2017

Privacy v. Cybersecurity : How Much Power Should the Government Have?

Julina M. Schaeffer

Julina Schaeffer
Fall 2016

I. Introduction: History and Current Law

In April of 2000, Ted Leonsis, president of the Interactive Properties Group at AOL was quoted as saying "To date, digital entertainment has been a failure."[1] Cyberspace, the internet and social media have come a long way since then. With such tremendous growth in such a short period of time, the law has not been able to keep up with the times. Cybersecurity is a problem that no one law, country or agency has been able to fully address and it is unclear as to when or how cybersecurity will be comprehensively solved.

There are numerous laws and agencies that have attempted to battle the cybersecurity issue, but no single law that addresses cybersecurity in its entirety. The Federal Trade Commission Act prohibits, "unfair or deceptive acts or practices in affecting commerce,"[2] while the Department of Homeland Security has goals and strategies that primarily involve government infrastructure.[3] Generally speaking, there are no cybersecurity laws, just many that relate to the concept of cybersecurity or laws that seek to reprimand those with inadequate data security.

Interwoven into the concept of cybersecurity is the issue of privacy. This is why there are no laws to date that deal with cybersecurity directly. It seems that no one can agree on how far the law can go to ensure safety in cyberspace. Everyone wants to be protected, but at the same time, doing so would most likely infringe upon our privacy rights.

Recently, the country was divided when the government wanted Apple to unlock the phone of the San Bernardino shooters[4]. The government wanted to be able to obtain more information

1 "The Failure of New Media," The Economist, April 17, 2000, http://www.economist.com/node/318323 (last visited Dec. 1, 2016).
2 15 U.S.C. § 45(a)(1) (2012).
3 https://www.dhs.gov/cybersecurity-overview (last visited Dec. 1, 2016).
4 https://en.wikipedia.org/wiki/FBI-Apple_encryption_dispute (last visited Dec. 1, 2016).

on who the shooters contacted and determine if any information stored on the phone could prevent future attacks while Apple felt this was an invasion of privacy that would open the door to letting the government unlock a phone whenever and to whomever they pleased.[5] This problem was never resolved as the government was able to get outside help, most likely from hackers, to unlock the phone.[6] The government also never told Apple how they were able to unlock the phone.[7] In response, Apple released a security update to resolve an encryption problem.[8] Herein lies the problem, do we allow the government access to our personal, private online data in order to create a safer online community and essentially waive our right to privacy? Or do we continue to keep our right to privacy intact, but risk the safety of ourselves and our country? Is there any middle ground where we can keep the majority of our rights, but still ensure our cybersecurity? If we do allow our rights to be infringed upon, how far down the metadata path should we allow the government to go? This paper will seek to examine the patchwork of laws that are in place and seek to address the arguments for and against cybersecurity laws and policies. The only thing that is clear is that cybersecurity and privacy are directly related and both issues must be addressed when discussing cybersecurity.

1. What is cybersecurity?

"Cybersecurity: precautions taken to guard against crime that involves the internet, especially unauthorized access to computer systems and data connected to the internet."[9] There have been many attempts at defining exactly what cybersecurity is, however there has not been

5 *Id.*
6 *Id.*
7 *Id.*
8 *Id.*
9 https://www.dictionary.com/browse/cybersecurity?s=t

one precise definition to define the term. Typically, cybersecurity refers to the act of protecting information communications technology and their contents.[10]

"Cybersecurity involves the protection of both private and public networks."[11] Many laws are aimed at either the public or private sectors, but not both. Yet, cybersecurity affects both the public and private sectors at the same time. A cyber attack on the private-sector can and will affect the public-sector. Therefore, there should not be a distinction between the two when cybersecurity laws are proposed.

The Department of Homeland Security has attempted to address cybersecurity, but maintains that a number of factors prevent the securing of cyberspace.[12] Those factors include the difficulty of reducing vulnerabilities in complex networks, the ability of malicious actors to operate from anywhere in the world and the link between cyberspace and the physical world.[13] The Department of Homeland Security is aware of "high-consequence events" and the vulnerabilities that may be caused by cyber attacks and have continued their efforts in creating a safe cyber world.

In February of 2013, President Obama signed Executive Order 13636: Improving Critical Infrastructure Cybersecurity.[14] The Order established a policy of the United States government to increase the volume, timeliness and quality of cyber threat information shared with the private

[10] Eric A. Fisher, Cong. Research Serv., R43831, Cybersecurity Issues and Challenges: In Brief (2016).
[11] Cyberwars: Navigating Responsibilities for the Public and Private Sector: Positive Cybersecurity Law: Creating a Consistent and Incentive-Based System Symposium, 19 Chap. L. Rev. 401 (2016).
[12] https://www.dhs.gov/cybersecurity-overview (last visited Dec. 1, 2016).
[13] *Id*.
[14] https://www.federalregister.gov/documents/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity (last visited Dec. 1, 2016).

sector so as to allow those entities to better protect themselves against cyber threats.[15] The Order went on to assert that privacy and civil liberties protections were maintained while sharing critical information in order to protect critical infrastructure.[16] Further, the Order included a cybersecurity framework that would entail a set of standards that address cyber risks.[17] However, the Order left the details of the framework and policies regarding this cybersecurity plan up to the individual agencies, Secretary and Attorney General.[18] The Order, while great in theory, did little to establish much more than what should be included in policies regarding cybersecurity.[19] No where in the Order were there any specific plans for policies to safeguard infrastructure from cyber attacks.[20] The framework merely instituted a program that needed to be in place, a deadline of the details of the program and listed the individuals responsible for creating such a program.[21] No specifics were included. This was a great start, and acknowledgment that there is a cybersecurity problem that needs to be addressed according to privacy standards is the first step to solving the problem.

2. Where We Stand Today

The Department of Homeland Security, in conjunction with other agencies, instituted the National Cybersecurity Protection System ("NCPS").[22] Known as the "EINSTEIN" program, the system enables the Department of Homeland Security to defend the federal government's

15 *Id.*
16 *Id.*
17 *Id.*
18 *Id.*
19 *Id.*
20 *Id.*
21 *Id.*
22 https://www.dhs.gov/national-cybersecurity-protection-system-ncps (last visited Dec. 1, 2016).

technology infrastructure against cyber attacks.[23] The system primarily focuses on four areas including: detection, analytics, information sharing and prevention.[24] Detection creates alerts of malicious or harmful network activity.[25] Analytics provide analysts with the ability to compile and analyze information regarding cyber activity and enables analysts to inform those affected about cybersecurity threats and vulnerabilities.[26] Information sharing allows Homeland Security to quickly exchange cyber threat information among other agencies in order to prevent cybersecurity incidents from occurring.[27] Finally, prevention provides a defense and ability to limit malicious network traffic.[28] The main objective to prevention is to identify malicious network activity in order to enhance cybersecurity analysis, awareness and response.[29] The government is taking steps to secure cyber networks, however their main focus is securing the networks for the Federal government, essentially the dot.gov domains. From the government viewpoint, an attack on the federal government would cripple the entire country and affect both the public and private sectors, therefore that is where the main focus lies.

After the federal government, the focus on protection lies with the financial service industry, followed by the electric power industry and the defense industry.[30] Additionally, Homeland Security has partnered with antivirus companies to take proactive measures to stop threats before they are able to reach a large audience.[31] Further, the Department of Homeland

23 *Id.*
24 *Id.*
25 *Id.*
26 *Id.*
27 *Id.*
28 *Id.*
29 *Id.*
30 Securing Cyberspace: Our Shared Responsibility; DHS Speech, April 25, 2011 (LEXIS).
31 *Id.*

Security began development of the National Cyber Incident Response Plan (NCIRP).[32] This plan would coordinate the response of numerous agencies, governments and private firms in the event of a cyber attack, similar to response plans for kinetic attacks.[33]

Lastly, plans are being developed to secure the internet for consumers and industry users.[34] The U.S. government continues to research, test and evaluate protocols to integrate into the current systems to maintain a safe "pipeline for the future."[35] That is where we stand today, continuing research to ensure the safety of the internet. However, no one seems quite certain how to maintain that level of safety.

II. The Right to Privacy, The All Writs Act and the Freedom of Information Act

"The right to life has come to mean the right to enjoy life, - the right to be let alone."[36] In 1890, Samuel Warren and Louis Brandeis published a Harvard Law Review Article that has since become one of the most influential and highly regarded articles to advocate for the right to privacy.[37] Privacy generally means "making private information about an individual unavailable to parties who should not have that information."[38] "Privacy, therefore, involves individuals' ability to control their personal data."[39] Essentially, the right to privacy and cybersecurity entail the protection of users against unauthorized use of their data.

32 *Id*.
33 *Id*.
34 *Id*.
35 *Id*.
36 Warren, Samuel; Brandeis, Louis, *The Right to Privacy*, 4 Harv. L. Rev. 1, (1890).
37 *Id*.
38 David Clark, Thomas Benson and Herbert S. Lin, At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues, 9 (2014).
39 Cyberwars: Navigating Responsibilities for the Public and Private Sector: Positive Cybersecurity Law: Creating a Consistent and Incentive-Based System Symposium, 19 Chap. L. Rev. 401, 405 (2016).

The All Writs Act of 1789 allows the U.S. Federal Courts to "issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law."[40] Until Apple refused to help the FBI, the All Writs Act was not given much thought when it came to cybersecurity.[41] The All Writs Act has been understood to authorize a federal court to issue writs to non-parties directing them to provide "reasonable technical assistance" to the government in executing a search warrant.[42] The debate over this conferred power stems from the question of just how much power should judges be allowed in compelling a private person to help the government execute a search warrant.[43] In response to the dispute between Apple and the FBI, a judge in California ordered Apple to create new software, at the expense of Apple, to unlock the phone of the San Bernardino shooters.[44] Conversely, a judge in New York refused to compel Apple to help the government unlock the phone of a convicted drug trafficker.[45] [46] So, who is right?

The seminal case regarding the All Writs Act is *United States v. New York Tel. Co*.[47] In this case, the Supreme Court determined that the Court could order the telephone company to assist in the installation of pen registers under the All Writs Act.[48] The pen registers were to be used to aid Federal law enforcement officers in investigating illegal gambling that was being conducted

40 All Writs Act, 28 U.S.C.S. § 1651 (LEXIS 2016).
41 In re An Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, 2016 U.S. Dist. LEXIS 20543 (2016).
42 https://www.lawfareblog.com/coherent-middle-ground-apple-fbi-all-writs-act-dispute (last accessed on Dec. 1, 2016).
43 *Id*.
44 *Id*.
45 *Id*.
46 In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court, 149 F. Supp. 3d 341(2016).
47 *United States v. New York Tel. Co*., 434 U.S. 159 (1977).
48 *Id*. at 172.

through the use of the telephone.[49] The telephone company had declined to fully comply with the original court order, arguing that, *inter alia*, the All Writs Act did not provide a basis for such an order.[50] The Court stated that the power conferred under the Act extends, under appropriate circumstances, to persons who are in a "position to frustrate the implementation of a court order or the proper administration of justice," even though the party is not involved in the wrongdoing.[51] "Appropriate circumstances," are to be determined through the third-party's closeness to the case, the burden the requested assistance would impose upon the third-party and the necessity to the government of receiving the requested assistance.[52]

In the recent California case, a judge ordered Apple to assist in the search of a cell phone.[53] The Order stated that Apple was required to bypass or disable the auto-erase function, whether or not it had been enabled.[54] In order to accomplish this task, Apple would have been forced to create a Software Image File ("SIF") that would have allowed Apple to conduct a brut force attack on the cell phone.[55] The brut force attack would allow the FBI to submit passcodes until the correct one was found.[56] Typically, after three wrong passcodes a phone is locked.[57] This is the feature that the FBI wished to bypass using the new software.[58] The SIF would be uploaded to the phone through an upgrade to the phone.[59]

49 *Id*. at 161.
50 *Id*. at 162-63.
51 Id. at 174.
52 *Id*.
53 In re An Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, 2016 U.S. Dist. LEXIS 20543 (2016).
54 *Id*. at 2.
55 *Id*.
56 *Id*.
57 *Id*.
58 *Id*.
59 *Id*.

In the New York case, also filed in 2016, the DEA executed a search warrant and seized the phone of a suspect alleged to be involved in drug trafficking.[60] Nothing was done with the phone until approximately one year later, when the DEA sought a warrant to search the seized evidence, including the cell phone.[61] Similar to the California case, the agents here were unable to access the information stored on the phone as the phone was password protected.[62] After conferring with the FBI and still unable to unlock the phone, the DEA sought the help of Apple to bypass the security code.[63] With the help of Apple, the government petitioned the Court for permission to unlock the phone and relied exclusively on the All Writs Act.[64] The application was sealed as the judge feared that public dissemination of the facts could harm an ongoing criminal investigation.[65] The judge determined that the three factors laid out in *New York Tel. Co*., weigh against issuing the requested order.[66] Further, the All Writs Act required that the writ be "agreeable with the usages and principles of law."[67] The judge concluded that the extraordinary relief that was requested did not comport with this requirement of the statutory language of the All Writs Act.[68]

Some have argued that neither the New York or California Court applied the All Writs Act correctly.[69] In the California case, the Court required Apple to create new software to unlock the

60 In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court, 149 F. Supp. 3d 341, 344 (LEXIS 2016).
61 *Id*. at 345.
62 *Id*. at 346.
63 *Id*.
64 *Id*.
65 *Id*. at 347.
66 *Id*. at 351.
67 *Id*.
68 *Id*.
69 https://www.lawfareblog.com/coherent-middle-ground-apple-fbi-all-writs-act-dispute (last visited on Dec. 1, 2016).

phone, while in the New York case, the software to unlock the phone was already in place and extensive resources of the third party (Apple) would not be needed to comply with the order.[70] In relation to privacy and cybersecurity, many who agreed with Apple believed that this would open the door to allowing the government to use the All Writs Act to infringe on their privacy rights and obtain metadata on anyone whenever the court deemed it necessary. On the other hand, those who agreed that Apple should be forced to unlock the phones felt that the safety of our country was more important than the infringement upon our right to privacy.

Applying the three factors from *New York Tel. Co*., it would appear that the two cases should have been decided the other way around. Applying those factors first to the California case, Apple was not close to the case, the burden on apple to perform the request was extremely high and the necessity of the aid to the government was not as strong as the government wanted the Court to believe. Other than selling iPhones, Apple had nothing to do with the criminal activity of the San Bernardino shooters. Further, the government wanted Apple to create new software to upload to the phone to bypass the security feature on the phone. Apple contended that this software did not exist and the time, expense and burden on the company was extensive. Finally, the need for Apple to aid the government was not as dire as the government argued. The shooters were dead and there was no telling whether or not there would even be any information on the phone to aid in any future terrorist attacks. While many people do keep lots of information on their phones, it doesn't seem likely that future terrorist plans would be saved on a cellular phone. As it turned out, the government was able to unlock the phone, but to this day, they refuse to reveal how that was accomplished. It may be inferred that the Court decided this Order based on feelings rather than the law. No person wants to see harm come to their country, but I am not

70 *Id.*

convinced that forcing Apple to open the door to future privacy infringements would prevent such harm from occurring in the future. As for the New York case, Apple was a little closer to that investigation. Apple helped the government draft the application to the court and even conceded that they would help the government as long as there were a court order in place. The burden on Apple here was low. No new software needed to be created in order to facilitate the request. Finally, without the help from Apple, the government would not have been able to progress any further in retrieving the information from the phone. The DEA enlisted the help of the FBI to unlock the phone, but the FBI was unable to aid in that request. Without the help of Apple, the information pertaining to the investigation would not be recovered. It would appear that the *New York Telephone Co*., factors were met and therefore the Order should have been granted. The New York judge concluded his decision by saying that he would not offer an opinion on whether government interests, such as national security, should always prevail against societal interests. He stated that should be left up to the legislature, especially with the quickly growing technological advances that were not available just a few years ago.

III. Case Law and Gaps in the Legal Framework

The government contends that they have numerous plans, strategies, methodologies and procedures in place to keep critical infrastructure safe from cyber threats and attacks. Yet, there are no laws in place today that comports with that statement. Further, the plans and procedures that are in place primarily protect governmental bodies and agencies from attacks, but do not extend those same strategies to the general public. Consumer protections are in place that discipline those companies that do not have high enough standards to protect consumers from

data breaches. That is about the extent of the safety that is afforded to U.S. civilians. Hence the reason President Obama said that we "currently exist in a state of a cyber-security emergency."[71]

The Freedom of Information Act ("FOIA") allows the public the right to request access to records from any federal agency.[72] The Act was created to keep the public informed about their government.[73] However, FOIA does have many exceptions when information does not need to be disclosed when requested.[74] Included in those exceptions are interests such as national safety and personal privacy.[75]

Cybersecurity primarily concerns technologies, processes and policies that help to prevent or reduce the negative impact of hostile actors on information technology systems.[76] Cybersecurity can both protect and violate privacy.[77] Data security measures provide privacy rights to users in cyberspace and protect those users from having unauthorized users access their information.[78] Other cybersecurity measures used to share information with agencies or even measures taken to block certain internet traffic from reaching its destination may violate privacy rights.[79] This is why there is such tension and confusion when it comes to cybersecurity and privacy. While the two are quite different from each other, they tend to intersect, which makes it difficult for lawmakers to address this issue.

a. Riley v. California

71 Presidential Policy Directive 20 (PPD 20); Press Release, The White House Office of the Press Secretary, 2012 Presidential Policy Directive (on file with author). https://fas.org/irp/offdocs/ppd/ppd-20.pdf

72 https:www.foia.gov (last visited Nov. 6, 2016).

73 *Id*.

74 *Id*.

75 *Id*.

76 David Clark, Thomas Benson and Herbert S. Lin, At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues, 9 (2014).

77 *Id*. at 100.

78 *Id*.

79 *Id*.

The issue in Riley v. California addressed the question of whether police may, without a warrant, search digital information on a cell phone seized from the arrestee.[80] In Riley, suspect was arrested for possession of concealed and loaded firearms after he was pulled over for driving with expired tags.[81] Pursuant to policy, the car was impounded and searched.[82] The fruits of the search turned up a cell phone.[83] The cell phone contained pictures linking Riley to a gang and evidence that Riley was involved in a shooting a few weeks earlier.[84] Riley was charged with that shooting.[85] Riley moved to suppress the photographic evidence, alleging that the search violated his Fourth Amendment rights.[86] The Supreme Court agreed and granted the motion for suppression.[87]

Based on the outcome of this case, it can be inferred that privacy comes at a cost. While we are afforded the right to privacy, we may not pick and choose when that privacy right should be relevant and when it should be ignored. Cyberspace, metadata and digital devices are included in the right to privacy and without laws stating otherwise, incriminating evidence on our personal electronics may not be searched in violation of those rights. Additionally, technological advances have gone far beyond what most could have ever predicted. The Court noted that cell phones can hold an exorbitant amount of information ranging from pictures, addresses and bank statements to receipts and phone call records.[88] Physically, no one would carry around all of that

80 *Riley v. California*, 134 S. Ct. 2473 (2014).
81 *Id*. at 2477.
82 *Id*.
83 *Id*.
84 *Id*.
85 *Id*.
86 *Id*.
87 *Id*.
88 *Id*. at 2478.

information, however that information can all be stored on a smart phone further aiding in the argument that cell phones should not be searched under the Fourth Amendment.[89] While the outcome here is not what many would want, the legislature needs to find a way to address the fact that technology has outgrown the law.

The lower courts focused on preventing the destruction of evidence.[90] The Courts claimed that cell phones are subject to data encryption and remote wiping and therefore the risk of losing evidence is great. However, this argument was not convincing as there are other ways to prevent the loss of data from a cell phone and there is not evidence that these types are issues are even a current problem.[91] As to remote wiping, that can be prevented by disconnecting a phone from the network by turning the phone off or removing the battery.[92] As for encryption problems, officers can place the phone in foil lined bags to isolate the phone from radio waves.[93] If there are still concerns, the Court suggested application of the exigent circumstances exception to search the phone immediately. [94]

b. FTC v. Wyndham Worldwide

Wyndham Worldwide, a hospitality company that manages and franchises hotels and timeshares, was alleged to have engaged in unfair cybersecurity practices that exposed their customers' personal data to unauthorized access and theft.[95] The Federal Trade Commission ("FTC") alleged that Wyndham stored credit card numbers in clear, readable text; Wyndham used easily guessed passwords to access its system; Wyndham failed to use security measures to

89 *Id*. at 2479.
90 *Id*. at 2485.
91 *Id*. at 2486.
92 *Id*. at 2487.
93 *Id*.
94 *Id*.
95 *FTC v. Wyndham Worldwide, Inc*., 799 F.3d 236, 240 (3d. Cir. 2016).

limit access to its system; Wyndham did not ensure that the hotels implemented adequate security measures; and failed to adequately restrict third party networks to its system.[96] Because of the inadequate security measures in place, Wyndham's network was subjected to three separate cybersecurity attacks.[97] The FTC alleged that these attacks resulted in $10.6 million dollars in fraud loss.[98]

The Court relied on the Federal Trade Commission Act of 1914, which prohibited unfair methods of competition in commerce.[99] Under the Act,

> the Commission shall have no authority to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.[100] In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence.[101]

Wyndham unsuccessfully argued that the alleged conduct fell outside the scope of the meaning of "unfair."[102] Wyndham next argued that Congress excluded the FTC's unfairness authority by enacting measures such as the Gramm-Leach-Bliley Act[103] and the Children's Online Privacy Protection Act[104].[105] The Court was not persuaded by this argument either. After several other unsuccessful arguments regarding Wyndham's conduct, the Court established that Wyndham's

96 *Id*. at 240.
97 *Id*. at 241.
98 *Id*. at 240.
99 15 U.S.C.S. § 45
100 15 U.S.C.S. § 45(n)
101 *Id*.
102 *Wyndham* at 244.
103 The Gramm-Leach-Bliley Act required the FTC to establish standards for financial institutions to protect consumers' personal information.
104 The Children's Online Privacy Protection Act required the FTC to enact regulations requiring children's websites to disclose their information gathering techniques.
105 *Wyndham* at 247.

conduct was indeed, unfair and the FTC had authority to regulate data security under the unfairness prong of § 45.[106] Essentially, the Wyndham Court felt that because Wyndham had voluntarily promoted themselves as ensuring the safety of consumer's data information, they had availed themselves to the Act. Wyndham had published a privacy policy on its website that essentially was a lie. The policy, created by Wyndham, stated that they had security measures in place that would protect personally identifiable information, including the use of a 128 bit encryption system. FTC argued that Wyndham used no such program and therefore acted deceptively.[107] The Court found Wyndham's lack of security to be egregious.[108] It is important to note that while there are no general federal laws which require a website to implement a privacy policy, one that is adopted voluntarily is subject to unfair trade practices if it is not adhered to as stated.

The Court went on to decide whether Wyndham had fair notice that its conduct could fall within the meaning of the Act.[109] The Court stated that Wyndham was not entitled to know with certainty what cybersecurity practices are required by the Act.[110] Wyndham was only entitled to notice of the meaning of the statute and not the FTC's interpretation.[111] As to fair notice, regarding the meaning of the statute, the Court decided Wyndham was given fair notice and affirmed the decision of the lower courts, which ruled in favor of the FTC.[112]

c. EPIC v. NSA

106 *Id.*
107 *Id.* at 248.
108 *Id.*
109 *Id.* at 249.
110 *Id.*
111 *Id.* at 250.
112 *Id.* at 254.

In *EPIC v. NSA*, the plaintiff sued the National Security Agency ("NSA") alleging it had violated its duty under the Freedom of Information Act ("FOIA").[113] Plaintiff had requested information from the NSA seeking the disclosure of communications between the NSA and a private company regarding encryption and cybersecurity.[114] The request arose after a cyber attack on Google that primarily targeted the Gmail accounts of Chinese human rights activists.[115]The NSA responded with a Glomar[116] response, which Plaintiff challenged.[117] The NSA claimed one of the FOIA exceptions, specifically, exemption 3.[118] Exemption 3 provides that records exempted from disclosure by statute are shielded from disclosure, if the statute either requires that the matter be withheld from the public in such a manner so as to leave no discretion on the issue or establishes criteria for particular matters to be withheld.[119] The burden was on the NSA to prove that the withheld information relates to the organization or function of the NSA.

The Court determined that if the NSA were to answer the FOIA request, it might be forced to reveal whether or not the attack on Google was investigated and whether that attack was considered to be a potential attack to U.S. Government systems.[120] The Court concluded that this evaluation would fall within the broad scope of the National Security Agency Act and its Information Assurance mission.[121] Therefore, the FOIA request was exempted.[122]

d. EPIC v. DHS

113 *Epic v. NSA*, 678 F.3d 926 (D.C. Cir. 2012).
114 *Id*.
115 *Id*. at 929.
116 A Glomar response is the term for the phrase, "I can neither confirm nor deny."
117 *Id*. at 930.
118 *Id*. at 931.
119 *Id*.
120 *Id*. at 934-35.
121 *Id*. at 935.
122 *Id*.

In *EPIC v. DHS*, Plaintiff, Electronic Privacy Information Center ("EPIC"), brought action against the United States Department of Homeland Security ("DHS") under the Freedom of Information Act ("FOIA").[123] EPIC requested information regarding the Defense Industrial Base Cyber Pilot ("DIB Cyber Pilot") program.[124] The program aimed to protect U.S. critical infrastructure by providing classified threat information to companies that were voluntary participants or their Commercial service providers.[125] EPIC sought the records to determine if the program followed Federal wiretap laws.[126]

DHS responsive search resulted in over 16,000 pages of potential documents.[127] After careful review of each page, 1276 pages were released to EPIC.[128] 117 pages were released in their entirety, while the remaining 1159 pages were partially redacted.[129] EPIC believed some documents were inadvertently excluded.[130] DHS responded and released four additional documents that had mistakenly been marked non-responsive and excluded under FOIA exemptions.[131]

EPIC brought this action alleging DHS' search for the documents was inadequately conducted and contends that DHS improperly redacted or withheld documents.[132] The Court used a standard of reasonableness to determine that DHS' search for the documents was

123 *Elec. Privacy Info. Ctr. v. United States Dep't of Homeland Sec*., 117 F.Supp. 3d 46 (D.C. Cir. 2015).
124 *Id*. at 52.
125 *Id*.
126 *Id*.
127 *Id*. at 55.
128 *Id*.
129 *Id*.
130 *Id*.
131 *Id*. at 56.
132 *Id*.

meticulous, organized and thorough.[133] The Court then went through each of the five exemptions that DHS used for the withheld and redacted documents.[134] After careful analysis, the Court determined that DHS properly excluded documents under FOIA exemptions 1, 3, 4 and 5.[135] However, the Court concluded that the DHS did not meet its burden in proving that documents withheld under FOIA exemption 7 was proper.[136] Therefore, the Court granted the government's motion for summary judgment for documents exempted under exemptions 1, 3, 4 and 5, but it denied without prejudice summary judgment for the documents exempted under exemption 7.[137]

e. Putting it all together

After review of the cases, it is apparent that there are still many issues when dealing with cybersecurity and privacy. However, some issues have been settled or can be inferred from the language of the decisions.

Riley established that privacy rights are extended to our cell phones, however the question remains on whether cell phones can be searched only after arrest or seizure or whether police will require a warrant that explicitly particularizes a cell phone search.[138] Based on the language in the decision, it can be inferred from *Riley* that a warrant should be obtained prior to searching a cell phone. The Court did not appear concerned with loss of evidence from a cell phone. The Court extensively discussed why loss of evidence was not something to be concerned of regarding cell phones, thus absent exigent circumstances, officers should not search a cell phone without first obtaining a search warrant.

133 *Id*. at 58.
134 Id. at 59.
135 *Id*. at 59-65.
136 *Id*. at 67.
137 *Id*.
138 *Riley v. California*, 134 S. Ct. 1870 (2014).

Wyndham infers that companies have a duty to protect its consumers from fraudulent conduct in cyberspace.[139] While the threshold standard as to the level of security does not appear to be very high, voluntary protections that are implemented, or advertised as being implemented, are required to actually be in place. There are still questions on what is needed to establish adequate data security, as there is no bright line rule or law that specifically requires any company to have a privacy policy in place. Additionally, the actual authority of the FTC, under the Act, is to ensure fair business practices, which does not necessarily imply that they have the authority to regulate cybersecurity. On the other hand, the FTC believes their authority includes regulating matters in cyberspace. In the future, the role of the FTC should be clarified, or at least modified, to include what matters in cyberspace they have the authority to regulate. If they are not given the authority over regulating cyberspace, it is not clear who else would be better suited to govern these types of matters.

In today's age where you can do practically anything and everything online, most consumers assume that their information is protected. This is another example of how the law has not been able to keep up with technology. While most companies provide security for their online users, there is nothing that requires them to do so. Nonetheless, if a breach occurs, as we have seen in the past with companies like Target and Home Depot, it can cost those companies millions of dollars to settle class action lawsuits.

The *EPIC* cases were both examples of FOIA requests and how exemptions do or do not apply when agencies receive requests for documents.[140] However, these cases clearly

139 *Wyndham Worldwide*, 799 F.3d 236 (2016).

140 *Epic v. NSA*, 678 F.3d 926 (D.C. Cir. 2012); *Elec. Privacy Info. Ctr. v. United States Dep't of Homeland Sec*., 117 F.Supp. 3d 46 (D.C. Cir. 2015)

demonstrate that exemptions are a case-by-case basis and therefore, once again, no bright line rule applies.

While these cases do not all relate to the same issues, indirectly they all relate to privacy and cyberspace. After reading these cases, it is clear that privacy and cyberspace have a vast variety of issues and that is why no one law is able to govern these topics. What is clear, is that while no one law currently governs privacy and cyberspace, there does need to be some laws enacted that are able to address both issues.

IV. Issues with enacting laws regulating cyberspace

a. Government/Public Sector

The government has attempted to implement laws, plans and procedures to regulate cyberspace. The main focus on cyberspace is to prevent cyber threats and ensure the safety of the country. While the government has implemented some laws and regulations in regards to cyberspace, the laws do not address many issues in cyberspace. Cybersecurity policies largely deal with protecting information. This is why there are so many concerns regarding privacy rights when it comes to dealing with cybersecurity.

A number of proposals regulating cyberspace wish to implement measures to block internet traffic containing malware before it gets to its specified destination.[141] However, the problem with that is then all in bound internet traffic would need to be inspected.[142] Some

[141] National Research Council, Division on Engineering and Physical Sciences, and Computer Science and Telecommunications Board. At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues. Washington, US: National Academies Press, 2014. ProQuest ebrary. Web. 30 November 2016.

[142] *Id*. at 100.

believe this would infringe upon our privacy rights entirely too much as the inspection of traffic by anyone other than the intended recipient would go too far into the invasion of our liberty.[143]

Other proposals regarding increasing cybersecurity capabilities include sharing information with the government in order to identify and respond to cyber threats and intrusions.[144] The type of information that would be shared would include information that is associated directly with malware intrusions, such as email servers with personal identifiers.[145] While this would allow government entities to further protect the country from cyber threats and attacks, the concern is that some organizations would then risk exposing themselves to regulatory attention and possible loss of advantages with their competitors.[146] *Wyndham* exposed themselves to regulatory attention because they posted a privacy policy regarding an encryption system which they didn't appear to actually be using.[147] Most in bound traffic is not malicious or hostile and to cast such a wide net as to include all in bound network traffic would essentially deteriorate any hope of retaining a right to privacy in cyberspace.[148] In order to not infringe on privacy interests entirely, personally identifiable markers would have to be removed prior to sending the information and the information would have to only include what is necessary to enhance cybersecurity measures.[149] Of course, how to remove the identifiers will create problems because at some point, someone in cyberspace will be able to see those identifiers prior to them being removed. Moreover, what is deemed "necessary to enhance cybersecurity measures" is

143 *Id.*
144 *Id.*
145 *Id.* at 101.
146 *Id.*
147 See *FTC v. Wyndham Worldwide*, 799 F.3d 236 (2015).
148 At the Nexus of Cybersecurity and Public Policy at 101.
149 *Id.*

subjective and therefore what one may deem necessary, another may not. It will be difficult to distinguish where that line will begin and end.

The NSA has been collecting telephony metadata for years, however they do not (allegedly) obtain telephone content, only the time, date, place of the call and the numbers called and received. In 1979, the Supreme Court held that pen registers did not violate privacy interests as only the numbers dialed were recorded, not the content.[150] I think that the courts will rely on this case regarding how much information can be obtained before a privacy intrusion occurs on the internet. While we have come a long way from using pen registers, the idea is similar in that cybersecurity entails what websites are visited and who emails are being sent to or received from. The content is not always important, (obviously sometimes it is), but as a start, the who, what, and when will be less intrusive than the content.

b. Private Sector

To further complicate matters, today unauthorized users can post pictures and videos on social media, such as Facebook or YouTube, without permission of the person depicted in the picture or video. If there were laws enacted to regulate cyberspace, they would have to address video privacy in today's age of social media. "Today's online-video technologies create new threats to privacy."[151] Copyright laws address protect people from others using their work, however these laws do little to protect privacy rights.[152] The Digital Millennium Copyright Act ("DMCA") incorporated notice and takedown, where the copyright holder can have unauthorized use of their work immediately taken down.[153] There are arguments that have been raised

150 See *Smith v. Maryland*, 99 S. Ct. 2577 (1979).
151 "We, the Paparazzi": Developing a Privacy Paradigm for Digital Video, 95 Iowa L. Rev., 919, 927 (2010).
152 *Id.* at 929.
153 *Id.*

regarding improper use of the DMCA because the Act does not actually require that the work be registered copyrighted work. Websites receive thousands of takedown requests daily and do not have the time to research each one. Rather than deal with the hassle, most will just take down the alleged copyrighted work. For example, Google regularly receives notices to take down links to works that may infringe copyright. Since February of 2011, to date, Google has taken down 1.97 billion URLs, resulting in 948,000 affected websites.[154]

While there is no similar law enacted for privacy concerns, a notice and takedown regulation aimed at privacy would help to alleviate those who have been subjected to such conduct. With things like bullying and revenge porn on the rise, privacy concerns on social media have greatly increased. The problem with enacting such a law would raise concerns regarding first amendment freedom of speech rights. Similar to *Riley*[155], the right to freedom of speech and privacy comes with a cost. Do we continue to allow people to post whatever they wish online and social media at the cost to others' privacy? Further, enacting a takedown of this magnitude would essentially allow anyone to request takedown of any content they didn't agree with or that they deemed to be offensive. There needs to be a balance. There needs to be regulations on what we can post about others, and still maintain our freedoms. It is one thing to post about what one's own thoughts and beliefs and an entirely different issue when it comes to posting about someone else. At the very least, we each have the "right to be let alone[156]," and that includes postings on social media. If a privacy takedown were enacted, it would need to be specific as to what could be requested to be taken down. It would need to be offensive to a reasonable and prudent person,

[154] Google Transparency Report, Requests to Remove Content Due to Copyright, https://www.google.com/transparencyreport/removals/copyright/#glance (last visited Dec. 1, 2016).

[155] See *Riley v. California*, 134 S. Ct. 1870 (2014).

[156] Warren, Samuel; Brandeis, Louis, *The Right to Privacy*, 4 Harv. L. Rev. 1, (1890).

and it would need to be aimed at a particular individual. Generalizations, while they may be offensive, would not be enough to outweigh the impact on civil liberties.

V. Proposed Action

a. Presidential Policy Directive on United States Cyber Incident Coordination

The first policy directive to address cybersecurity was Presidential Policy Directive ("PPD") 20.[157] PPD 20 affirmed a procedure for "cyber collection operations that are reasonably likely to result in 'significant consequences.'"[158]

In July 2016, President Obama approved a Presidential Policy Directive[159] ('PPD") 41, which established clear principles that will govern the Federal government's activities in cyber incident response.[160] The PPD was focused on "significant cyber incidents."[161] Significant cyber incidents are those that will likely result in "demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people."[162]

PPD 41 outlined five principles intended to guide the government during any cyber incident.[163] The first being a shared responsibility principle in which both the public and private sectors would work together to protect the country from "malicious cyber activity and managing cyber incidents and their consequences."[164] The PPD then addressed a "risk based

157 https://fas.org/irp/offdocs/ppd/ppd-20.pdf (last visited on Dec. 1, 2016).
158 *Id.*
159 Presidential Policy Directive – 41- https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident (last visited on Dec. 2, 2016).
160 https://www.whitehouse.gov/the-press-office/2016/07/26/fact-sheet-presidential-policy-directive-united-states-cyber-incident-1 (last visited on Dec. 2, 2016).
161 *Id.*
162 *Id.*
163 *Id.*
164 *Id.*

response" in which the government would balance the need for response during a cyber incident against the harm to the country, people and civil liberties.[165] Affected entities must be ensured their rights to privacy as well as other civil liberties and therefore the federal government must safeguard the details of any cyber incident.[166] The federal agency first affected by a cyber incident must immediately notify other federal agencies in order to facilitate a unified response to the incident.[167] Finally, the PPD asserted that the response to a cyber incident must balance the need for national security against the need to quickly restore and recover operations.[168]

The principles outlined in PPD 41 were aimed at significant cyber incidents. Incidents are given a severity number, zero through five, and anything incident at a three or above is considered significant.[169] Additionally, the PPD assigned each government agency to be lead agencies in dealing with specified categories of cyber incidents.[170] If any of these presidential policy directives are to be replaced with new directives will be up to the next president. President-elect Trump, once in office, will hold the power to replace any previous presidential policy directives, if he so chooses.

b. White House Cybersecurity National Action Plan (CNAP)

165 *Id.*
166 *Id.*
167 *Id.*
168 *Id.*
169 *Id.*
170 *Id.*

In early 2016, President Obama proposed the Cybersecurity National Action Plan.[171] The plan proposes a long term strategy to enhance cybersecurity awareness and protections as well as maintain public safety and national security.[172]

CNAP established the "Commission on Enhancing National Cybersecurity [173] The Commission, comprised of non-government top business and strategic thinking men and women, will make recommendations to strengthen cybersecurity in both public and private sectors.[174] CNAP additionally proposed a $3.1 billion Information Technology Modernization Fund to help manage government information technology as well as manage how the government manages cybersecurity.[175] Further, CNAP seeks to secure the online accounts for all users in the country by adding an additional layer of security beyond password protection.[176] To accomplish this mission, the Commission will look to align with companies such as Google, Microsoft, Paypal, Venmo, and MasterCard, among others, to increase security for online account users, make financial transactions more secure and take steps to safeguard personal data in online transactions between citizens and the government.[177] In addition, the government will seek to establish new ways of identification for online users, other than a social security number.[178] The government is well aware that identity fraud has quickly become the fasted growing crime the country faces today and that is one of the reasons the government is looking to combat the consequences of cyber attacks both in the government information technology world as well as

171 https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan (last visited Nov. 15, 2016).
172 *Id.*
173 *Id.*
174 *Id.*
175 *Id.*
176 *Id.*
177 *Id.*
178 *Id.*

in the private sector.[179] The main goal of CNAP is to raise the level of cybersecurity for the entire country.[180]

While $3.1 billion may seem like an exorbitant amount of money to spend on this proposed plan, it is important to note that in 2015 Federal agencies spent over $80 billion on information technology ("IT"), with a significant portion on cybersecurity.[181] The Department of Defense accounts for almost 25% of that amount, while most other agencies spend about 7%.[182] Therefore, it is not an impossibility that CNAP will be approved. The government spends billions on cybersecurity and that amount is likely to increase in the future. The 2017 budget request for IT investment is $81.6 billion, with $19 billion of that for cybersecurity.[183]

c. Department of Homeland Security

The Department of Homeland Security ("DHS") takes a collective approach to combating cyber crimes and vulnerabilities.[184] DHS maintains that by working together with other agencies and private sector organizations, they are better able to understand and protect critical infrastructure.

In a letter from Lisa Sotto, Chair of DHS' Data Privacy and Integrity Advisory Committee to Jeh Johnson, Secretary of the U.S. Department of Homeland Security, dated February 17, 2016, Ms. Sotto submitted recommendations in addressing privacy protections and cybersecurity in regards to behavioral or algorithmic analytics.[185] Algorithmic analytics establishes baselines for

179 *Id.*
180 *Id.*
181 Eric A. Fisher, Cong. Research Serv., R43831, Cybersecurity Issues and Challenges: In Brief (2016).
182 *Id.*
183 *Id.*
184 https://www.dhs.gov/topic/protecting-critical-infrastructure (last visited Dec. 1, 2016).
185 Letter from Lisa J. Sotto, Chair DHS Data Privacy and Integrity Advisory Committee, to Jeh Johnson Secretary of the United States Department of Homeland Security and Karen

network traffic and uses algorithms to spot potential cybersecurity threats.[186] Currently, DHS has implemented a pilot program called, "Logical Response Aperture," to assess the effectiveness of algorithmic analytics.[187]

The letter stated privacy issues that may exist in implementing algorithmic analytics include the mishandling of information connected to individuals, correlation of data with privacy interests, and improper alignment with notice, access, use and sharing information.[188] Further, there are different categories of information that call for different levels of response in protecting privacy interests.[189] At a minimum, all traffic flow into and out of the system would generally flow unimpeded and require only the basic levels of privacy protections.[190] However, information that appeared to contain malware or some other type of cyber threat would need to be looked into with more detail and special care would have to be taken to protect privacy interests.[191] Additionally, sample data used for training purposes would need to ensure that any classified information remain protected.[192] If privacy concerns do arise, existing protections for Federal systems and data would apply including proper training safeguards and privacy notices.[193] Because analysts will be looking for anomalies in the traffic patterns, there is concern that sensitive information could be revealed and privacy interests infringed upon. However, the report on algorithmic analytics stated that:

Neuman Chief Privacy Officer of the United States Department of Homeland Security (February 17, 2016) https://www.dhs.gov/sites/default/files/publications/dpiac-report-2016-01-algorithmic-analytics_0.pdf (last visited on Dec. 2, 2016).

186 *Id*. at 4.
187 *Id*. at 6.
188 *Id*. at 8.
189 *Id*.
190 *Id*.
191 *Id*.
192 *Id*.
193 *Id*.

Analysts will not be reading emails unless those messages appear to be directly related to malicious behavior, such as phishing messages. Analysts will not be issuing queries for individual records, using personally identifiable information in queries, or retrieving personally identifiable or sensitive information unless there is a priori reason to believe that the data being requested is part of malicious behavior.[194]

While this program is aimed at the Federal government there are several private sector companies who have implemented similar programs to help protect their companies from cyber threats.[195] It is recommended that the government "develop benchmarks for success relative to private sector efforts."[196]

VI. Conclusion

Our technology today has far surpassed the laws that are currently in place. In order to keep up with today's technology, new laws must be enacted to combat issues in cyberspace. Cyberspace must be regulated so as to keep our nation and people safe from harm. However, those laws must comport with the rights and freedoms that in which our country was founded. Specifically, our privacy rights must remain, however, there may need to be limitations placed on our freedom in order to balance the safety of all. This is no easy task, as giving up part of our freedoms will not be something most will agree with, however our privacy rights already come at a cost. We allow those that commit crimes to keep evidence of their crimes suppressed if it were to violate their privacy rights. At some point, cyberspace must be regulated, and it may entail limitations on our freedom. But the question remains, do we limit our freedom to access cyberspace or do we limit our right to privacy? There is no immediate answer. We must simply wait and see what laws and regulations will be enacted in the future. One can only hope that cyber warfare does not occur before we are able to fully regulate cyberspace.

194 *Id*. at 27.
195 *Id*. at 7.
196 *Id*.

Julina Schaeffer
Fall 2016