2016

Finding The Perfect Balance: Combating Cyber Attacks Without Intruding on Civil Liberties

Andrew Richman

Andrew Richman
Finding The Perfect Balance: Combating Cyber Attacks Without Intruding on Civil Liberties

Part I: Introduction

The time has passed where the only threat to the United States and its people are that of physical combat. A new war is being waged all around us today, the Cyber War. Over the last decade, an influx of cyber hacking attacks has hit US government agencies, businesses and individuals.[1] These attacks are threatening the way both the government and businesses use the Internet and store their private information.[2] Cyber attacks have resulted in many companies and individuals throughout the United States calling for new security protocols, and legislative intervention to help combat this issue.[3] With lawmakers' adamant to help secure both government and business' digital security, doing so may come at a privacy cost for individuals who use the Internet everyday.[4]

After more than five years of attempting to provide government regulations to combat cyber security concerns, Congress has made its final push.[5] While companion bills were introduced and passed in 2015 respectively in both the House of Representatives and the Senate, legislatures have been obstinate to secure a system in which a new government intermediary will help field threats from private entities, and facilitate warnings to other potential victims.[6] This

---

[1] Ian Bremmer, *These 5 Facts Explain The Threat of Cyber Warfare*, TIME MAGAZINE, June 19, 2015, *available at* http://time.com/3928086/these-5-facts-explain-the-threat-of-cyber-warfare/
[2] Jennifer Steinhauer, *House Passes Cybersecurity Bill After Companies Fall Victim to Data Breaches*, NEW YORK TIMES, April 22, 2015, http://www.nytimes.com/2015/04/23/us/politics/computer-attacks-spur-congress-to-act-on-cybersecurity-bill-years-in-making.html?_r=0.
[3] Patricia Zengerle, *House Passes Cyber-Threat Information Bill*, Reuters, April 22, 2015, http://www.reuters.com/article/2015/04/22/us-usa-cybersecurity-congress-idUSKBN0ND2IN20150422.
[4] Andy Greenberg, *House Passes Cybersecurity Bill Despite Privacy Protests*, WIRED MAGAZINE, http://www.wired.com/2015/04/house-passes-cybersecurity-bill-despite-privacy-protests/
[5] Chris Velazco, *Budget Bill Heads to President Obama's Desk With CISA Intact*, ENGADGET, http://www.engadget.com/2015/12/18/house-senate-pass-budget-with-cisa/
[6] Gregory T. Nojeim, Senior Counsel and Director of the Freedom, Security and Technology Project, Hearing Before the Senate Homeland Security and Government Affairs Committee on Protecting America From Cyber

information-sharing platform is believed to open up means of communication between private entities and the government, helping each combat such attacks, as well as provide government agencies with information necessary to help catch and persecute such attackers.[7]

Legislators finally achieved this goal in December 2015.[8] The Cybersecurity Act of 2015 (CSA) was inserted "into a must-pass Omnibus [spending bill] at the 11th hour, without debate."[9] Fearing an impending government shutdown, President Obama was obliged to sign the two thousand plus page spending package that funds the government through September 2016.[10] This has secured the highly controversial Cybersecurity Act of 2015, a place in United States law.[11] Little is known about what long-term effects this hidden bill could have, but on initial inspection, it seems as if it will do more harm than good for the people of the United States.[12]

It is inevitable for a bill like this to be scrutinized harshly, just a few years following the release of thousands of National Security Administration (NSA) documents. However, the opponents to this bill may have a serious reason to be speaking out against it.[13] This bill seems to have been drafted broadly, tending to make the bill not only one for cyber security, but for cyber surveillance.[14]

Attacks (January 28, 2015), *available at* https://d1ovv0c9tw0h0c.cloudfront.net/files/2015/01/HSGAC-Cybersec-tes-1-28-15-final-TEH.pdf

[7] *Id*.

[8] Tom Risen, *Obama Signs Cybersecurity Law In Spending Package*, U.S. NEWS, December 18, 2015, *available at* http://www.usnews.com/news/articles/2015-12-18/obama-signs-cybersecurity-law-in-spending-package.

[9] *Id*.

[10] *Id*.

[11] Velazco, *supra* note 5.

[12] *Id*.

[13] Robyn Greene, *The Protecting Cyber Networks Act: Undermines Privacy, Enables Cyber-Surveillance, and Threatens Internet Security*, OPEN TECHNOLOGY INSTITUTE, (April 20, 2015), https://www.newamerica.org/oti/the-protecting-cyber-networks-act/

[14] Opposition Letter to Representatives, Civil Society Organizations, (April 20, 2015), https://static.newamerica.org/attachments/2885-coalition-letter-from-55-civil-society-groups-security-experts-and-academics-opposing-pcna/Coaltion%20Letter%20Strongly%20Opposing%20PCNA.b24d1869025848cb96385603d8208dea.pdf

The overly broad language of the CSA may result in companies to significantly expand monitoring of their users information and permit sharing to the federal government of private user information that would otherwise be illegal under previous cyber bills.[15] Additionally, the bill requires federal entities to automatically distribute this user information to other agencies, like the NSA, and authorizes law enforcement to use this to investigate any threats of crime that they may find.[16]

While it is necessary to help combat cyber criminals that threaten the foundation of the modern technological era, it is of greater concern to protect the privacy interests granted to individuals in the United States. Part II of this Note will provide a history of cyber attacks and the road that was taken to get to the CSA. Part III will provide an analysis of how the passing of the CSA will result in the undermining of the Electronic Communications Protections Act (ECPA), and could potentially invoke constitutional issues within the Fourth Amendment. Part IV will argue for an amending of such legislation that will narrow the scope of the bill to encompass that which the bill intends to cover, only cyber security.

Part II: The Road To The CSA

The last decade has seen an unprecedented increase in the number of cyber attacks throughout the world.[17] As technology advances, and cyber defense measures improve, cyber criminals and their offensive tactics change.[18] What started as mild disruptions by pranksters installing worms and viruses on basic computers has evolved into malware codes that can spread

---

[15] Jadzia Butler, *Cybersecurity Information Sharing In the "Omnious" Budget Bill: A Setback for Privacy*, CDT, (December 17, 2015) https://cdt.org/blog/cybersecurity-information-sharing-in-the-ominous-budget-bill-a-setback-for-privacy/

[16] Risen, *supra* note 8.

[17] NATO, Cyber Security Infographic, http://www.nato.int/docu/review/2013/cyber/Cyber-Security-in-Focus/EN/index.htm

[18] Gregory Webb, *Evolution of Cyber Attacks Infographic*, VENAFI, (August 21, 2013), https://www.venafi.com/blog/post/evolution-of-cyber-attacks-infographic/

throughout entire networks of company computers.[19] Hacking has become a profession, and with an increase of malicious targeting of businesses and government agencies, the stakes have been raised.[20] Reasons for the attacks differ, from anarchist groups such as Anonymous, to college students just trying to get an extra buck, the results are the same, secrets are leaked and money is lost.[21]

The history of cyber attacks dates back to the late 1980s, when the first computer worm was created.[22] This virus, generated by Robert Morris, "was the first widespread instance of a denial-of-service (DoS) attack."[23] While the Internet was still developing into what it would become today, the "Morris Worm" laid the foundation for future hackers to follow.[24] This worm would also gain the attention of Congress, as they passed the Federal Computer Fraud and Abuse Act (CFAA), which made certain cyber crimes a felony offense.[25] But computer hacks at this point were nothing more than an annoyance, and a hobby for computer fanatics.[26]

As the personal computer began to integrate into the average American family household, from 22.9 percent of households owning one in 1993 to 61.8 percent of households in 2003, hackers began to realize the potential damage they could cause and the rewards they could quickly reap.[27] Most importantly, the Internet began to grow in popularity and the information

---

[19] *Id.*
[20] *Id.*
[21] *See generally* Andy Greenberg, *Google's Three Tips For Sabotaging the Cybercrime Economy*, WIRED MAGAZINE, September 24, 2015, *available at* http://www.wired.com/2015/09/google-offers-3-lessons-crippling-online-crime-economy/?mbid=social_fb
[22] Ted Julian, *Defining Moments in the History of Cyber-Security and the Rise of Incident Response*, INFOSECURITY-MAGAZINE, December 4, 2014, http://www.infosecurity-magazine.com/opinions/the-history-of-cybersecurity/
[23] *Id.*
[24] *Id.*
[25] Florida Tech University Alliance, *A Brief History of Cyber Crime,* http://www.floridatechonline.com/resources/cybersecurity-information-assurance/a-brief-history-of-cyber-crime/
[26] Webb, s*upra* note 18.
[27] Statista, Percentage of Households With a Computer At Home From 1984 to 2010, http://www.statista.com/statistics/184685/percentage-of-households-with-computer-in-the-united-states-since-1984/; *See generally* Webb, *supra* note 18.

average people and homeowners began to share over the World Wide Web would soon create a new black market for hackers.[28]

As quoted by internationally known hacker, Space Rogue, "[t]he web changed [things], putting stuff at everyone's fingertips. Money became the driving force behind the hacks."[29] The world began to run on computers, from "the stock market, to hospitals, and credit card transactions" and before the risk was assessed, hackers would make these businesses and innocent individuals pay.[30] The early 2000s would see a sharp increase in attacks, ranging from malicious spam malware to steal login credentials, to DoS attacks on Microsoft, affecting hundreds of thousands of computer users.[31] Federal entities were so slow to target and catch these cyber criminals, that in 2003 Microsoft offered five million dollars for information that would help lead to arrests of hackers affecting their operating system.[32]

The Internet age would be flipped upside down in 2007 when Albert Gonzalez, a young hacking mastermind, and his criminal enterprise, revealed to have stolen over 180 million credit card accounts from TJX, the company which owned Target, Home Depot and many more.[33] While working simultaneously for the Secret Service, he and his affiliates inflicted damage to the company that would total more than four hundred million dollars over a two-year period.[34] This put governments and businesses on full watch, as the world now could see the true damage that cyber criminals could cause.[35]

---

[28] Jose Pagliery, *The Evolution of Hacking*, CNN, June 4, 2015, http://www.cnn.com/2015/03/11/tech/computer-hacking-history/
[29] *Id.*
[30] *Id.*
[31] *Id.*
[32] Paul R. La Monica, *Microsoft: Bounty Hunter*, CNN MONEY, November 5, 2003, http://money.cnn.com/2003/11/05/technology/microsoftbounty/
[33] James Verini, *The Great Cyberheist*, NEW YORK TIMES MAGAZINE, November 10, 2010, *available at* http://www.nytimes.com/2010/11/14/magazine/14Hacker-t.html?_r=0
[34] *Id.*
[35] *Id.*

Things worsened over the next few years and into today.[36] As new hacking groups and criminal organizations have formed and flourished, the rate and cost to major companies, has increased substantially.[37] Just in 2014, attacks occurred against companies such as Sony Pictures, Home Depot, and JP Morgan.[38] The JP Morgan breach "affected more than 76 million households and seven million small businesses," thus deemed the biggest hack of consumer data in United States history.[39] Estimates figure that the "annual cost to the global economy from cybercrime is more than $400 billion."[40]

The effects of a cyber attack go far beyond that of money and the bottom line.[41] As countries become more dependent on technology, "the threat posed by any one cyber attack can have devastating effects around the world."[42] Money is not the only worry, as cyber attacks have been carried out by multiple nations such as Russia, China, Iran and North Korea, lives could be threatened.[43] The potential exists that an attack could "cause physical destruction" and a "cyber Pearl Harbor" with a single keystroke.[44] The United States government is just as prone, as in 2014 alone there were over 67,000 cyber attacks on federal agencies.[45] This is compared to only 5,500 in 2006, an increase of over 1,100 percent in fewer than ten years.[46]

---

[36] Pagliery, *supra* note 28.
[37] Webb, *supra* note 18.
[38] Nojeim, *supra* note 6.
[39] Press Release, Office of Homeland Security, Secretary Napolitano Opens New Cybersecurity and Communications Integration Center, (October 30, 2009), http://www.dhs.gov/ynews/releases/pr_1256914923094.shtm
[40] Center for Strategic and International Studies, *Ness Losses: Estimating the Global Cos of Cybercrime*, June 2014, *available at* http://csis.org/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf
[41] Andrew Nolan, CONG. RESEARCH SERV., R43941, CYBERSECURITY AND INFORMATION SHARING: LEGAL CHALLENGES AND SOLUTIONS, (2015), at 2.
[42] *Id.*
[43] *Id.*
[44] Leon E. Panetta, Sec'y U.S. Dep't of Def., *Remarks on Cybersecurity to the Business Executives For National Security* (October 11, 2012)
[45] Andrea Peterson, *This Terrifying Chart Explains Why Cybersecurity is Such a Big Problem For The Government*, THE WASHINGTON POST, (June 18, 2015), *available at* https://www.washingtonpost.com/news/the-switch/wp/2015/06/18/this-terrifying-chart-explains-why-cybersecurity-is-such-a-big-problem-for-the-government/
[46] *Id.*

Today, to understand the sharing aspect of the CSA, it is important to discern how exactly companies and entities monitor, combat and subsequently share cyber threats. Most entities use cyber security providers, who deliver "signatures" to help combat malicious cyber activity.[47] These signatures are "specific machine readable patterns of network traffic that affect the integrity, confidentiality or availability of computer networks, systems and information."[48] They report back specific cyber threat indicators, which hackers store within IP addresses, domains, emails, and files in which the signature can read.[49]

The occurrence and complexity of these attacks increase each year, as hackers become more adept to the changing signature scans and other attempts of both the government and private companies to gain the upper hand.[50] Previously, over 75 percent of perceived threats were made using basic spam, which could be prevented quite easily.[51] Today, that basic form of cyber warfare has fallen to 42 percent, while malware and phishing are perceived to be 59 percent and 57 percent of current threats respectively, which result in much larger and undetected data breaches.[52] The success of these criminals has risen as well, as the number of successful attacks has increased by 144 percent in the last five years and the time spent for both agencies and companies to combat such attacks has increased by 221 percent.[53] These numbers are shocking, and it is apparent that some action must be taken to help combat this issue.

---

[47] Michael Daniel, White House Cybersecurity Coordinator, 007 or DDoS: What is Real World Cyber? at the RSA Conference (February 28, 2013), *available at* http://www.whitehouse.gov/sites/default/files/docs/2013-02-28_final_rsa_speech.pdf

[48] DOUGLAS LOVELACE, TERRORISM: COMMENTARY ON SECURITY DOCUMENTS: THE CYBER THREAT 23 (Oxford University Press, Volume 140, 2015)

[49] *Id.*

[50] Steinhauer, *supra* note 2.

[51] CYBER SECURITY AND TRANSFORMATIONAL TECHNOLOGIES: KEEPING SYSTEMS AND DATA SAFE 4 (The Lockheed Martin Cyber Security Alliance, 2012) *available at* http://www.lockheedmartin.com/content/dam/lockheed/data/isgs/documents/LM-Cyber-Security-Transformational-Technologies.pdf

[52] *Id* at 6.

[53] Steinhauer, *supra* note 2.

B. Unsuccessful Attempts at Securing Cyber Networks

Following attacks on the Pentagon, Department of Defense, NASA, and major US banking institutions, legislators proposed an information sharing system called the Cyber Intelligence Sharing and Protection Act (CISPA) in 2011.[54] The bill was the origin of the current CSA, and proposed a way for the government and private companies to share data instantaneously without the need for court orders.[55] The bill passed through the House of Representatives by a vote of 248 to 168, but did not make it much farther, as adversaries began speaking out against the bill.[56] A year after its dissolution, in early 2013, the bill was proposed to the House of Representatives in an identical form.[57]

This bill and the encompassing cyber security measures seemed to have a positive outlook for legislators, as President Obama even signed an executive order "setting forth a proposed program to support the cyber security efforts of privately owned [businesses]."[58] After the release of thousands of sensitive government documents from whistleblower Edward Snowden, things quickly changed.[59] With government snooping and privacy fears at the forefront of US minds, CISPA was slowly dismembered, as privacy opponents cited a few major flaws with the bill, which are similar to the ones that plague CSA today.[60]

One of CISPA's major defects was its definition of "cyber threat information."[61] "Cyber threat information" was defined as "intelligence in the possession of an element of" anyone

[54] NATO, The History of Cyber Attacks – a Timeline, *available at* http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm
[55] Mark Peckham, *5 Reasons the CISPA Cybersecurity Bill Should Be Tossed*, Time Magazine Opinion, April 19, 2012, *available at* http://techland.time.com/2012/04/19/5-reasons-the-cispa-cybersecurity-bill-should-be-tossed/
[56] Jay P. Kesan, *Creating a Circle of Trust To Further Digital Privacy and Cybersecurity Goals*, Mich. St. L. Rev. 1475, 1480, (2014)
[57] *Id*. at 1480.
[58] *Id*.
[59] *Id*.
[60] Butler, s*upra* note 15.
[61] Kesan, s*upra* note 53 at 1501.

outside the government intelligence community.[62] This definition was very vague, opening the door for countless interpretations of what included a "cyber threat."[63] CISPA was the first bill to try to break down legal barriers between government entities and the private sector, as it could expand the scope of what information they could receive.[64] For example, "a company like Google, Facebook, Twitter, or AT&T could intercept your emails and text messages, send copies to one another and to the government, and modify those communications or prevent them from reaching their destination if it fits into their plan to stop 'cyber security' threats."[65]

This bill was so broad that the White House threatened to veto the bill if it reached President Obama's desk.[66] The White House believed that CISPA "still seek[ed] additional improvements and if the bill, as currently crafted, were presented to the President, his senior advisors would recommend that he veto the bill." [67] This seemed to be the final blow to CISPA, as the Administration stated that they "remain[ed] concerned that the bill does not require private entities to take reasonable steps to remove irrelevant personal information when sending cyber security data to the government or other private sector entities." [68] While the bill lost its steam, due to the aforementioned Snowden leaks, the Obama Administration did seem to have their sights set on an information-sharing platform in the near future, once the publicity surrounding government privacy concerns started to subside.[69]

C. The Revival of Information Sharing and an Overview of the CSA

---

[62] *Id*. at 1495.
[63] Peckham, s*upra* note 52.
[64] *Id*.
[65] *Id*.
[66] Executive Office Of The President, Statement of Administration Policy (April 26, 2013), *available at* https://www.whitehouse.gov/sites/default/files/omb/legislative/sap/113/saphr624r_20130416.pdf
[67] *Id*.
[68] *Id*.
[69] Steven Dennis, *Obama Pushes for Deals on Cybersecurity, Trade, Taxes*, (January 13, 2015), available at http://blogs.rollcall.com/white-house/obama-meeting-with-top-congressional-leaders-without-harry-reid/? pos=adpb

While CISPA died in its tracks in 2013, this information-sharing platform has continuously been lauded as a necessary means to help protect private entities and government agencies against the threat of hackers.[70] Some proponents argue that the "receipt of critical threat data can and has been shown to prevent potential cyber attacks and mitigate ongoing threats."[71] The "one point of general agreement amongst cyber-analysts is the perceived need for enhanced and timely exchange of cyber-threat intelligence."[72]

Recently, the Senate and House legislators reevaluated the deficiencies of the original CISPA bill and revived it in early 2015.[73] Similar bills were introduced and passed in both the Senate and the House within 2015.[74] The House version, the Protecting Cyber Networks Act (PCNA), gained more steam than CISPA ever did, and even to many Democrats' surprise, also gained support with the White House.[75] In the Senate, the Cybersecurity Information Sharing Act (CISA) entailed much of what was contained within the PCNA.[76] While there existed many overlaps between the two bills, they became the basis for the now in effect CSA.[77] However it seems many of the privacy protections, which were contained in the previous bills, have been pushed aside.[78]

The CSA bill puts a recently developed agency, the National Cybersecurity and Communications Integration Center (the Center), to develop the process in which private entities

---

[70] Steinhauer, *supra* note 2.
[71] Kimberly Peretti, *Cyber Threat Intelligence: To Share or Not to Share—What Are the Real Concerns?*, 13 PVLR 1476 (2014)
[72] Nolan, *supra* note 41.
[73] Greenberg, *supra* note 4.
[74] Tom Risen, *Cybersecurity Bill Passes In* Senate, US News (October, 27, 2015), *available at* http://www.usnews.com/news/articles/2015/10/27/opposition-mounts-as-cybersecurity-bill-goes-before-senate
[75] *Id*.
[76] Abigail Tracy, *The Problems Experts And Privacy Advocates Have With The Senate's Cybersecurity Bill*, Forbes, October 29, 2015, *available at* http://www.forbes.com/sites/abigailtracy/2015/10/29/the-problems-experts-and-privacy-advocates-have-with-the-senates-cybersecurity-bill/ (Outlining CISA and how it compares with PCNA)
[77] *Id*.
[78] Butler, *supra* note 15.

will share information with the government.[79] This Center has been established under the umbrella of the Department of Homeland Security (DHS), which has already funded 1.2 billion dollars to the Center as of 2014, with 800 million dollars set aside for cyber security programs.[80]

The CSA has four major flaws that worry privacy and civil liberty advocates.[81] The first issue is that the CSA provides an overarching authorization for companies to monitor their networks for "cyber security purposes."[82] Second, the CSA authorizes companies to share a large amount of their user information with the government and with one another, granted that the shared information is a "cyber threat indicator," which includes "information that is necessary to describe or identify . . . any . . . attribute of a cyber security threat."[83] Next, it would allow companies to disseminate this information with any government agency, and encourages it to directly share with the newly established Center, but would require that information to also be disseminated to other government agencies ranging from the FBI to the NSA.[84] The CSA would then allow any government agency that receives this information, to use it for investigation or prosecution of any crimes that could result in "a specific threat of death, a specific threat of serious bodily harm, or a specific threat of serious economic harm."[85]

Part III: Analysis

A. Laws That Will Be Implicated By The CSA

The issues within the CSA may cross a multitude of legal lines.[86] The CSA traverses into territories of electronic privacy laws, most significantly being the Electronic Communications

[79] H.R. Con. Res. 2029, 114th Cong., Division N Title II (2015) (enacted)
[80] U.S. CONGRESSIONAL BUDGET OFFICE, S.2519, NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER ACT OF 2014 COST ESTIMATE (2014), *available at* https://www.cbo.gov/publication/45594
[81] Butler, *supra* note 15; *See generally* Peretti, *supra* note 71.
[82] H.R. Con. Res. 2029, 114th Cong., Division N Title I Sec. 102(4) (enacted)
[83] H.R. 2029, Division N Title I Sec. 102(6)
[84] H.R. 2029, Division N Title I Sec. 105(d)(A)
[85] *Id*.
[86] Pereitti, *supra* note 71.

Privacy Act (ECPA). The CSA has also been alleged to overstep the government's scope of a permissible search and seizure under the Fourth Amendment.[87]

The ECPA restricts the government's use of wire tapping transmissions of electronic data by a computer, prohibits access to stored electronic communications, and tracing of such.[88] The statute prohibits the disclosure or use of any contents of any electronic communication that was obtained through an illegal interception.[89] This includes providers who are able to monitor their own networks, but are not permitted to release such information.[90]

The Fourth Amendment protects American citizens from unreasonable searches and seizures by government officials, and compliance with such requires a court warrant.[91] This protection only extends to individuals when there is a "reasonable expectation of privacy."[92] While it will take a multitude of court interpretations to figure out how far the CSA can extend, it seems that it may violate the Fourth Amendment and have an impact over what information can and cannot be shared by the new law.

B. The CSA Undermines the Current ECPA.

The first major issue is that the CSA authorizes companies to monitor all of their users' activities, opening the door for unauthorized interception of private information.[93] Right now, the ECPA, the most in depth law that covers this area, prevents any person or entity to intercept any electronic communication.[94] To intercept, means to use "any electronic . . . device, to acquire the contents or the substance . . . or meaning of the communication."[95] Furthermore, the ECPA

[87] *Id.*
[88] *Id.*
[89] Electronic Communications and Privacy Act, 18 U.S.C. §2511(1)(c)-(d) (1986)
[90] *Id.*
[91] U.S. Const. amend. IV
[92] *Id.*
[93] Butler, *supra* note 15.
[94] 18 UCS §2511 (2)(a)(i)
[95] *Id.*

prohibits the disclosure or use of the contents of any electronic communication that was obtained in violation of the statue.[96] With a general reading of this provision, this privacy law would seem to be in conflict with the new CSA.

The ECPA has two exceptions that the CSA intends to work around.[97] The exceptions provide that information can be retrieved with authorization by "a party to the communication" and allows companies to supervise their own networks for self-defense.[98] The first exception has already been trouble for courts, as it is difficult to determine in electronic communications, who is exactly a "party to the communication."[99] During a DoS attack, any user on a network who has opened a malicious file can be construed to fall under this definition of a "party to the communication."[100]

The second exception allows service providers to monitor their own systems with consent of the user, in "the normal course of employment, while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service."[101] This enables these providers to conduct some monitoring to detect or defend against an attack after gaining consent of the individual, and may then disclose such communications recovered.[102] While there is one court who has disagreed, most courts have determined that this exception can only be used with the purpose of protecting one's own

[96] 18 U.S.C §2511(2)(ii)(B)
[97] *Id.*
[98] *Id.*; Gilday v. Dubois, 124 F.3d 277, 297 (1st Cir. 1997) (stating that for the consent exception to apply, the consent must be one who is a party to the communication)
[99] *See generally* Dep't of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, (2009), www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf
[100] Caro v. Weintraub, 618 F.3d 94 (2d Cir. 2010)
[101] 18 U.S.C §2511(2)(a)(i)
[102] *Id*.

"equipment and rights."[103] Barring these exceptions, narrowly interpreted as courts have held, the ECPA prevents any person or entity from intercepting and disclosing any other electronic communications, protecting American's privacy in the electronic realm.[104]

The CSA states that private entities can now "*[n]otwithstanding any other provision* of law . . . for a *cyber security purpose* monitor any information system of such private entity . . . [or] information that is stored on, processed by, or transiting an information system monitored by the private entity."[105] This appears the CSA gives private companies blanket permission to monitor any traffic coming through its site, completely waiving the provisions of the Wiretap Act and the ECPA.[106] The language "[n]otwithstanding any other provision of law" would suggest that the CSA now trumps the ECPA, expanding the scope of ISP monitoring in ways far beyond current law.[107] This provision allows businesses and service providers to now monitor all of its users, without a consensual agreement and not only to protect themselves.[108] More troublesome, is what these companies can do with the information that it collects.

Next, the CSA will enable these companies to take the overbroad security monitoring it has been granted, and disseminate it to the Center, who will then distribute it to other government organizations and private entities.[109] The CSA defines something that can be shared as "cyber threat indicators," which means "information that is necessary to describe or identify . . . any other attribute of a cyber security risk."[110] Again, directly contrary to the exact language of

---

[103] United States v. Pervaz, 118 F.3d 1 (1st Cir. 1997) (holding that a company could intercept electronic communications to help protect its customers); Campiti v. Walonis, 611 F.2d 387 (1st Cir. 1979) (Held that company could monitor and intercept calls as protection of its own equipment and rights)
[104] 18 U.S.C §2511 (1)
[105] H.R. 2029, Division N Title I Sec. 104(a) (emphasis added).
[106] Jennifer Granick, *CISA Pits DHS Against the FCC and FTC on User Privacy*, JUST SECURITY (December 16, 2015), *available at* https://www.justsecurity.org/28386/omnicisa-pits-government-against-self-privacy/
[107] *Id*.
[108] *Id*.
[109] *Id*.; H.R. 2029, Division N Title I Sec. 105(d)(A)
[110] H.R. 2029, Division N Title I Sec. 102(6)

the ECPA, which does not authorize service providers to ever disclose or divulge to private entities or government personnel any contents of communications for the purpose of protecting a third party.[111] Courts have consistently held, that even if the provider is acting out of inherent self-interest, in no way does the ECPA allow "unlimited" interceptions and then subsequent disclosures of those unauthorized seizures.[112] This issue was something that even the DHS itself was wary about in the Senate version of the CSA back in August 2015, as Deputy Secretary of the DHS stated,

> [w]hile the [CISA] seeks to incentivize non-federal sharing through a DHS portal, the bills authorization to share with any federal agency "notwithstanding any other provision of law" undermines that policy goal . . . . The authorization to share cyber threat indicators and defensive measures with "any other entity or the Federal Government," "notwithstanding any other provision of law" could sweep away important privacy protections, particularly the provisions in the [ECPA] limiting the disclosure of the content of electronic communications to the government by certain providers.[113]

The way the CSA is written, can be construed very broadly, to often times include information of a potentially innocent person.[114] "Cyber threat indicators" in the new CSA, has been expanded from its origin bills, to now include provisions to share information that describe attributes of a cyber security threat and potential harms caused by an incident.[115] This

---

[111] *See generally* Aaron J. Burstein, *Amending the ECPA to Enable a Culture of Cybersecurity Research*, 22 Harv. J.L. & Tech. (2008)

[112] United States v. Auler, 539 F.2d 642, 646 (7th Cir. 1976); United States v. Councilman, 418 F.3d 67 (1st Cir. 2005) (holding that the narrow exception did not permit a provider to intercept and copy all incoming communications)

[113] Alex Wilhelm, *Department of Homeland Security Highlights Privacy Concerns In Senate Cybersecurity Bill*, TECHCRUNCH (August 3, 2015), *available at*, http://techcrunch.com/2015/08/03/department-of-homeland-security-highlights-privacy-concerns-in-senate-cybersecurity-bill/

[114] Mike Godwin, *The Many, Many, Many Flaws of CISA*, RSTREET (October 27,2015), *available at* http://www.rstreet.org/op-ed/the-many-many-many-flaws-of-cisa/

[115] Open Technology Institute, Summary Comparison Chart: Information Sharing Authorities and Privacy Protections Under CISA, PCNA, and NCPAA, *available at* https://static.newamerica.org/attachments/12213-intelligence-committees-hijacked-cyber-negotiations-and-raced-to-the-bottom-on-privacy/UpdatedChartofCyberInfoSharingBillsComparisonChart.be53df22fbef42ae8e17672179e57eb5.pdf (Chart outlining the differences between CISA, PCNA, and CSA)

information may allow sharing of unnecessary Personally Identifiable Information (PII).[116] PII could include any sensitive information shared across the web, such as medical information, Social Security Numbers, or financial information.[117] For example, an innocent victim's computer may have been compromised by an unsuspecting hacker, and is now being accessed to engage in malicious activity, such as spear phishing emails, without the user's knowledge.[118] The service provider, or any company whose system this hacker reaches, can now share the IP address not of the hacker but of this victim.[119] This will release not only the private identity of who the victim is, maybe even some PII of this innocent customer.[120]

While in the CSA's defense they do encourage and require for a non-federal entity to remove any personal identification that they find, these restrictions still seem to be overly broad.[121] The CSA provides that a non-Federal entity must "review [a] cyber threat indicator to assess whether such cyber threat indicator contains any information not directly related to a Cybersecurity threat the non-Federal entity knows at the time of sharing to be personal information of a specific individual . . . and remove such information."[122] It can also implement a technical process to search for such individual information.[123]

Yet, what is a non-Federal entity supposed to do when they do not "know at the time of sharing" whether a cyber threat indicator contains personal information not "directly related" to

---

[116] *Id*.
[117] Margaret Rouse, *Personally Identifiable Information,* WHATIS, *available at* http://searchfinancialsecurity.techtarget.com/definition/personally-identifiable-information
[118] *Id*.; Federal Burearu of Investigation, Spear Phishers: Angling to Steal Your Financial Info, (April 1, 2009), *available at* https://www.fbi.gov/news/stories/2009/april/spearphishing_040109 (spear phising is "a virtual trap set by cyber thieves that uses official-looking e-mails to lure you to fake websites and trick you into revealing your personal information.")
[119] Granick, s*upra* note 109.
[120] *Id*.
[121] H.R. 2029, Division N Title I Section 104(d)(2)(A)
[122] *Id*.
[123] H.R. 2029, Division N Title I Section 104(d)(2)(B)

such cyber threat indicator? According to the recent CSA guidelines that the DHS released, if a non-Federal entity does not know at the time of sharing, "the non-federal entity is not required to alter the shared information."[124] In the heat of the moment of a massive security breach, this leaves the door open for entities to now claim that they simply did not know of any personal information at the time of sharing, and ultimately circumvent the tedious, and possibly costly option of searching for personal information.

This information is intended to be protected private information that the ECPA is sought to safeguard. However the CSA now guards all non-Federal sharers, shielding them behind a veil of liability protection.[125] The CSA provides that "no cause of action shall . . . be maintained in any court against any private entity . . . for the monitoring of an information system . . . that is conducted in accordance with this title."[126] Combined with the fact that non-Federal entities seem to be able to share the "kitchen sink," as long as they "did not know" it contained personal information, these same non-Federal entities now receive complete government protection for committing such acts.[127] All of this seems to eradicate the ECPA, resulting in far less protection for individuals on their devices.[128] The dissemination of this information, while illegal under the ECPA, may have far greater consequences for individuals.

C. The CSA and the Fourth Amendment

The passing of the CSA has opened the door by privacy advocates of its potential Fourth Amendment violations. These advocates suggest that because the CSA allows the federal

[124] The Department of Homeland Security, Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Mesaures with Federal Entities Under the Cybersecurity Information Sharing Act of 2015, 11 (February 16, 2016), *available at* https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_%28Sec%20105%28a%29%29.pdf
[125] *Id*., H.R. 2029, Division N Title I Section 106.
[126] H.R. 2029, Division N Title I Section 106(a).
[127] *Id*.; Granick, *supra* note 109.
[128] *Id*.

government to use information contained within shared cyber security threats, to investigate or prosecute individuals for crimes outside the scope of cyber crime, that individuals Fourth Amendment rights are at stake.[129] While this new government tool for prosecution does raise concern, the CSA seems to be drafted perfectly to circumvent Fourth Amendment violations, as they are presently interpreted.

The Fourth Amendment protects Americans against "unreasonable searches and seizures."[130] A "search" under the Fourth Amendment, specifically in the context of electronic communication, takes place when the governments monitoring violates "an expectation of privacy" that society considers reasonable.[131] A seizure, in turn, occurs "when there is some meaningful interference with an individuals interests" in their property.[132] It seems that the CSA could implicate the government on the search aspect of the Fourth Amendment, more so than the seizure.

In *Katz v. United States*, the Supreme Court held that there was an expectation of privacy in electronic telephone conversations.[133] However, in *Smith v. Maryland*, the Supreme Court held that no reasonable expectation of privacy existed on telephone records.[134] Finding where the information shared in the CSA falls between these two expectations, will determine whether such conduct could be considered a Fourth Amendment violation. However, an individual will first have to show that a government actor conducted the invalid search.[135]

---

[129] Robyn Green, *Sharing At of 2015 Is Cyber-Surveillance, Not Cybersecurity*, OPEN TECHNOLOGY INSTITUTE (April 9, 2015), *available at* https://www.newamerica.org/oti/cybersecurity-information-sharing-act-of-2015-is-cyber-surveillance-not-cybersecurity/
[130] U.S. Const. amend. IV.
[131] Katz v. United States, 389 U.S. 347, 360 (1967)
[132] United States v. Jacobsen, 466 U.S. 109 (1984)
[133] *Id*.
[134] 442 U.S. 735 (1979)
[135] Lizzy Finnegan, *CISA and the War On Privacy*, BREITBART (November 10, 2015), *available at* http://www.breitbart.com/tech/2015/11/10/cisa-and-the-war-on-privacy/

The Fourth Amendment only protects an individual against the actions of the government, not of individuals.[136] For the private entities that share information under the CSA, they will have to be regarded as an agent of the government in order for any individual to claim that the search that has occurred, is in fact a Fourth Amendment violation.[137] A search could be treated as a government search, "if the government coerces, dominates, or directs the actions of a private person."[138] Whether a private entity is considered an agent of the government, "necessarily turns on the degree of the government's participation in the private party's activities."[139] Many courts have employed a two-part totality of the circumstances test, which states that the government had to know of and acquiesce the intrusive conduct, and then whether the party performing the search intends to "assist law enforcement efforts or further his own ends."[140]

Using this test, one can analyze the conduct that will be taking place by private entities under the CSA. First, it seems that the government not only knows of, but also is encouraging businesses and private entities to engage in this monitoring and sharing of conduct. But, whether private entities are engaging in this type of activity to assist law enforcement, or to further their ends, is going to be an area of concern for courts in the time to come. On one side, these entities will be sharing information about attacks, which have already occurred, meaning that their interest in sharing this is limited, except to the extent of helping law officials find criminals. On the other side entities will be sharing this information in real time, with the hope that the Center has seen a similar cyber indicator, and can provide ways in which to stop it. While the former

[136] Burdeau v. McDowell, 256 U.S. 465, 475 41 S.Ct. 574, 65 L.Ed. 1048 (1921)
[137] U.S. v. Souza 223 F.3d 1197, 1201 (10th Cir. 2000)
[138] Pleasant v. Lovell, 876 F.2d 787, 796 (10th Cir. 1989).
[139] Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602, 614 (1989)
[140] *Souza*, 223 F.3d at 1201.

seems to suggest that these private entities could be acting simply to assist law enforcement, the latter provides that they will be acting to further their own ends.

Notwithstanding any of the foregoing, an even bigger challenge to anyone bringing such claim will rest in the fact that the government does not make sharing mandatory.[141] The CSA makes it clear that nothing within its title creates a duty for any one, to share anything.[142] This may weaken any individual's argument that a private entity that is engaging in information sharing is in fact a government agent.[143] It has been held that, if a government agent "is involved "merely as a witness," the requisite government action is absent and the search will be deemed private."[144] However, the argument can still be made, as the 10th Circuit has held, that conduct is suspicious, and closer to a government actor, if a private search follows government encouragement.[145] Here, although the government is enticing private companies to share, the companies will seemingly be engaging in this conduct to advance their own interests, to help combat cyber attacks against them, improving their service to their customers.[146] For these reasons, the Fourth Amendment most likely will not be implicated.

If an individual can show that a private entity is determined to be a government actor in terms of the CSA, the next question will be whether there is a search in which an expectation of privacy exists.[147] The CSA makes it clear that any of the government agencies that receive cyber-threat information, can then use the information to investigate or prosecute.[148] The text of the bill clearly states,

---

[141] H.R. 2029, Division N Title I Section 106(e).
[142] *Id*.
[143] *Souza*, 223 F.3d at 1202.
[144] *Id*.
[145] *Id*.
[146] Jeremy Broggi, *Building on Executive Order 13,636 to Encourage Information Sharing For Cybersecurity Purposes*, 37 HARV. J.L. & Pub. Pol'y 653, 662 (2014)
[147] *Id*. at 663.
[148] H.R. 2029, Division N Title I Sec. 105(d)(A)

> Cyber threat indicators and defensive measures provided to the Federal Government under this title may be disclosed to . . . any Federal agency, department, component, officer, employee, or agent of the Federal Government solely for (i) a cyber security purpose . . . (iii) the purpose of responding to, or otherwise preventing or mitigating a specific threat of death, a specific threat of serious bodily harm, or a specific threat of serious economic harm . . . (v) [for] the purpose of preventing, investigating, disrupting, or prosecuting an offense arising out of a threat described in clause (iii).[149]

While problematic, it may not extend to private information that has been held to have an expectation of privacy. It will ultimately come down to what type of personal information will make it past the non-Federal entities doors, and into the hands of the government. Courts have held that information conveyed to third parties, or information exposed to employees in their ordinary course of business, does not have a reasonable expectation of privacy.[150] Information such as email address names, email subject lines, websites visited, and amount of data transferred all fall outside the scope of a reasonable expectation of privacy under the Fourth Amendment.[151]

However, if an individual's email is compromised and malicious content is sent within an email exchange between said individual and another, it is possible that this exchange could be shared from the Internet provider, as a cyber security threat to the government. The government could then be in possession of these emails, and if this exchange contained anything in reference to bodily harm or death to someone, then the government could investigate or even prosecute using these emails.[152] Under *United States v. Warshak*, the Sixth Circuit determined that a "subscriber enjoys a reasonable expectation of privacy in the contents of emails "that are stored

[149] *Id*.
[150] United States v. Miller, 425 U.S. 435, 96 S.Ct. 1619 L.Ed.2d 71 (1976)
[151] United States v. Forrester, 412 F.3d 500, 510 (9th Cir. 2008)
[152] H.R. 2029, Division N Title I Sec. 105(d)(A)

with, or sent or received through, a commercial [Internet Service Provider (ISP)]."[153] This court went further to state that the "government may not compel a commercial ISP to turn over the contents of a subscriber's emails without first obtaining a warrant based on probable cause."[154] There are a number of possible PII or individuals information that may be sent to the Center in the coming years, that could present a case in which a reasonable expectation of privacy has been violated and a possible Fourth Amendment violation. Until then it will matter upon the precaution these private entities take in scrubbing and protecting their customers' private information.

Finally, if an individual is successful in proving that the private entity should be considered a government agent, and that they committed an invalid search by violating a reasonable expectation of privacy, the government may still be able to argue for a Fourth Amendment exception. The first, while brief, is a search conducted with consent. In this regard, if these entities include or enable a consent form on their website or service that their information is subject to such dissemination, maybe through a click-wrap agreement, then there would be no expectation of privacy for such user.[155]

If no consent was acquired, then the government may still be able to argue a "special needs" exception. If the government has a special need, it may eliminate the need for a warrant, only if the government can show that the search is reasonable at its inception and it is reasonable in scope.[156] The courts will balance the intrusion on individuals with the benefit of such warrantless searches to society.[157] While the government says it has a need to protect its citizens

[153] 631 F.3d 266, 288 (6th Cir. 2010)
[154] *Id*.
[155] United States v. Angevine, 281 F.3d 1140 (10th Cir. 2002)
[156] New Jersey v. T.L.O, 469 U.S. 325, 341 (U.S. 1985)
[157] Michigan Dep't of State Police v. Sitz, 496 U.S. 444, 449 (U.S. 1990)

form bodily harm or from death, it may not outweigh the intrusion on individuals, by being able to look through protected emails. While the information sharing could fall under the "special needs" doctrine, it would be specifically tailored to the details involving the initial cyber attack.[158] But a person who is being investigated through a CSA sharing, for an erroneous suspicion of a cyber attack, could end up being charged with a completely unrelated crime during the investigation.[159] All in all, the broad language of the CSA while difficult may open the door for Fourth Amendment challenges, as individuals' personal information may be released to the government through the sharing of private entities.

Part IV: Narrowing the Scope of the CSA

It is evident that some level of information sharing may be necessary when it comes to preventing future cyber attacks and hacking. While it certainly will not end such conduct, it may be a step in the right direction, granted this step is taken with privacy interests in mind. As the CSA is currently construed however, this information sharing challenges the authority of the ECPA, and could be a potential Fourth Amendment concern.[160] The purpose of the CSA can be achieved by a re-drafting to focus many aspects and provide for a narrower interpretation.

First, the definition of "cyber threat indicator" should be changed, removing the final two subsections, F and G, which provide that a "cyber threat indicator" can be a description of actual or potential harm caused by an incident, and "any other attribute of a Cybersecurity threat."[161] These two subsections are vague, and when drafting a bill that will enable such massive data collecting, these definitions open the door for private entities to share more rather than share less.

[158] Kesan, *supra* note 56.
[159] *Id*.
[160] Broggi, *supra* note 149.
[161] H.R. 2029, Division N Title I Sec 102(6)(F)-(G)

Next, the government hands the rights of the intermediary sharing system to that of a third party civilian agency, rather than a military agency.[162] As of now the CSA enables sharing by a third party or the government, to any government entity, including the NSA. Putting the responsibility of the intermediary in a private entities hands will stimulate more private involvement and enable the civilian agency to double check and scan such information that has been transmitted before releasing it to the government. Civilian agencies have recently had more transparency, as intelligence agencies are far more opaque.[163] The details about the scope and nature of civilian agency activities are more narrowly defined and interpreted, resulting in more understanding of what these agencies can and cannot do.[164]

This change will most likely encourage private entities that currently do not want to participate in sharing, for fear of government data collecting, to actually engage in this process. Many private entities have already publicly voiced their discontent with the CSA and the bills that preceded it, stating their desire to protect their users and their own information.[165] These companies include Apple, Twitter, Yelp, Wikipedia and Reddit.[166] After the Snowden leaks, mass collections by the government have resulted in little trust, that could be restored by having a third party intermediary.[167] While important cyber security information can still be shared in real time with the government, it would be beneficial to all parties to have it conducted through a non-governmental entity.

Additionally, even if a third party would be collecting this data, the bill needs to require that PII should be removed prior to sharing unless "it is necessary to identify or protect against a

---

[162] Nojeim, *supra* note 6.
[163] *Id*.
[164] *Id*.
[165] Juli Clover, *Apple Speaks Out Against Cybersecurity Information Sharing Act*, MACRUMORS (October 20, 2015), *available at* http://www.macrumors.com/2015/10/20/apple-speaks-out-against-cisa/
[166] *Id*.
[167] Finnegan, *supra* note 138.

threat."[168] As mentioned earlier, the CSA mandates the removal of PII, as long as the entity knows it isn't directly related to the threat, and if they are unsure, they are allowed to share it.[169] Changing this standard could greatly affect the bill, by limiting the scope of private entities ability to disseminate personal information. Further, the same standard should be adopted for the Center and the DHS. As of now, the Center has to destruct PII if it's *known* that the information isn't directly related to a threat. This new Center should only disseminate when it is *necessary* to block significant threats to national security.[170]

Finally, and most importantly, the Government should only be able to prosecute and arrest, for cyber security purposes, cyber criminals within the statute. Allowing the government to use information received through this cyber security bill to investigate non-computer crimes, changes the purpose of such bill. While it is important to stop crimes of serious bodily harm and death, it seems it can be achieved in ways that do not include mass data collection and sharing. This change would also seem to limit most potential violations that could arise of the Fourth Amendment.

Part IV: Conclusion

This Note puts forth the position that the Cybersecurity Act of 2015, currently undermines and violates the ECPA privacy laws, and raises potential Fourth Amendment violations. Cyber attacks are on a steady and violent rise, and have already resulted in a loss of billions of dollars for both the government and industries, making it is necessary to combat this problem, but it must be so without intruding into the civil liberties of the people of the United

[168] Open Technology Institute, *supra* note 118.
[169] Department of Homeland Security, *supra* note 127.
[170] *Id*.

States. This can be achieved through a narrower drafting of this legislation or new ideas, such as a third party intermediary.