Id.*
[547] *Id.*
[548] *Id.*
[549] *Katz v. United States* 389 U.S. 347 (1967)

found effects of the emerging technology at the time.[550] The issues in *Katz* were "whether a public telephone booth is a constitutionally protected area so the evidence obtained by attaching an electronic listening device to the top of such a booth is obtained in violation of the right to privacy of the user of the booth" and "whether physical penetration of a constitutionally protected area is necessary before a search and seizure can be said to be violative of the Fourth Amendment to the United States Constitution."[551] The United States Supreme Court created a two-tier method to determine if a person has a reasonable expectation of privacy; "[f]irst, that a person have exhibited an actual (subjective) expectation of privacy, and, second, that the expectation be one that society is prepared to recognize as 'reasonable[,]'."[552] This is the standard method of how intrusive a search can be.[553]

> "We can further learn how the Court treats emerging technologies by examining the line of post-Katz surveillance cases. These cases dealt with the warrantless use of new forms of surveillance in which the Court's focus was the specific type of technology used and the level of information it revealed. In United States v. Caceres, the Court faced the issue of whether the Fourth Amendment prohibited use of a recording device during conversations with the defendant. The Court held that it did not and declined to define the use of the device as search. The Court reasoned that the information received from the recording device was merely equivalent to an agent taking written notes; so no invasion of the defendant's expectation of privacy had occurred."[554]

A major area of contention to our issue is how the current issue ties to the *Katz* test. The court in *Katz* mentions that "the Fourth Amendment protects people, not places" in regards to the major issue of whether the phone booth the surveillance occurred was a constitutionally

[550] Koppel, Adam. Warranting a Warrant: Fourth Amendment Concerns Raised by Law Enforcement's Warrantless Use of GPS. University of Miami Law Review. At 1070
[551] *Katz*, 389 U.S. at 349
[552] *Id.* at 361 (Harlan, J. Concurring)
[553] *Id.* at 349
[554] *Id.*

protected area.[555] The government could argue in the current state of affairs, as in *Katz* that a hypothetical suspect lost their Fourth Amendment rights because they air their content of social media usage and IMSI location publically, as anyone with a IMSI detector or with a social media account can detect their activity; the former has been approved in *Katz* while the latter is yet to be determined.[556]

Even a simple act such as dialing a phone number to call is not protected by the Fourth Amendment.[557] In *Smith v. Maryland*,[558] the Supreme Court refused to acknowledge that a search had occurred when authorities obtained a number dialed on a phone through the use of a pen register.[559] The Supreme Court reasoned that since the person freely passes the number to the phone company as they dial in and therefore assumes the risk that the information could be caught by the police.[560] They also justified this ruling by citing that the pen register only records the number dialed and nothing else.[561] This surely is an on point case relevant to the current dilemma before us.

In *Smith*, the petitioner, Michael Lee Smith was believed to be allegedly making threatening and obscene phone calls to Patricia McDonough, who was robbed a few days earlier.[562] After locating his address and phone number using his car's license plate, the police requested Patricia's telephone company mounted a pen register at its central office to record the phone numbers from the petitioner's home to see if he was the one making threatening calls to

[555] *Id*. at 351 (footnote 9)
[556] *Id*.
[557] Koppel. at 1071
[558] *Smith v. Maryland*, 442 U.S. 735 (1979)
[559] Koppel. at 1071
[560] *Id.* at 1071
[561] *Id.* at 1071
[562] *Smith*, 442 U.S. at 737

Patricia.[563] The pen register revealed that it was indeed the petitioner making these calls so the LEOs in the case subsequently obtained a warrant to search the petitioner's home and arrest the petitioner.[564] In this case, the court found that the petitioner had no subjective expectation of privacy that the phone numbers he dialed were private.[565] The Court reasoned that most telephone subscribers do not believe that their phone numbers will be secret under the facts of the case.[566] Furthermore, their phone numbers must have been conveyed to the phone company in order for their phones to work, thereby losing any hope that the petitioner in *Smith* would be able to meet the second prong of the *Katz* test.[567]

Again, in a hypothetical case, the Government could contend that tracking a suspect via his IMSI would not require a warrant because IMSIs, like phone numbers, hold no subjective or societal expectation of privacy. They would contend that society does not believe their location, like their phone number in *Smith*, will be a secret given that they would know and even desire their phone's IMSI to constantly give their phone's (and incidentally, their own) location on a consistent basis so they can be in constant reach with friends and family. The Court in *Smith* has stated "repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."[568] The Government must be wary of the other

[563] *Id*.
[564] *Id*.
[565] *Id*. at 743
[566] *Id*.
[567] *Id*.
[568] *Id*. at 744

important distinction between pen registers and IMSIs; pen registers do not acquire communication information but, IMSIs do obtain communication information.[569]

United States v. Knotts is a similar on point case but for starkly different reasons.[570] In *Knotts*, the Respondent and his two codefendants were convicted of manufacturing methamphetamines.[571] The government placed a locational "beeper" into a drum of chloroform given to the codefendant Armstrong to be taken to Darryl Petschen's (the other codefendant) house where they proceeded to create the narcotics.[572] After arriving to Petschen's house, Armstrong moved the drum of chloroform to Petschen's vehicle where the LEOs pursued from then on using visual surveillance, keeping the beeper as a backup in case they lost sight of Armstrong.[573] "During the latter part of this journey, Petschen began making evasive maneuvers, and the pursuing agents ended their visual surveillance[;] [a]t about the same time officers lost the signal from the beeper, but with the assistance of a monitoring device located in a helicopter the approximate location of the signal was picked up again about one hour later."[574]

The LEOs in the *Knotts* case relied on their visual observations of the Respondent's cabin as well as the beeper's data and their pursuit of Armstrong to obtain a warrant to search the cabin.[575] The LEOs found a full drug laboratory at the Respondent's cabin and subsequently arrested him and the codefendants.[576] The Supreme Court in *Knotts* reasoned that, "A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in

[569] *Id*. at 741
[570] *United States v. Knotts*, 460 U.S. 276 (1983)
[571] *Id*.
[572] Id. at 278
[573] *Id*.
[574] *Id*.
[575] *Id*.
[576] *Id*.

his movements from one place to another[;] [w]hen Petschen traveled over the public streets he voluntarily conveyed to anyone who wanted to look the fact that he was traveling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property."[577] The *Knotts* Court stated that the codefendants had a reasonable expectation of privacy in the cabin but they did not have it while travelling on the roads to get there.[578] The *Knotts* Court goes further to state that they "would never equate police efficiency with unconstitutionality" in that sensory augmenting technology is not per se an unreasonable search.[579] Future, appellate litigants could use this as a premise in favor of the government for a future IMSI or any case against the mass data gathering program as IMSI can be used to track a target if they left the home by the reasoning in *Knotts*.[580]

However, this is in stark contrast with the Supreme Court's ruling in *United States v. Karo* in which a similar case was decided differently hinging on one important material fact.[581] In *Karo*, the Court was asked to weigh in on two questions left unanswered by *Knotts*: "whether installation of a beeper in a container of chemicals with the consent of the original owner constitutes a search or seizure within the meaning of the Fourth Amendment when the container is delivered to a buyer having no knowledge of the presence of the beeper, and (2) whether monitoring of a beeper falls within the ambit of the Fourth Amendment when it reveals information that could not have been obtained through visual surveillance."[582] In *Karo*, the LEOs used a beeper to shadow a drum of ether as it was stored in a warehouse and the codefendants'

[577] *Id*. at 281-282
[578] *Id*. at 282
[579] *Id*. at 284
[580] *Id*.
[581] *United States v. Karo*, 468 U.S. 705 (1984)
[582] *Id*. at 707

houses for a period of a few days.[583] The case hinged on one question and answer: "This case thus presents the question whether the monitoring of a beeper in a private residence, a location not open to visual surveillance, violates the Fourth Amendment rights of those who have a justifiable interest in the privacy of the residence. Contrary to the submission of the United States, we think that it does."[584] This will undoubtedly be mandatory authority in a hypothetical court case involving someone followed via electronic eavesdropping by the Government with a private residence as the *Katz* test will undoubtedly apply in these situations.

Presently, the United States Supreme Court has not ruled on whether the use of cellular phone GPS tracking by law enforcement would require a warrant or if the information obtained by these new technologies falls under the reasonable expectation of privacy.[585] However, in *United States v. Jones*, the Supreme Court ruled "that the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a 'search."[586] In *Jones*, the FBI along with local police mounted a GPS tracking device on the respondent's car and shadowed his location for a period of 28 days.[587] The GPS tracker was accurate to within 50 feet; the government would be hard pressed to argue that IMSI tracking would be materially, if not factually different from this case.[588] In the not too distant future, the Supreme Court will likely settle this issue and provide a fundamental framework to balance the legitimate law enforcement interests with our constitutional safeguards against being

[583] *Id*. at 708
[584] *Id*. at 714
[585] Koppel. at 1072
[586] *United States v. Jones*, 132 S. Ct. 945, 948 (2012)
[587] *Id*. at 947
[588] *Id*.

usurped by technological advancements.[589] Lower courts have been split on the application of the reasonable expectation of privacy test to these new technologies; further challenges are to be expected on how current laws apply.[590] This becomes particular vital as the technology becomes cheaper and broadly used by smaller police departments and the public as well.[591]

"Governmental use of GPS devices as a means of obtaining vehicle location information constitutes a search under the Fourth Amendment because [of] the intrusive nature of the technology and the detail of information transmitted invade upon individuals' reasonable expectations of privacy[;] [t]herefore, law-enforcement agents should be required to provide a warrant based on probable cause before using this technology."[592] In fact, it is argued that their use constitutes an extrasensory surveillance method which under current common law would require a warrant for use since it operates to replace, not enhance human perception.[593] The use of this form of GPS by civilians is growing astronomically and this combined with the belief that government can track them without their knowledge or consent could lead to mass abnormal behavior.[594]

Acquisition of cellular phone site location by law enforcement officials constitutes a search under the Fourth Amendment for the fact that it is violative of the suspect's reasonable expectation of privacy.[595] There should be a warrant requirement for accessing the information as well so no loop holes will exist to circumvent our rights.[596] People carry their cell phones

[589] Koppel. at 1073-74
[590] *Id.* at 1073
[591] *Id.* at 1073
[592] *Id.* at 1083
[593] *Id.* at 1085
[594] *Id.* at 1086
[595] *Id.* at 1086
[596] *Id.* at 1086

wherever they go; to the mall, to the grocery store, to a friend's house and to their homes too. As law enforcement officials use applications like IMSI to obtain a person's location in real time, a person may be tracked in many of the aforementioned places; the Supreme Court has consistently ruled that a person has a reasonable expectation of privacy in their own home.[597] Law enforcement breaks the law when they use this technology to track a person in their home without a warrant; this typically happens because one may go indoors and outdoors at will, doing errands, picking up the mail and washing the car, all the while being tracked without a person's knowledge or consent.[598] The frequency in which people travel in and out of these protected privacy areas (such as their homes, homes of friends, etc) demands for the possession of a warrant before the use of tracking technology so our Fourth Amendment rights will not be mitigated due to some logistical technicality.[599]

Concluding Remarks

In short, most (if not all) people do not expect their movements to be tracked by either the Government or any business.[600] They expect to use their cell phones to make phone calls, send text messages to friends, tweet what's currently on their mind on Twitter or share a photo on Instagram. They do not expect that their lives will be secretly watched and profiled by any law enforcement agency, the NSA or any corporation.[601] Any citizen that has knowledge of this would be outraged that their personal life has been made a spectacle due to some mistake or

[597] *Id.* at 1086
[598] *Id.* at 1086
[599] *Id.* at 1086-87
[600] *Id.* at 1087
[601] *Id.* at 1087

because their cellular IMSI was used in order to find another person.[602] The use of this technology can say a lot about a person's life, all of which is clearly within their reasonable expectation of privacy.[603] Cell phones are carried in purses and holsters that rarely show their content to the outside world.[604] Again, they scream for Fourth Amendment protection as they illustrate the user's expectation of privacy.[605]

The task to strike the needed balance between civil liberty protection and protection from crime is a hard one to forge. Cellular phones' IMSI have the potential for great capabilities for LEOs and their crime fighting goals.[606] However, the technology demands greater fortifications from corporate and government surveillance and intrusion.[607] "Moreover, cell phone tracking implicates the most fundamental Fourth Amendment privacy concern, the right to privacy in the home[;] [r]equiring a warrant based on probable cause would save citizens from a world of embarrassment, fear, and privacy invasion."[608]

Currently, Corporate America and the government are in denial of the reality that the use of this technology justifies the issuance of a warrant.[609] Conflicting state common law will warrant a Supreme Court ruling to clear once and for all whether a warrant for the use of this technology is needed for government use and if it is illegal for private use.[610] Time will show that the need to protect our civil liberties shall prevail.[611]

---

[602] Alder, et al
[603] Koppel 1088
[604] *Id.* at 1088
[605] *Id.* at 1088
[606] *Id.* at 1089
[607] *Id.* at 1089
[608] *Id.* at 1089
[609] *Id.* at 1089
[610] *Id.* at 1089
[611] *Id.* at 1089

WORKS CITED

'It's legal': Probe into Facebook and Apple spying rejected by Ireland. 26 July 2013. RT. web. 29 July 2013. <http://rt.com/news/ireland-apple-facebook-nsa-investigation-628/>.

Ackerman, Spencer. *Bill Would Keep Big Brother's Mitts Off Your GPS Data*. 26 May 2011. Condé Nast. web. 23 July 2013. <bill-would-keep-big-brothers-mitts-off-your-gps-data>.

—. *CIA Chief: We'll Spy on You Through Your Dishwasher*. 15 March 2012. Condé Nast. web. 23 July 2013. <http://www.wired.com/dangerroom/2012/03/petraeus-tv-remote/>.

Adler, Andrew. "The Notice Problem, Unlawful Electronic Surveillance, and Civil Liability Under the Foreign Intelligence." *University of Miami Law Review* (2007): 393-440. web. 11 June 2013.

Al-Haramain Islamic Foundation v. Obama. No. 11-15468. United States Circuit Court for the Ninth Circuit. 7 august 2012. web. 20 July 2013.

Arends, Brett. *10 signs your co-worker is a spy Commentary: Why colleagues might be making it harder to do your job*. 19 July 2013. The Wall Street Journal. web. 19 July 2013. <http://www.marketwatch.com/story/is-your-co-worker-a-spy-2013-07-19?pagenumber=2>.

Baetz, Juergen. "Germany's Merkel urges patience on NSA answers." *AP Top News Package* 2013. web. 19 July 2013.

Bailey, Ronald. "Your Cellphone Is Spying on You." *Reason* January 2013: 34-39. web. 29 May 2013.

Bamford, James. *Connecting the Dots on PRISM, Phone Surveillance, and the NSA's Massive Spy Center*. 12 June 2013. web. 14 June 2013. <http://www.wired.com/threatlevel/2013/06/nsa-prism-verizon-surveillance/>.

—. *The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)*. 15 March 2013. Wired. web. 16 June 2013. <http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all/>.

Bartash, Jeffrey. *Democrats, Republicans switch views on NSA surveillance*. 11 June 2013. The Wall Street Journal. web. 16 June 2013. <http://blogs.marketwatch.com/election/2013/06/11/democrats-republicans-switch-views-on-nsa-surveillance/>.

Bump, Philp. *NSA's Massive Email Collection Started with Cheney and Ended With Obama*. 27 June 2013. The Atlantic Monthly Group. web. 1 August 2013. <http://www.theatlanticwire.com/national/2013/06/nsa-emails-stellarwind/66658/>.

—. *Update: Now We Know Why Googling 'Pressure Cookers' Gets a Visit from Cops*. 1 August 2013. The Atlantic Monthly Group. web. 1 August 2013. <http://m.theatlanticwire.com/national/2013/08/government-knocking-doors-because-google-searches/67864/#.UfqCSAXy7zQ.facebook>.

Cavanaugh, Tim. *What do They know about you? An interview with NSA analyst William Binney*. 10 June 2013. The Daily Caller. web. 16 June 2013. <http://dailycaller.com/2013/06/10/what-do-they-know-about-you-an-interview-with-nsa-analyst-william-binney/?print=1>.

Chow, Raymond. "Why-Spy? An Analysis of Privacy and Geolocation in the Wake of the 2010 Google "Wi-Spy" Controversy." *Rutgers Computer and Technological Law Journal* 39 (2013): 57-93. web. 24 July 2013.

Chrisafis, Angelique. *France 'runs vast electronic spying operation using NSA-style methods' Intelligence agency has spied on French public's phone calls, emails and internet activity, says Le Monde newspaper*. 4 July 2013. Guardian News and Media Limited. web. 4 August 2013. <http://www.theguardian.com/world/2013/jul/04/france-electronic-spying-operation-nsa>.

Clifford, Stephanie. *Attention, Shoppers: Store Is Tracking Your Cell*. 14 July 2013. The New York Times Company. web. 23 July 2013. <http://www.nytimes.com/2013/07/15/business/attention-shopper-stores-are-tracking-your-cell.html?pagewanted=1&_r=0>.

Donohue, Laura. "NSA snooping is legal. It isn't constitutional." *The Washington Post* 23 June 2013. web. 20 July 2013.

Dreyfuss, Ben. *What is the NSA's PRISM program? (FAQ)*. 7 June 2013. web. 18 July 2013. <http://news.cnet.com/8301-1009_3-5788253-83/what-is-the-nsas-prism-program-faq>.

EU's response to NSA? Drones, spy satellites could fly over Europe. 29 July 2013. RT. web. 29 July 2013. <http://rt.com/news/eu-drones-proposal-nsa-678/>.

Flaherty, Anne. "Google Asks FISA Court To Lift Gag Order." *AP Top News Package* 2013. web. 18 June 2013.

Fottrell, Quentin. *Who's a bigger snoop: the NSA or your Boss?* 10 June 2013. The Wall Street Journal. web. 10 June 2013. <http://www.marketwatch.com/story/whos-a-bigger-snoop-the-nsa-or-your-boss-2013-06-10>.

Gallagher, Dan. *NSA snooping reportedly includes Google, Facebook, Apple, others*. 2013 June 6. The Wall Street Journal. web. 7 June 2013. <http://blogs.marketwatch.com/thetell/2013/06/06/nsa-snooping-reportedly-includes-google-facebook-apple-others/>.

"GCHQ to File Report over US Prism Spy Programme Links." *International Business Times* 8 June 2013. 23 June 2013.

Gellman, Barton. *U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program*. 6 June 2013. web. 8 June 2013. <http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html>.

Gidari, P Coie A. "Designing the Right Wiretap Solution: Setting Standards under CALEA, IEEE Security & Privacy." *IEEE Security & Privacy* 4 (2006): 29-36. web.

<http://ejournals.ebsco.com.ezproxy.net.ucf.edu/direct.asp?ArticleID=49D4A206BFACC3D11ADC>.

Greenwald, Glenn. *NSA collecting phone records of millions of Verizon customers daily*. 5 June 2013. web. 7 June 2013. <http://www.guardian.co.uk/world/2013/jun/06/nsa-phone-records-verizon-court-order>.

Harris, Andrew. *Spy Agency Sought U.S. Call Records Before 9/11, Lawyers Say*. 30 June 2006. Bloomberg L.P. web. 3 August 2013. <http://www.bloomberg.com/apps/news?pid=newsarchive&sid=abIV0cO64zJE>.

Johnston, Ian. *EU funding 'Orwellian' artificial intelligence plan to monitor public for "abnormal behaviour" The European Union is spending millions of pounds developing "Orwellian" technologies designed to scour the internet and CCTV images for "abnormal behaviour"*. 9 September 2009. Telegraph Media Group Limited. web. 4 August 2013. <http://www.telegraph.co.uk/news/uknews/6210255/EU-funding-Orwellian-artificial-intelligence-plan-to-monitor-public-for-abnormal-behaviour.html>.

Koppel, Adam. "Warranting a Warrant: Fourth Amendment Concerns Raised by Law Enforcement's Warrantless Use of GPS." *University of Miami Law Review* (2010): 1088-1061. web. 8 June 2013. <http://www.lexisnexis.comezproxy.net.ucf/hottopics/lnacademics/?shr=t&sfi=AC00NBGenSrch&csi=7371>.

Kravets, David. *Cops Can Track Cellphones Without Warrants, Appeals Court Rules*. 30 July 2013. Condé Nast. web. 30 July 2013. <http://www.wired.com/threatlevel/2013/07/warrantless-cell-tracking/>.

—. "Declassified Memos Confirm Dragnet Phone Surveillance Program Was No Secret From Congress." 31 July 2013. *Wired.com.* Condé Nast. web. 2 August 2013. <http://www.wired.com/threatlevel/2013/07/phone-dragnet-no-secret/>.

—. *House to Vote on Repealing NSA Dragnet Phone Surveillance*. 23 July 2013. Condé Nast. web. 23 July 2013. <http://www.wired.com/threatlevel/2013/07/nsa-phone-surveillance-vote/>.

LaFraniere, Sharon. *Russian Spies, They've Got Mail Regulations Allow Security Services to Tap Into Systems of Internet Providers*. 7 March 2002. The Washington Post. web. 3 August 2013. <http://www.washingtonpost.com/wp-dyn/articles/A51550-2002Mar6.html>.

Lawner, Kevin J. "Post-Sept. 11th international surveillance activity—a failure of intelligence: the Echelon interception system & the fundamental right to privacy in Europe." *Pace International Law Review* 14.2 (2002): 435-480. web. 7 August 2013. <http://web.ebscohost.com.ezproxy.net.ucf.edu/ehost/detail?sid=170d584a-5e37-41eb-957e-5011e32f3a02%40sessionmgr113&vid=1&hid=117&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=lft&AN=502444530>.

MacAskill, Ewen. *New NSA leaks show how US is bugging its European allies Exclusive: Edward Snowden papers reveal 38 targets including EU, France and Italy*. 30 June 2013. Guardian News and Media Limited. web. 4 August 2013. <http://www.theguardian.com/world/2013/jun/30/nsa-leaks-us-bugging-european-allies?INTCMP=SRCH&guni=Article:in%20body%20link>.

Markoff, John. *Taking Spying to Higher Level, Agencies Look for More Ways to Mine Data*. 25 February 2006. The New York Times Company. web. 3 August 2013. <http://www.nytimes.com/2006/02/25/technology/25data.html?ei=5088&en=d231d2f98b31262a&ex=1298523600&pagewanted=print&_r=0>.

McCullagh, Declan. *Feds tell Web firms to turn over user account passwords Secret demands mark escalation in Internet surveillance by the federal government through gaining access to user passwords, which are typically stored in encrypted form.* 25 July 2013. CBS Interactive Inc. web. 26 July 2013. <http://news.cnet.com/8301-13578_3-57595529-38/feds-tell-web-firms-to-turn-over-user-account-passwords/>.

—. *NSA spying flap extends to contents of U.S. phone calls*. 15 June 2013. CBS Interactive Inc. web. 16 June 2013. <<http://news.cnet.com/8301-13578_3-57589495-38/nsa-spying-flap-extends-to-contents-of-u.s-phone-calls/>.

Miller, Daniel. *Revealed: Hundreds of words to avoid using online if you don't want the government spying on you (and they include 'pork', 'cloud' and 'Mexico')*. 26 May 2012. web. 18 July 2013. <http://www.dailymail.co.uk/news/article-2150281/REVEALED-Hundreds-words-avoid-using-online-dont-want-government-spying-you.html>.

Perez, Evan. *Tech firms push back over NSA secrecy*. 12 June 2013. The Wall Street Journal. web. 16 June 2013. <http://www.marketwatch.com/story/tech-firms-push-back-over-nsa-secrecy-2013-06-12>.

Pimmentel, Benjamin. *Why Google, Facebook must nip spy tag Analyst warns of fears of a 'U.S. version of the Chinese Internet'*. 12 June 2013. The Wall Street Journal . web. 12 June 2013. <http://www.marketwatch.com/story/why-google-facebook-must-nip-spy-tag-2013-06-12>.

Plourde-Cole, Haley. "Back to Katz: Reasonable Expectation Of Privacy In The Facebook Age." *Fordham Urban Law Journal* (2010): 571-628. web. 14 June 2013.

Police to track Moscow metro passengers' SIM cards. 29 July 2013. web. 30 July 2013. <http://rt.com/news/moscow-metro-sim-surveillance-759/>.

Poulsen, Kevin. *Feds Are Suspects in New Malware That Attacks Tor Anonymity*. 5 August 2013. Condé Nast. web. 5 August 2013. <http://www.wired.com/threatlevel/2013/08/freedom-hosting/>.

Press, Associated. *Thousands take to streets in Germany to protest US surveillance of Internet*. n.d. The Washington Post. web. 29 July 2013. <http://www.washingtonpost.com/world/europe/thousands-take-to-streets-in-germany-to-protest-us-surveillance-of-internet/2013/07/27/dbe3333e-f6c6-11e2-81fa-8e83b3864c36_story.html#>.

Press, The Associated. "EU justice chief: US surveillance a 'wake-up call'." *AP English Worldstream - English* 2013. web. 19 July 2013. <http://ezproxy.net.ucf.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=nsm&AN=AP3618791e4f29426293a7125ab4dce3a4&site=ehost-live>.

Satter, Raphael. "Leaked docs give new insight into NSA's searches." 31 July 2013. *News (AP, UPI, etc.).* AP Top News Package. web. 1 August 2013. <A href="http://ezproxy.net.ucf.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=nsm&AN=AP68b0aebc582542e6b03a28b6665fd893&site=ehost-live">Leaked docs give new insight into NSA's searches</A>.

Shakir, Faiz. *NSA Whistleblower To Expose More Unlawful Activity: 'People…Are Going To Be Shocked'*. 12 May 2006. Center for American Progress Action Fund. web. 3 August 2013. <http://thinkprogress.org/security/2006/05/12/5319/more-unlawful-activity/>.

Soltani, Ashkan. *How Protecting Your Privacy Could Make You the Bad Guy*. 23 July 2013. Condé Nast. web. 23 July 2013. <http://www.wired.com/opinion/2013/07/the-catch-22-of-internet-commerce-and-privacy-could-mean-youre-the-bad-guy/>.

Tassell, Rebecca Van. "Walking A Thin Blue Line: Balancing The Citizen's Right To Record Police Officers Against Officer Privacy." *Brigham Young University Law Review* 2013.1 (2013): 183-212. web. 1 June 2013.

team, Guardian US interactive. *A Guardian Guide to your Metadata*. 12 June 2013. Guardian News and Media Limited. web. 4 August 2013.

<http://www.theguardian.com/technology/interactive/2013/jun/12/what-is-metadata-nsa-surveillance#meta=0001100>.

Tracy, Jen. *New KGB Takes Internet by SORM The Russian government has just authorized itself to spy on everything its citizens do on the Net -- and to punish ISPs that won't help. So much for post-Soviet civil rights.* 4 February 2000. Mother Jones and the Foundation for National Progress. web. 3 August 2013. <http://www.motherjones.com/politics/2000/02/new-kgb-takes-internet-sorm>.

Traynor, Ian. *European firms 'could quit US internet providers over NSA scandal' European commission vice-president says American cloud services providers could suffer loss of business*. 4 July 2013. Guardian News and Media Limited. web. 4 August 2013. <http://www.theguardian.com/world/2013/jul/04/european-us-internet-providers-nsa>.

Yahoo wins lawsuit to declassify docs proving resistance to PRISM. 16 July 2013. web. 29 July 2013. <http://rt.com/news/yahoo-data-collection-court-case-165/>.

Yost, Pete. "Hostile Hill territory on NSA surveillance issue." *AP Top News Package* 18 July 2013. web. 19 July 2013.