WHAT DOES THIS MEAN? EXAMINING LEGISLATIVE AMBIGUITIES IN THE CYBERSECURITY ACT OF 2015 AND THE POTENTIAL FOR A FUTURE CIRCUIT SPLIT ON INTERPRETATION

Sarah E. Hsu Wilbur[*]

I. INTRODUCTION

Cybersecurity attacks are ever-evolving and ever-increasing threats to companies and individuals alike.[1] For example, the recent distributed denial-of-service (DDoS) attacks[2] that occurred on October 21, 2016, disrupted service to Spotify, Twitter, PayPal, Netflix, and Amazon, among others.[3] The attackers infected "hundreds of thousands of internet-connected devices" with malicious software—the Mirai botnet—and then used those devices to attack New Hampshire-based corporation Dyn, Inc., an Internet infrastructure company and domain name service provider in charge of

*J.D. Candidate, 2018, Seton Hall University School of Law; B.S., University of Florida. I would like to thank Professor Kristin Johnson for sparking my interest in cybersecurity law, which led me to write this Comment, and for her valuable guidance in writing this Comment. I would also like to thank my husband, Daniel Wilbur, and my family for their unending love and support.

[1] *See, e.g.*, Fayaz Khaki, *The Ever Increasing Cyber Security Challenge*, FIN. TIMES (June 9, 2014, 7:46 AM), http://capgemini.ft.com/secure-information/the-ever-increasing-cyber-security-challenge_a-41-362.html.

[2] Margaret Rouse & Peter Loshin, *Definition: Denial-Of-Service Attack*, TECHTARGET (2007), http://searchsecurity.techtarget.com/definition/denial-of-service (last updated Dec. 2016) (defining a denial-of-service attack as "a security event that occurs when an attacker takes action that prevents legitimate users from accessing targeted computer systems, devices or other network resources" and noting that these types of attacks "typically flood servers, systems or networks with traffic in order to overwhelm the victim resources and make it difficult or impossible for legitimate users to use them").

[3] Joseph Menn et al., *Cyber attacks disrupt PayPal, Twitter, other sites*, REUTERS (Oct. 21, 2016, 9:20 AM), http://www.reuters.com/article/us-usa-cyber-idUSKCN12L1ME; NBC News, *3rd Cyberattack 'Has Been Resolved' After Hours of Major Outages: Company*, NBC NEWS (Oct. 21, 2016, 9:32 AM), http://www.nbcnewyork.com/news/local/Major-Websites-Taken-Down-by-Internet-Attack-397905801.html (last updated Oct. 21, 2016, 6:53 PM). *See also* Nate Lanxon et al., *The Possible Vendetta Behind the East Coast Web Slowdown*, BLOOMBERG TECH. (Oct. 21, 2016, 9:08 AM), https://www.bloomberg.com/news/articles/2016-10-21/internet-service-disrupted-in-large-parts-of-eastern-u-s (stating that on October 21, 2016, hackers flooded U.S. servers with phony traffic, causing the servers to crash and millions of people to lose Internet access to some of the most popular websites in the world) (last updated Oct. 22, 2016, 1:54 AM).

redirecting a lot of Internet traffic.[4] Referred to as a "stunning breach of global internet stability,"[5] the attack spawned "from millions of internet addresses, making it one of the largest attacks ever seen."[6] This cyberattack caused outages in both the United States and Europe.[7] Security experts say the attack was a particularly powerful DDoS attack where the perpetrators flooded the targets with so much "junk traffic," causing them to freeze.[8]

Enacting legislation can help mitigate and prevent cyberattacks by establishing criminal and/or civil penalties for cyberattacks, by requiring companies to implement programs to identify potential cybersecurity risks and threats, and by requiring the government to thoroughly review cyber laws regularly.[9] Information sharing can also help mitigate and prevent cyberattacks.[10] On December 18, 2015, the legislative and executive branches of the United States government passed the Cybersecurity Act of

[4] Menn et al., *supra* note 3; Symantec Security Response, *Mirai: What you need to know about the botnet behind recent major DDoS attacks*, SYMANTEC CORP. (Oct. 27, 2016), https://www.symantec.com/connect/blogs/mirai-what-you-need-know-about-botnet-behind-recent-major-ddos-attacks ("A distributed denial of service attack (DDoS) on DNS provider Dyn last week managed to disrupt an array of the internet's biggest websites, including Spotify, Twitter, and PayPal. What was most interesting about this attack was that it was largely carried out using an Internet of Things (IoT) botnet called Mirai[.] . . . Mirai works by exploiting the weak security on many IoT devices. It operates by continuously scanning for IoT devices that are accessible over the internet and are protected by factory default or hardcoded user names and passwords.").

[5] Menn et al., *supra* note 3.

[6] *Id.*

[7] *Id.*

[8] *Id.*

[9] *See* Press Release, Michael F. Nozzolio, What Can Be Done to Prevent Cyber Attacks in the Future? (July 28, 2015), https://www.nysenate.gov/newsroom/press-releases/michael-f-nozzolio/what-can-be-done-prevent-cyber-attacks-future. *See also* Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARV. J.L. & TECH. 429, 465, 467–69 (2012) ("Some argue that more stringent criminal laws and more vigorous enforcement of such criminal laws will deter cyberattacks. However, such an approach generally requires specific knowledge of the adversary's identity, which is difficult in the context of cyberattacks. . . . Having a comprehensive legal structure to address cybercrime requires many elements, including laws specifying prohibited conduct and penalties for such conduct, law enforcement with sufficient authority to collect the necessary electronic evidence, and laws addressing complicated international jurisdictional issues. . . . Because it is difficult to criminalize cyberattacks and to enforce existing criminal laws, some commentators have proposed using civil law instead. Resorting to the civil legal system would enable victims to hold parties liable for behavior that leads to harm. Liability may be imposed on either the attacker or intermediary parties.").

[10] *See* UNITED STATES DEPARTMENT OF DEFENSE, THE DOD CYBER STRATEGY 3 (Apr. 2015), https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf; Erik M. Mudrinich, *Cyber 3.0: The Department of Defense Strategy for Operating in Cyberspace and the Attribution Problem*, 68 A.F. L. REV. 167, 185 (2012). *See generally* Ariana L. Johnson, Note, *Cybersecurity for Financial Institutions: The Integral Role of Information Sharing in Cyber Attack Mitigation*, 20 N.C. BANKING INST. 277 (2016).

2015 (CSA or the Act)[11] with the hopes of mitigating and preventing cybersecurity attacks like the Dyn DDoS attack.[12]

The CSA is perhaps "the most significant piece of federal cyber-related legislation enacted to date."[13] Absent any changes, the CSA will remain in effect for ten years—until September 30, 2025.[14] The CSA, however, contains some ambiguous language in its text—specifically, the phrases "unauthorized effort," "unauthorized access," "cybersecurity purpose," "cybersecurity threat," "defensive measure," and "cyber threat indicator"—related to the concept of authorization.[15] These ambiguities resemble ambiguities in the Computer Fraud and Abuse Act (CFAA)[16] that are at the center of an existing circuit split of interpretation regarding the CFAA's scope.[17]

Two ambiguous phrases in the CFAA—"without authorization" and "exceeds authorized access"—pose interpretive problems for the judiciary because the concept of "authorization" is not defined in the CFAA.[18] As a result, the conduct prohibited under the CFAA can differ depending on the jurisdiction because various circuit courts have interpreted the term "authorization" differently.[19] Some courts have interpreted "authorization" broadly to encompass violations of "corporate computer use restrictions."[20] Other courts have interpreted "authorization" narrowly to exclude computer misuse and misappropriation.[21] Thus, what exactly is or is not authorized under the CFAA and what constitutes "exceeding authorized access" seems to depend on the jurisdiction.[22]

The CSA uses phrases similar to those in the CFAA—"unauthorized effort" and "unauthorized access"—and also does not define them. Additionally, the CSA contains the phrases "cybersecurity purpose" and

---

[11] Cybersecurity Act of 2015 §§ 101–407, 6 U.S.C. §§ 1501–33 (2015) [hereinafter CSA], http://www.intelligence.senate.gov/sites/default/files/legislation/Cybersecurity-Act-Of-2015.pdf.

[12] *See* David J. Bender, *Congress Passes the Cybersecurity Act of 2015*, NAT'L L. REV. (Dec. 20, 2015), http://www.natlawreview.com/article/congress-passes-cybersecurity-act-2015.

[13] Sullivan & Cromwell LLP, *The Cybersecurity Act of 2015*, at 1 (Dec. 22, 2015), https://www.sullcrom.com/siteFiles/Publications/SC_Publication_The_Cybersecurity_Act_of_2015.pdf.

[14] CSA, *supra* note 11, § 111(a).

[15] *See infra* Part III.A (discussing the ambiguities contained in these phrases).

[16] Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030 (2012).

[17] *See infra* Part II (discussing this circuit split).

[18] *See infra* Part III (discussing these issues).

[19] *See infra* Part II (discussing these interpretations in detail).

[20] Allison D. Burroughs et. al., *When is Hacking a Crime? Potential Revisions to the CFAA*, 58 BOSTON BAR J. 13, 14 (Summer 2014).

[21] *Id.* at 15.

[22] *See infra* Part II.

"cybersecurity threat," both of which the CSA defines broadly. The CSA defines "cybersecurity purpose" as the purpose of protecting information and information systems from cybersecurity threats.[23] The CSA defines a "cybersecurity threat" as anything that "*may* result in an *unauthorized effort* to adversely impact the security, availability, confidentiality, or integrity of [information or information systems.]"[24] "Authorization" under the CSA stems from the broad definitions of "cybersecurity threat" and "cybersecurity purpose," which courts could interpret broadly or narrowly, just as with the CFAA. How courts interpret "authorization" under the CSA is important because this will effectively determine the scope of what entities can do and which liability protections they can claim under the CSA.

This Comment examines the CSA and its ambiguous language, compares this language to relevant portions of the CFAA, and concludes with recommendations for addressing these concerns. Part II of this Comment describes the current circuit split that exists among the federal circuit courts of appeals over the interpretation of "without authorization" and "exceeds authorized access" under the CFAA,[25] and the problems that this split causes. Part III of this Comment describes Title I, a major part of the CSA, and its ambiguous language that mirrors similar language in the CFAA, which, if not amended, could lead to a future circuit split of interpretation. Part IV of this Comment argues that Congress should amend the CSA to clarify its legislative ambiguities surrounding the concept of "authorization" that resemble the troubling phrases in the CFAA, to avoid a future circuit split of interpretation. Absent any amendments, however, this Comment contends that courts should interpret the ambiguous language in the CSA narrowly, following the courts on the narrow interpretation side of the CFAA circuit split. Part V of this Comment examines a few state-enacted cybersecurity laws addressing authorization and uses the language of those statutes to suggest how Congress could amend the CSA's language. Ultimately, this Comment argues that Congress should reexamine the CSA and work on amending its ambiguous phrases by clarifying their meaning and application, specifically with regard to "authorization" under the Act so that it can clarify the CSA's scope and reach of its liability protections, as well as prevent a future circuit split of interpretation.

---

23 CSA, *supra* note 11, § 102(4).

24 CSA, *supra* note 11, § 102(5)(A) (emphasis added).

25 *See infra* Part II.

II. THE EXISTING CIRCUIT SPLIT OVER INTERPRETING THE CONCEPT OF "AUTHORIZATION" IN THE CFAA

Congress originally enacted the CFAA to address increasing computer crime and fraud.[26] The CFAA creates both civil and criminal liability for its perpetrators.[27] CFAA violations "require an unauthorized access—either an 'access without authorization' or an act that 'exceed[s] authorized access.'"[28] Section 1030(a)(2) prohibits a person who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains (A) information contained in a financial record of a financial institution, or of a card issuer[;] . . . (B) information from any department or agency of the United States; or (C) information from any protected computer[.]"[29] Section 1030(a)(4) prohibits a person who "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value[.]"[30] At first glance, these two phrases—"without authorization" and "exceeds authorized access"—seem simple and straightforward, but they prove "surprisingly hard" to apply to specific cases.[31] Circuit courts have interpreted these phrases differently, creating disagreement about the scope of "authorization" under the CFAA.

---

[26] *See Statutory Interpretation—Computer Fraud and Abuse Act—Ninth Circuit Holds That Employees' Unauthorized Use of Accessible Information Did Not Violate the CFAA.—United States v. Nosal, 676 F.3d 854 (9th Cir. 2012) (En Banc)*, 126 HARV. L. REV. 1454, 1454 (2013) (stating that Congress passed the CFAA in 1986 "to address the growing problem of intentional trespass into others' computer files, known as 'hacking'"); Shawn E. Tuma, *"What Does CFAA Mean and Why Should I Care?"—A Primer on the Computer Fraud and Abuse Act for Civil Litigators*, 63 S.C. L. REV. 141, 155–56 (2011) (internal citations omitted) (stating the CFAA's original purpose was to address increasing hacking and computer crime directed at government computers, but that "its use has certainly expanded beyond that, both by Congressional expansion of the statutory language and through application by the courts"—initially it was just a federal criminal statute, but courts expanded the CFAA "to permit the recovery of civil damages and injunctive relief for certain of its violations").

[27] *See* 18 U.S.C. § 1030(a), (g) (2012); Michael M. Ratoza, *Ninth Circuit Expands Criminal Liability Under Computer Fraud and Abuse Act*, BULLIVANT HOUSER BAILEY PC (May 2011), http://www.bullivant.com/Computer-Fraud-Abuse-Act.

[28] Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1561–62 (2010). *See also* UNITED STATES DEPARTMENT OF JUSTICE OFFICE OF LEGAL EDUCATION, PROSECUTING COMPUTER CRIMES 5–12 (Scott Eltringham ed., 2015), https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf (describing how various courts have interpreted the phrases "without authorization" and "exceeds authorized access," which have been at issue in a number of cases).

[29] 18 U.S.C. § 1030(a)(2).

[30] *Id.* § 1030(a)(4).

[31] *See* Orin S. Kerr, *Norms of Computer Trespass*, 116 COLUM. L. REV. 1143, 1154 (2016).

Some distinction, but not much of a difference, exists between these two phrases.[32] The phrase "without authorization" is not defined in the CFAA, but "exceeds authorized access" is defined as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter[.]"[33] What do these phrases mean exactly? These phrases could mean people who access a computer they are not allowed to access (i.e., outside hackers) or they could mean people who access a computer they are allowed to access, but then access information on that computer that they are not allowed to access (i.e., inside hackers). They could also mean something else.

A. *The Broad Interpretation of "Authorization" in the CFAA*

On one side of the circuit split, the United States Courts of Appeals for the First,[34] Fifth,[35] Seventh,[36] and Eleventh[37] Circuits have interpreted "exceeds authorized access" broadly[38] to include violating the "intended use" of the authorized access,[39] violating business computer use policy restrictions,[40] violating a duty of loyalty imposed under agency law,[41] and violating an employer's confidentiality agreement.[42]

In *EF Cultural Travel BV v. Explorica, Inc.*,[43] the First Circuit found that a former travel agency employee exceeded authorized access under the CFAA when he retained a consultant to design a computer program called a "scraper"[44] to gather and analyze pricing information from his former

---

[32] *See* Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420 (7th Cir. 2006) (internal citation omitted) ("The difference between 'without authorization' and 'exceeding authorized access' is paper thin, . . . but not quite invisible.").

[33] 18 U.S.C. § 1030(e)(6). *See also* DEPARTMENT OF JUSTICE, *supra* note 28 (discussing the meaning of the phrases "without authorization" and "exceeding authorized access" by citing to cases that have interpreted these phrases).

[34] EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577 (1st Cir. 2001).

[35] United States v. John, 597 F.3d 263 (5th Cir. 2010).

[36] *Citrin*, 440 F.3d 418.

[37] United States v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010).

[38] *See* Stephanie Greene & Christine Neylon O'Brien, *Exceeding Authorized Access in the Workplace: Prosecuting Disloyal Conduct Under the Computer Fraud and Abuse Act*, 50 AM. BUS. L.J. 281, 293–99 (2013).

[39] *See John*, 597 F.3d at 271–72.

[40] *See Rodriguez*, 628 F.3d at 1260, 1263.

[41] *Citrin*, 440 F.3d at 420.

[42] *See* EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 583–84 (1st Cir. 2001).

[43] 274 F.3d 577 (1st Cir. 2001).

[44] *Explorica*, 274 F.3d at 579 ("The scraper has been likened to a 'robot,' a tool that is extensively used on the Internet. . . . Like a robot, the scraper sought information through the Internet. Unlike other robots, however, the scraper focused solely on [defendant's] website, using information that other robots would not have. Specifically, [defendant] utilized tour codes whose significance was not readily understandable to the public. With the tour codes, the scraper accessed [defendant's] website repeatedly and easily obtained pricing information

employer's public website, which he then used to gain a pricing advantage over his former employer.[45] More specifically, although the former employee was authorized to use the employer's website, he exceeded this authorization by using his inside knowledge and information to obtain information, in an attempt to undercut his former employer, that the general public could not access.[46]

The *Explorica* court noted that prior to leaving his employer to start a competing travel agency business, the employee voluntarily entered a confidentiality agreement with his employer that prohibited him from disclosing any information that could reasonably be construed as contrary to his employer's interests.[47] The court found that this employment agreement could determine the boundaries of "authorized" access and held that the employee exceeded authorized access because he obtained confidential information—i.e., inside knowledge about pricing and tour codes—as an employee and then used that information for an illicit purpose in violation of the employment agreement.[48] The court thus affirmed the District Court's finding that the employee likely violated the CFAA by exceeding authorization given to him by his employer.[49]

The Seventh Circuit in *International Airport Centers, L.L.C. v. Citrin*[50] took a slightly different approach to "authorization" under the CFAA, holding that an employee's "authorization" terminates when he or she engages in misconduct that violates the "duty of loyalty that agency law imposes on an employee."[51] In other words, when an employee acts adversely to his or her employer's interest, this breach of the duty of loyalty terminates the employer-employee agency relationship, which thus terminates the employee's authorization "because the only basis of his [or her] authority had been that [agency] relationship."[52]

The Fifth Circuit held in *United States v. John*[53] that "exceeds authorized access" under the CFAA means going beyond the "intended use" of a system for which one's access was authorized.[54] In *John*, a Citigroup employee accessed confidential client account information that she was authorized to access, but then provided that information to someone who

for those specific tours.").

45 *Id.* at 579–80, 583–84.

46 *Id.* at 583–84.

47 *Id.* at 582.

48 *Id.* at 581–84.

49 *Id.* at 585.

50 440 F.3d 418 (7th Cir. 2006).

51 *Id.* at 420.

52 *Id.* at 420–21.

53 597 F.3d 263 (5th Cir. 2010).

54 *Id.* at 271–72.

used it to incur fraudulent charges.[55] The employee was obviously authorized to obtain certain confidential information because of where she worked, but she could only use that information for specific purposes, not however she wanted to, and especially not for illegal purposes.[56] Simply put, just because one is authorized to access confidential information does not give one the right to use that information for criminal purposes or for any purpose other than what is permitted.[57] The *John* majority concluded that authorized access under the CFAA can include limitations on use of information taken by persons who are permitted to access a system or a system's data "when the user knows or reasonably should know that he or she is not authorized to access a computer,"[58] and when the information is obtained to further or perpetrate a crime.[59]

The Eleventh Circuit similarly held in *United States v. Rodriguez*[60] that a Social Security Administration employee exceeded authorized access under the CFAA when he used his access to a federal database for non-business purposes, which was against the employer's policy.[61] Specifically, the employee abused his access to obtain personal identifying information of his former girlfriends and other women.[62] Though the information was not used for an illegal purpose (unlike in *John*), the *Rodriguez* court held that the employee exceeded authorized access under the CFAA when he acquired personal information for a non-business purpose, which violated his employer's policy that restricted him to accessing the database for business purposes only.[63]

B. *The Narrow Interpretation of "Authorization" in the CFAA*

On the other side of the split, the United States Courts of Appeals for the Second,[64] Fourth,[65] and Ninth[66] Circuits have adopted a narrower view of "exceeds authorized access," positing that this phrase should be limited to perpetrators who get information they are not allowed to access on a computer that they are otherwise permitted to use.[67] In other words,

55 *Id.* at 269.
56 *Id.* at 272.
57 *See id.*
58 *Id.* at 271.
59 *John*, 597 F.3d at 271.
60 628 F.3d 1258 (11th Cir. 2010).
61 *Id.* at 1263.
62 *Id.* at 1261.
63 *Id.* at 1263.
64 United States v. Valle, 807 F.3d 508 (2d Cir. 2015).
65 WEC Carolina Energy Sols. LLC v. Miller, 687 F.3d 199 (4th Cir. 2012).
66 United States v. Nosal, 676 F.3d 854 (9th Cir. 2012).
67 *See id.* at 863–64.

"'exceeds authorized access' in the CFAA does not extend to violations of use restrictions," but rather applies to violations of access restrictions.[68]

In *WEC Carolina Energy Solutions LLC v. Miller*,[69] the Fourth Circuit held that a person exceeds authorized access under the CFAA when he or she "accesses a computer without permission or obtains or alters information on a computer beyond that which he [or she] is authorized to access."[70] *Miller* involved an employee who downloaded certain confidential information that he was permitted to access, resigned from the company, and then presented the downloaded information to his former employer's competitor to gain the competitor's business.[71] The *Miller* court held that though the employee may have misappropriated information, he did not exceed authorized access under the CFAA because he did not hack into the employer's system nor did he obtain information that he was not authorized to get.[72] The court seemed to indicate that misappropriating information could be grounds for reprimand and/or termination, but does not constitute a CFAA violation because the CFAA is more concerned with preventing people from getting information they are not permitted to obtain.[73]

In a similar vein, the Second Circuit in *United States v. Valle*[74] held that "exceeds authorized access" means exceeding "the parameters of authorized access" by using a computer that one has permission to use, but entering a part of that computer where he or she is not allowed to go.[75] *Valle* involved a New York City police officer who actively participated in an Internet sex obsession community where he talked with other users about kidnapping, torturing, cooking, and even cannibalizing various women, though he apparently never acted on those elaborate plans.[76] While the officer's acts were undoubtedly disturbing to say the least, the issue was whether he

---

[68] *Id.* at 863.

[69] 687 F.3d 199 (4th Cir. 2012).

[70] *Id.* at 206.

[71] *Id.* at 202.

[72] *See id.* at 206–07.

[73] *See id*. at 207 ("[W]e agree with the district court that although Miller and Kelley may have misappropriated information, they did not access a computer without authorization or exceed their authorized access. . . . Our conclusion here likely will disappoint employers hoping for a means to rein in rogue employees. But we are unwilling to contravene Congress's intent by transforming a statute meant to target hackers into a vehicle for imputing liability to workers who access computers or information in bad faith, or who disregard a use policy. . . . [W]e reject an interpretation of the CFAA that imposes liability on employees who violate a use policy, choosing instead to limit such liability to individuals who access computers without authorization or who obtain or alter information beyond the bounds of their authorized access.").

[74] 807 F.3d 508 (2d Cir. 2015).

[75] *Id.* at 524.

[76] *Id.* at 512.

exceeded authorized access on his work computer to live out his fantasy.[77] The officer admitted he violated his employment terms, but argued that he did not exceed authorized access under the CFAA because he was authorized to obtain the information he accessed in the law enforcement search database.[78] The government, on the other hand, argued the officer *did* exceed authorized access because he obtained information for a non-law enforcement purpose from a database that was dedicated solely to law enforcement purposes.[79]

The *Valle* court reasoned that to hold the officer liable here would expose millions of unsuspecting individuals to potential criminal liability.[80] The *Valle* court first examined the CFAA's text, purpose, and legislative history,[81] and concluded it supported both broad and narrow interpretations of the CFAA.[82] Specifically, the *Valle* majority found that courts could interpret "exceeds authorized access" to mean one of two things: (1) someone who is allowed to access a computer and does so with an inappropriate purpose or to get or modify information; or (2) someone who is allowed to access a computer and does so to get or modify information that he or she is *not* allowed to acquire for any purpose.[83] Because this

---

[77] *Id.* at 511–12.

[78] *Id*. at 523.

[79] *Id.* at 524.

[80] *Valle*, 807 F.3d at 527. *See also* WEC Carolina Energy Sols. LLC v. Miller, 687 F.3d 199, 207 (4th Cir. 2012) ("[W]e are unwilling to contravene Congress's intent by transforming a statute meant to target hackers into a vehicle for imputing liability to workers who access computers or information in bad faith, or who disregard a use policy. . . . Thus, we reject an interpretation of the CFAA that imposes liability on employees who violate a use policy, choosing instead to limit such liability to individuals who access computers without authorization or who obtain or alter information beyond the bounds of their authorized access.").

[81] *See Valle*, 807 F.3d at 525 (internal citations omitted) ("Congress enacted the CFAA in 1984 to address 'computer crime,' which was then principally understood as 'hacking' or trespassing into computer systems or data. . . . The Senate Committee Report to the 1986 amendments specifically described 'exceeds authorized access' in terms of trespassing into computer systems or files. In heightening the *mens rea* requirement for section 1030(a)(2), the Committee explained that it did not want to hold liable those 'who inadvertently "stumble into" someone else's computer file or computer data,' which was 'particularly true in those cases where an individual is authorized to sign onto and use a particular computer, but subsequently exceeds his authorized access by mistakenly entering another computer or data file that happens to be accessible from the same terminal.' . . . Congress was also careful to note that 'section 1030 deals with an "unauthorized access" concept of computer fraud rather than the mere use of a computer. Thus, the conduct prohibited is analogous to that of "breaking and entering."'" . . . Consequently, the legislative history consistently characterizes the evil to be remedied—computer crime—as 'trespass' into computer systems or data, and correspondingly describes 'authorization' in terms of the portion of the computer's data to which one's access rights extend.").

[82] *Id.* at 511–12.

[83] *Id.* at 523–24.

ambiguous language lent itself to both interpretations, the *Valle* majority applied the rule of lenity and adopted the narrower construction in favor of the defendant.[84] In short, the rule of lenity states that where courts can only guess as to an ambiguous criminal law's legislative intent, courts should interpret that law in favor of the defendant.[85] This rule ensures that people will have fair notice of what is a crime.[86]

Most recently, the Ninth Circuit held in *United States v. Nosal*[87] that "exceeding authorized access" does not apply to those who violate use restrictions and does not include computer misappropriation or misuse,[88] but rather is limited to those who violate "restrictions on access to information."[89] *Nosal* involved a former employee who left his executive search firm employer to create a competing business.[90] He persuaded his former coworkers to use their employee computer access to download confidential information from the employer.[91] The issue was whether the former employee, intending to defraud, helped his former coworkers exceed their authorized access in violation of CFAA's section 1030(a)(4).[92] The former employee argued that "exceeds authorized access" applied to hackers

---

[84] *Id.* at 523. *See also* Maracich v. Spears, 133 S. Ct. 2191, 2209 (2013) (internal citations omitted) ("[T]he rule of lenity only applies if, after considering text, structure, history, and purpose, there remains a grievous ambiguity or uncertainty in the statute such that the Court must simply guess as to what Congress intended. . . . Only where 'the language or history of [the statute] is uncertain' after looking to 'the particular statutory language, . . . the design of the statute as a whole and to its object and policy,' does the rule of lenity serve to give further guidance. . . . 'The rule [of lenity] comes into operation at the end of the process of construing what Congress has expressed, not at the beginning as an overriding consideration of being lenient to wrongdoers.'"); United States v. Santos, 553 U.S. 507, 514 (2008) ("The rule of lenity requires ambiguous criminal laws to be interpreted in favor of the defendants subjected to them.").

[85] *See supra* note 84; *Valle*, 807 F.3d at 526–27.

[86] *Valle*, 807 F.3d at 526–27. *See also* United States v. Harriss, 347 U.S. 612, 617 (1954) (stating that a criminal statute violates the constitutional requirement of definiteness when it "fails to give a person of ordinary intelligence fair notice that his contemplated conduct is forbidden by the statute," because people should not be held criminally liable for actions that they "could not reasonably understand to be proscribed"); Connally v. Gen. Constr. Co., 269 U.S. 385, 391 (1926) ("[T]he terms of a penal statute creating a new offense must be sufficiently explicit to inform those who are subject to it what conduct on their part will render them liable to its penalties is a well-recognized requirement, consonant alike with ordinary notions of fair play and the settled rules of law; and a statute which either forbids or requires the doing of an act in terms so vague that men of common intelligence must necessarily guess at its meaning and differ as to its application violates the first essential of due process of law.").

[87] 676 F.3d 854 (9th Cir. 2012).

[88] *Id.* at 863 (following the reasoning of other courts who recognized that the CFAA's plain language did not include computer misuse or misappropriation).

[89] *Id.* at 863–64.

[90] *Id.* at 856.

[91] *Id.*

[92] *Id.*

and not to people who misused information they were allowed to access.[93] The government, however, argued that "exceeds authorized access" included employees who violate restrictions on use of information that they are authorized to access, even if they lack culpable intent.[94] The *Nosal* court declined to adopt the broad interpretation because like the *Valle* court, it reasoned that criminalizing computer misappropriation or misuse[95] would have far-reaching effects on millions of people.[96] The court held that "exceeds authorized access" does not mean violating *use* restrictions, but rather, "is limited to violations of restrictions on *access* to information."[97] The *Nosal* majority noted that the narrower interpretation of "exceeds authorized access" made more sense considering the legislative history and text of the CFAA, which was enacted to "punish hacking—the circumvention of technological access barriers—not misappropriation of trade secrets—a subject Congress has dealt with elsewhere," namely the federal trade secrets statute, 18 U.S.C. § 1832.[98]

C. *The Problems the CFAA Circuit Split Creates*

Inconsistent interpretations of the CFAA are "highly problematic because they can induce noncompliance with congressional intent, displace the common law, abuse federal jurisdiction, and violate the rule of lenity."[99] The current circuit split prevents judges from establishing a congruent body of law regarding the scope of the CFAA as it relates to authorization.[100] Furthermore, the circuit split creates problems for individuals.[101] America

---

93 *Nosal*, 676 F.3d at 856.

94 *Id.* at 857–59.

95 Such misappropriation or misuse could include minor violations like checking Facebook or playing solitaire on one's work computer, which are things that many people do, yet are things the CFAA was not enacted to criminalize. *See Nosal*, 676 F.3d at 859–60 ("While ignorance of the law is no excuse, we can properly be skeptical as to whether Congress, in 1984, meant to criminalize conduct beyond that which is inherently wrongful, such as breaking into a computer. . . . Minds have wandered since the beginning of time and the computer gives employees new ways to procrastinate, by g-chatting with friends, playing games, shopping or watching sports highlights. Such activities are routinely prohibited by many computer-use policies, although employees are seldom disciplined for occasional use of work computers for personal purposes. Nevertheless, under the broad interpretation of the CFAA, such minor dalliances would become federal crimes.").

96 *Nosal*, 676 F.3d at 859, 862. For example, though things like checking Facebook or playing solitaire while at work may be against company policy and could be grounds for reprimand or termination, it does not seem fair to hold a person criminally, or even civilly, liable under the CFAA for such harmless conduct.

97 *Id.* at 864.

98 *Id.* at 863.

99 Myra F. Din, Note, *Breaching and Entering: When Data Scraping Should Be a Federal Computer Hacking Crime*, 81 BROOK. L. REV. 405, 424 (2015).

100 *Id.*

101 *See id.*

was founded on notions of due process and fair notice. Individuals should have notice that what they are doing is a crime and should not have to guess that something may or may not be a crime based on what jurisdiction they are in, given that various jurisdictions could interpret the same law differently.[102] The broad interpretation of authorization in the CFAA does not give fair notice to individuals of potential criminal conduct because it could encompass both serious and benign actions.[103] Thus, the narrower interpretation is the fairer and more logical interpretation.

Discerning the meaning of a particular law is often very challenging.[104] In recent decades, legislation has leaned toward combining both specificity and ambiguity.[105] Courts struggle to determine legislative intent and the meaning of ambiguous language and congressional inaction.[106] Sometimes

---

[102] *See* Theodore J. Boutrous, Jr. & Blaine H. Evanson, *The Enduring and Universal Principle of "Fair Notice"*, 86 S. CAL. L. REV. 193, 194–95 (2013) ("The fair notice requirement is an essential protection of the due process clause, and shields all defendants from unfair and arbitrary punishment. . . . The [Supreme] Court has traditionally analyzed fair notice challenges to criminal statutes under the 'void-for-vagueness' doctrine."); Stacy Nowicki, *No Free Lunch (or Wi-Fi): Michigan's Unconstitutional Computer Crime Statute*, 2009 UCLA J.L. & TECH. 1, 13–14 (2009) ("The void for vagueness doctrine challenges the language of a law as unconstitutional. It originates in the Due Process Clauses of the Fifth and Fourteenth Amendments[.] . . . A statute that does not clearly define forbidden behavior violates due process because it does not give the public notice of what activities are prohibited, and law enforcement can enforce the law in an arbitrary and discriminatory way. The void for vagueness doctrine requires that statutes contain clear, precise language so they 'give the person of ordinary intelligence a reasonable opportunity to know what is prohibited, so that he may act accordingly.'"); Paul H. Robinson, *Fair Notice and Fair Adjudication: Two Kinds of Legality*, 154 U. PA. L. REV. 335, 356 (2005) ("The Due Process Clauses of the Fifth Amendment and the Fourteenth Amendment require a criminal statute to be declared void when it is 'so vague that men of common intelligence must necessarily guess at its meaning and differ as to its application.' This void-for-vagueness doctrine 'forbids wholesale legislative delegation of lawmaking authority to the courts' and 'requires that . . . ordinarily legislative crime definition be meaningfully precise—or at least that it not be meaninglessly indefinite.'") (internal citations omitted).

[103] United States v. Valle, 807 F.3d 508, 527 (2d Cir. 2015); United States v. Nosal, 676 F.3d 854, 859–60 (9th Cir. 2012) ("[Broad] construction of the [CFAA] would expand its scope far beyond computer hacking to criminalize any unauthorized use of information obtained from a computer. This would make criminals of large groups of people who would have little reason to suspect they are committing a federal crime. While ignorance of the law is no excuse, we can properly be skeptical as to whether Congress, [in enacting the CFAA] in 1984, meant to criminalize conduct beyond that which is inherently wrongful, such as breaking into a computer. . . . Significant notice problems arise if we allow criminal liability to turn on the vagaries of private policies that are lengthy, opaque, subject to change and seldom read.").

[104] Robert A. Katzmann, *Making Sense of Congressional Intent: Statutory Interpretation and Welfare Policy*, 104 YALE L.J. 2345, 2360 (1995) (book review).

[105] *Id.* at 2348.

[106] Melissa W. Rawlinson, Note, *United States v. Singleton and the Witness Gratuity Statute: What Is the Best Approach for the Criminal Justice System?*, 14 BYU J. PUB. L. 227, 248 (2000).

legislators intentionally leave language ambiguous to give government officials and judges "the responsibility of adding flesh to the statutory skeleton."[107] Other times ambiguous language exists because that is the price legislators must pay in order to enact the law through compromise.[108] In the case of the CSA, the latter seems more likely. But even still, Congress should amend the CSA to clarify some of the ambiguities surrounding the concept of "authorization" that resemble the troubling phrases in the CFAA. This Comment promotes the narrow interpretation of "authorization" that the Second, Fourth, and Ninth Circuits have taken in the existing CFAA circuit split. Thus, absent a legislative amendment or a Supreme Court ruling to the contrary, courts should follow the Second, Fourth, and Ninth Circuits' lead and similarly interpret "authorization" narrowly as it relates to the CSA. As discussed in Part III.C., contrary holdings could lead to a similar circuit split of interpretation of the CSA and could have serious privacy implications.[109]

III. THE CSA

In the nearly three decades that have passed since Congress enacted the CFAA, the world has become exceedingly more dependent on computers and the Internet. President Barack Obama signed the CSA into law on December 18, 2015.[110] The CSA was part of a $1.1 trillion omnibus

[107] Katzmann, *supra* note 104, at 2348. *See also* Joseph A. Grundfest & A.C. Pritchard, *Statutes with Multiple Personality Disorders: The Value of Ambiguity in Statutory Design and Interpretation*, 54 STAN. L. REV. 627, 640 (2002) ("There are several entirely innocent and socially responsible rationales for certain forms of legislative ambiguity. At one extreme, Congress might not even recognize that it is creating ambiguity. It might also fail to legislate with precision because it wishes to avoid cluttering the statutory text with excessive detail. Apart from aesthetic concerns, Congress may lack the foresight and expertise needed to specify every last jot and tittle of a rule in the text of the statute, and it could be inefficient for a legislature even to try. Congress could also rationally decide that a legislative scheme will work better if discretion is delegated to the courts to resolve disputes according to flexible standards, even though the resulting flexibility generates foreseeable inconsistency in application. Legislating through [sic] standards may require ambiguity in the legislative language to confer that flexibility. Ambiguity can also arise over time as a consequence of unforeseen technological, economic, or social developments.").

[108] Robert A. Katzmann & Russell R. Wheeler, *Interbranch Communication: A Note on "Article III En Banc,"* 117 YALE L.J. POCKET PART 110, 117 (2007). *See also* Robert A. Katzmann & Stephanie M. Herseth, *An Experiment in Statutory Communication Between Courts and Congress: A Progress Report*, 85 GEO. L.J. 2189, 2197 (1997) ("Ambiguity can be inadvertent or deliberate (perhaps as a means of securing a majority coalition to enact the law)."); Robert A. Katzmann & Russell R. Wheeler, *A Mechanism for "Statutory Housekeeping": Appellate Courts Working with Congress*, 9 J. APP. PRAC. & PROCESS 131, 141 (2007) (stating that courts understand that legislative ambiguities are sometimes "the price of legislative compromise" to ensure a law's enactment).

[109] *See infra* Part III.C.

[110] *See* David M. Herszenhorn, *Congress Passes $1.8 Trillion Spending Measure*, N.Y. TIMES, Dec. 18, 2015, at A1, https://www.nytimes.com/2015/12/19/us/congress-spending-bill.html.

spending bill.[111] It consists of parts of three previously introduced bills:[112] one passed by the Senate—the Cybersecurity Information Sharing Act of 2015[113]—and two passed by the House—the Protecting Cyber Networks Act[114] and the National Cybersecurity Protection Advancement Act of 2015[115] The CSA was enacted in part to help facilitate the voluntary sharing of cybersecurity-related information between and among public and private entities without fear of reprisal.[116] A key part of the CSA is Title I, the

[111] Mike DeBonis & Kelsey Snell, *Here's what made it into Congress's big spending and tax Bills*, WASH. POST (Dec. 16, 2015), https://www.washingtonpost.com/news/powerpost/wp/2015/12/16/heres-what-made-it-into-congresss-big-tax-and-spending-bills/.

[112] Jasper Tran, *Cyberwars: Navigating Responsibilities for the Public and Private Sector: Navigating the Cybersecurity Act of 2015*, 19 CHAP. L. REV. 483, 483 (2016); Matthew Gardner & Moshe Broder, *CISA: Hope for More Cybersecurity, Challenges in Implementation and Interpretation*, PROCUREMENT LAWYER, Spring 2016, at 19, 20, http://www.wileyrein.com/media/publication/213_CISA-Hope-for-More-Cybersecurity-Challenges-in-Implementation-and-Interpretation.pdf ("[I]n 2015, the Senate and the House of Representatives advanced three versions of the bill, before a final combined version was inserted in late-December 2015 into the Cybersecurity Act of 2015."); Press Release, Jack Langer, U.S. House of Representatives, Key Intel Bills Added to Omnibus Legislation (Dec. 16, 2015), http://intelligence.house.gov/news/documentsingle.aspx?DocumentID=461 ("The Cybersecurity Act of 2015 is similar to the Protecting Cyber Networks Act (H.R. 1560), which passed the House on April 22 by a vote of 307-116. It also resembles the National Cybersecurity Protection Advancement Act of 2015, which passed the House by a vote of 355-63, and the Cybersecurity Information Sharing Act of 2015, which passed the Senate by a vote of 74-21.").

[113] Cybersecurity Information Sharing Act of 2015, S. 754, 114th Cong. (2015), https://www.congress.gov/bill/114th-congress/senate-bill/754/text.

[114] Protecting Cyber Networks Act, H.R. 1560, 114th Cong. (2015), https://www.congress.gov/bill/114th-congress/house-bill/1560/text.

[115] National Cybersecurity Protection Advancement Act of 2015, H.R. 1731, 114th Cong. (2015), https://www.congress.gov/bill/114th-congress/house-bill/1731.

[116] *See* Joel DeJesus, *New Grid Security Measures for 2016*, PUB. UTIL. FORTNIGHTLY, Feb. 2016, at 40, 41–42 (stating the Cybersecurity Act of 2015 "paves the way for more robust public and private monitoring and protection of information systems" and noting that the Act's "liability limits will ensure industries can take these steps to protect their information systems with limited risk of litigation"); Cadwalader, Wickersham & Taft LLP, *President Obama Signs Cybersecurity Act of 2015 to Encourage Cybersecurity Information Sharing* (Dec. 24, 2015), http://www.cadwalader.com/resources/clients-friends-memos/president-obama-signs-cybersecurity-act-of-2015-to-encourage-cybersecurity-information-sharing ("[The CSA] provides certain assurances to entities in the private sector to encourage such sharing [of 'cyber threat indicators and defensive measures with the federal government']. In addition to the protection against public disclosure and the limitations on the federal government's use of shared information, the Act's principal incentive to encourage information sharing is liability protection for private entities that share information in accordance with the Act."); United States House of Representatives, *Joint Explanatory Statement to Accompany the Cybersecurity Act of 2015*, at 1 (2015), http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/jes%20for%20cybersecurity%20act%20of%202015.pdf (stating the Cybersecurity Act of 2015 "is designed to create a voluntary cybersecurity information sharing process that will encourage public and private sector entities to share cyber threat information, without legal barriers and the threat of unfounded

Cybersecurity Information Sharing Act of 2015.[117] Title I has three primary provisions.[118] The first main provision authorizes private entities to monitor,[119] for cybersecurity purposes,[120] their information systems and data on those information systems (and others' information systems if the private entities get authorization and written consent).[121] Title I's second main provision authorizes private entities to implement "defensive measures"[122] to protect their rights and property.[123] Title I's third main provision offers liability protections (including protections against antitrust laws) for private entities who voluntarily share and receive "cyber threat indicator"[124] information with both public and private entities, provided they comply with the CSA's requirements. Such compliance includes removing a certain individual's personal information or "information that identifies a specific individual" before sharing it.[125] Title I thus permits private entities to

litigation—while protecting private information.").

117 CSA, *supra* note 11, §§ 101–11. *See also* Brad S. Karp, *Federal Guidance on the Cybersecurity Information Sharing Act of 2015*, HARV. L. SCH. FORUM ON CORP. GOVERNANCE & FIN. REGULATION (Mar. 3, 2016), https://corpgov.law.harvard.edu/2016/03/03/federal-guidance-on-the-cybersecurity-information-sharing-act-of-2015/; Latham & Watkins LLP, *What You Need to Know About the Cybersecurity Act of 2015* (Feb. 18, 2016), https://www.lw.com/thoughtLeadership/lw-Cybersecurity-Act-of-2015 (describing and summarizing the key provisions of the CSA); Cadwalader, Wickersham & Taft LLP, *supra* note 116 (summarizing the key provisions of the CSA).

118 Karp, *supra* note 117.

119 *See* CSA, *supra* note 11, § 102(13) (defining "monitor" as "to acquire, identify, or scan, or to possess, information that is stored on, processed by, or transiting an information system").

120 *See id.* § 102(4)–(5) (defining "cybersecurity purpose" as "the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability"; and defining "cybersecurity threat" as "an action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system.").

121 *Id.* § 104(a)(1).

122 *See id.* § 102(7) (defining "defensive measure" as "an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability," but explicitly "does not include a measure that destroys, renders unusable, provides unauthorized access to, or substantially harms an information system or information stored on, processed by, or transiting such information system not owned by (i) the private entity operating the measure; or (ii) another entity or Federal entity that is authorized to provide consent and has provided consent to that private entity for operation of such measure.").

123 *Id.* § 104(b)(1).

124 *See id.* § 102(6) (defining "cyber threat indicator").

125 CSA, *supra* note 11, § 106; John P. Carlin, *Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats*, 7 HARV. NAT'L SEC. J. 391, 434 (2016) (citing 6 U.S.C. § 1503(d)(2) (2015)). *See also U.S. Enacts Cybersecurity Information*

monitor networks, operate "defensive measures" on networks, and share and receive "cyber threat indicators"—all for "cybersecurity purposes," i.e., to protect information systems against cybersecurity attacks.[126]

The CSA, though, is not without its flaws. Its language contains much ambiguity and uncertainty.[127] As scholar Orin Kerr put it, the CSA's text describing what companies can monitor reflects the same struggles and problems that Congress had in enacting the CFAA—how does one describe unauthorized conduct that a cybersecurity law can target for surveillance?[128] Whereas the CFAA contains the phrases "without authorization" and "exceeds authorized access," the CSA contains the phrases "unauthorized effort" and "unauthorized access."[129] The CSA does not define these critical phrases that focus on the concept of "authorization," the same word the CFAA focuses on.[130] Because the CSA embodies legislative ambiguities similar to those present in the CFAA, this Comment suggests that Congress should amend the CSA to define these ambiguous phrases and/or include

Sharing Legislation, CSX SPECIAL REPORT (ISACA, Rolling Meadows, Ill.) Jan. 6, 2016, at 1, http://www.isaca.org/cyber/Documents/CSX-Special-Report_misc_Eng_0116.pdf (stating the CSA created a framework for both public and private entities to voluntary share cyber threat information with each other in an effort to defend against cyberattacks, while still protecting "individuals' privacy rights by ensuring that personal information is not unnecessarily divulged").

126 *See* CSA, *supra* note 11, § 104(a)–(c); Kristin N. Johnson, *Managing Cyber Risks*, 50 GA. L. REV. 547, 578–79 (2016). *See also* Tran, *supra* note 112, at 495 (stating the CSA "contains the majority of CISA's provisions, but with three notable exceptions: (1) network operators have monitoring privileges; (2) network operators can operate defensive measures; and (3) network operators can share cyberthreat information with others"); S. REP. No. 114-32, at 5 (2015), https://www.congress.gov/114/crpt/srpt32/CRPT-114srpt32.pdf ("Specifically, private entities are only authorized to monitor their own information systems or those of another private entity upon the authorization and written consent of such other entity. Moreover, such monitoring is limited to cybersecurity purposes. Essentially, these important limitations ensure that private entities are only authorized to monitor their information systems to protect against cybersecurity threats and vulnerabilities. Any other monitoring would require lawful authority other than that provided in this Act."); Gardner & Broder, *supra* note 112, at 20 (noting that Title I of the CSA authorizes private entities to "monitor their (or their customers') information systems for 'cybersecurity purposes,' operate defensive measures for cybersecurity purposes on their (or their customers') networks to protect their 'rights or property,' and voluntarily share and receive certain information" without fear of liability).

127 Orin Kerr, *How Does the Cybersecurity Act of 2015 Change the Internet Surveillance Laws?*, WASH. POST (Dec. 24, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/12/24/how-does-the-cybersecurity-act-of-2015-change-the-internet-surveillance-laws/.

128 *Id. See also* Gardner & Broder, *supra* note 112, at 26 (stating that the CSA allows private entities "the opportunity to reexamine their information and network security procedures and engage in information sharing and defensive measures to better protect information systems from external threats," but that these opportunities also bring "significant challenges in interpreting and applying key provisions of [the Act]").

129 Kerr, *supra* note 127.

130 *Id.*

examples of authorization to clarify the CSA's scope so that courts can uniformly interpret the CSA. Interpretation of "authorization" under the CSA should not be completely left up to individual court interpretation since this could result in various interpretations and in turn lead to a future circuit split similar to the one that currently exists with the CFAA.[131] This could also have serious privacy implications because of the broad power the CSA gives to entities to monitor and surveil computers and information systems, which could lead to potential future constitutional challenges.[132]

A. *Legislative Ambiguities Within the CSA*

The CSA contains ambiguous language that resembles the troublesome language in the CFAA. First, the CSA uses the ambiguous, undefined phrases "unauthorized effort" and "unauthorized access," which are similar to the problematic phrases in the CFAA.[133] "Authorization" is partially explained but not explicitly defined in Section 104 of the CSA,[134] which gives courts the ability to construe "authorization" broadly. How courts interpret "authorization" under the CSA is important because this effectively determines what activities fall within the scope and liability protections of the CSA. Second, the CSA contains the phrases "cybersecurity purpose" and "cybersecurity threat," both of which the CSA defines broadly.[135] The CSA defines "cybersecurity purpose" as the purpose of protecting information and

---

131 *See supra* Part II.

132 Such privacy implications could include allowing the government to collect large amounts of information that can be used for cybersecurity or non-cybersecurity purposes, increasing the National Security Agency's access to personal information, and/or erroneous receipt or distribution of personal information. *See* John Heidenreich, Note, *The Privacy Issues Presented by the Cybersecurity Information Sharing Act*, 91 N.D. L. REV. 395 (2015); Press Release, Open Tech. Inst., 55 Civil Society Groups, Security Experts, and Academics Strongly Oppose Intelligence Committees' Cybersecurity Information Sharing Bills (Apr. 21, 2015), https://www.newamerica.org/oti/press-releases/55-civil-society-groups-security-experts-and-academics-strongly-oppose-intelligence-committees-cybersecurity-information-sharing-bills/. *See also* Al Franken, Senator, Remarks of Sen. Al Franken on the Cybersecurity and Information Sharing Act of 2015 (Oct. 22, 2015), https://www.franken.senate.gov/?p=news&id=3269 ("The term 'cybersecurity threat' is really the lynchpin of the [CSA]: companies can monitor systems, share cyber threat indicators with one another or with the government, and deploy defensive measures to protect against any cybersecurity threats. . . . Under [its broad] definition, companies can take action even if it's unreasonable to think that security might be compromised. This raises serious concerns about the scope of all of the authorities granted by the bill and the privacy implications of those authorities. And security experts and advocates have warned that, in this context, establishing the broadest possible definition of 'cybersecurity threat' actually threatens to undermine security by increasing the amount of unreliable information shared with the government."). A detailed examination of such privacy implications is beyond the scope of this Comment.

133 *See* Kerr, *supra* note 127.

134 *See* CSA, *supra* note 11, § 104.

135 *Id.* § 102(4)–(5).

information systems from "cybersecurity threat[s]."[136] The CSA defines a "cybersecurity threat" as anything that "*may* result in an *unauthorized effort* to adversely impact the security, availability, confidentiality, or integrity of [information or information systems.]"[137] Thus, what constitutes a "cybersecurity purpose" hinges on how broadly courts construe "cybersecurity threat," which depends on how courts interpret "unauthorized effort." This could be very broad given that the CSA does not define "unauthorized effort." To limit the scope of authorization under the CSA, Congress should amend the CSA to define "unauthorized effort" or give examples of what constitutes an "unauthorized effort." Third, and lastly, the CSA contains the phrases "defensive measure" and "cyber threat indicator," both of which the CSA defines.[138] The legislative history reveals that Congress intended for these last two phrases to be narrowly construed, but their plain language definitions give courts the potential to construe them broadly.[139]

The CSA defines a "defensive measure" as "an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability."[140] The CSA, however, explicitly excludes the following from the definition of "defensive measures": measures that destroy, render unusable, provide *unauthorized access* to, or substantially harm "an information system or information stored on, processed by, or transiting such information system not owned by (i) the private entity operating the measure; or (ii) another entity . . . that is authorized to provide consent and has provided consent to that private entity for operation of such measure."[141] The legislative history behind this definition indicates that Congress intended "defensive measure" to be narrowly construed.[142] Legislators gave examples of how simple or complex a "defensive measure" could be, stating that it could be a simple security mechanism that restricts access to an entity's computer infrastructure or it could be a "sophisticated software tool[] to detect and protect against anomalous and unauthorized activities on a private entity's information system."[143] The legislative history also reveals that Congress intended for

136 *Id.* § 102(4).
137 CSA, *supra* note 11, § 102(5) (emphasis added).
138 *Id.* § 102(6)–(7).
139 *See* S. REP. NO. 114-32, *supra* note 126, at 4–5.
140 CSA, *supra* note 11, § 102(7)(A).
141 *Id.* § 102(7)(B) (emphasis added).
142 S. REP. NO. 114-32, *supra* note 126, at 5.
143 *Id.*

authorization to extend to "defensive measures" "that do not cause substantial harm to another entity's information systems or data on such systems, regardless of whether such non-substantial harm was intended or foreseen by the implementing entity."[144] This seems to imply that authorization to operate a "defensive measure" would be valid so long as it does not substantially harm another entity's system or system data and does not involve an offensive action such as hacking back into another entity's system. But since an entity can operate a "defensive measure" to detect, prevent, or mitigate "a known or suspected cybersecurity threat," and since "cybersecurity threat" is broadly defined, this could lead to "defensive measure" being broadly construed. Additionally, it is unclear whether authorization would extend to a "defensive measure" that harms, but does not *substantially* harm, another entity's system or system data.[145] It also remains uncertain what constitutes "substantial harm" and who decides whether something constitutes a "substantial harm."[146] These are some of the many questions the CSA leaves unanswered.

Relatedly, "cyber threat indicator" is an important phrase in the CSA because the CSA authorizes both public and private entities to share and receive information regarding "cyber threat indicators" with each other.[147] The CSA defines "cyber threat indicator" as:

> information that is necessary to describe or identify—(A) malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability; (B) a method of defeating a security control or exploitation of a security vulnerability; (C) a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability; (D) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability; (E) malicious cyber command and control; (F) the actual or potential harm caused by an incident, including a description of the information

144 *Id.*

145 *See* Gardner & Broder, *supra* note 112, at 23.

146 *See id.* (asking "what does it mean for a defensive measure to '*substantially* harm' information or an information system? Is there some lesser harm that would be permissible, and who would determine what qualifies as a less-than-substantial harm? Would the key distinction be whether the defensive measure executes some code on another system, or could a more 'passive' defense, such as blocking access from that system, also constitute 'substantial harm'?") (emphasis in original).

147 *See* S. REP. NO. 114-32, *supra* note 126, at 4 ("The term 'cyber threat indicator' is one of the most important definitions in [the CSA].").

> exfiltrated as a result of a particular cybersecurity threat; (G) any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or (H) any combination thereof.[148]

If something does not fall under one of these enumerated categories, then it is not a "cyber threat indicator" for purposes of the CSA. If something is a "cyber threat indicator," however, then private entities can use it to monitor networks, operate "defensive measures," or share and receive "cyber threat indicators" with the federal government[149]—provided, of course, that they do it in furtherance of a "cybersecurity purpose."[150] As long as they comply with this provision, entities will be protected from liability for sharing "cyber threat indicators" with the federal government or for using "cyber threat indicators" to monitor networks or operate "defensive measures."[151] Again, the situations that permit entities to share and receive "cyber threat indicators" with the government can be construed broadly because they focus on the same problematic phrases aforementioned—namely, "cybersecurity purpose" and "cybersecurity threat." It appears that Congress intended for "cyber threat indicator" to have a limited definition by enumerating what information could be shared between and among public and private entities.[152] But some have opined that "cyber threat indicators" could be interpreted very broadly, similar to the phrases "cybersecurity threat" and "defensive measure."[153]

---

148 CSA, *supra* note 11, § 102(6).

149 The CSA permits entities to share and receive "cyber threat indicators" and "defensive measures" for a "cybersecurity purpose." *Id.* § 104(c).

150 *Id.* § 104(d)(3)(a).

151 *Id.* § 106(b).

152 *See* S. REP. NO. 114-32, *supra* note 126, at 4 ("This narrow definition is a key privacy protection in the [CSA] because it creates an exhaustive list of the types of cyber threat information that can be shared among private and governmental entities, and only when they are necessary to describe or identify threats to information and information systems. Essentially, this definition limits the information that can be shared under [the CSA] to the techniques and 'malware' used by malicious actors to compromise the computer networks of their victims, not sensitive personal and business information contained in such networks.").

153 *See* Trevor Ford, *Cybersecurity Legislation for an Evolving World*, 50 U.S.F. L. REV. 119, 127 (2016) (citing *Cyber-Surveillance Bill to Move Forward, Secretly*, CTR. FOR DEMOCRACY & TECH. (Mar. 4, 2015), https://cdt.org/insight/cyber-surveillance-bill-to-move-forward-secretly/) ("The [Center for Democracy and Technology] objects to CISA because it argues that the definition of 'cyber threat indicators' (CTIs) is so broad that CISA's authorization for the sharing of threat indicators for any purposes *other* than cybersecurity risks the facilitation of government surveillance."); Heidenreich, *supra* note 132, at 404–05 (stating the definition of "cyber threat indicator" "is too broad to be meaningful," and because the definition is so broad, a private entity could share "nearly any piece of information" with the government).

The legislative history reveals that Congress intended the definition of a "cybersecurity threat" to encompass activities that could have "unauthorized and negative results."[154] A "cybersecurity threat," however, explicitly excludes any actions that solely involve "violation[s] of a consumer term of service or a consumer licensing agreement."[155] This appears to refer to the debate surrounding the CFAA where some circuit courts have concluded that violations of consumer terms of service or consumer licensing agreements constitute "exceed[ing] authorized access" under the CFAA.[156] Congress did not want to have a consumer agreement violation constitute a "cybersecurity threat" under the CSA. "Cybersecurity threat" does, however, include cyberattacks like the Dyn DDoS attack because these could have "unauthorized and negative results" like disrupting service of major websites for millions of people.[157] Additionally, as two scholars point out, a "cybersecurity threat" could also include entities that unsuspectingly become threats—for example, when a botnet or other malware overtakes an entity's systems, as occurred in the Dyn DDoS attack.[158] The CSA does not contemplate what happens if this occurs, and given the broad definition of "cybersecurity threat," public and private entities would presumably be able to monitor and/or operate "defensive measures" against the infected entity in such a situation. This would give broad authorization and liability protection to entities for these actions, but would be unfair to the person whose computer or information system was overtaken by something that he or she had no control over.

---

154 S. REP. NO. 114-32, *supra* note 126, at 4.

155 CSA, *supra* note 11, § 102(5)(B).

156 Gardner & Broder, *supra* note 112, at 22 ("The [CSA] specifically excludes 'any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.' Removing these types of violations from the definition of 'cybersecurity threat' is an apparent nod to the debate surrounding the Computer Fraud and Abuse Act (CFAA)[, which] has caused a 'sharp division' among the circuit courts regarding the appropriate scope and interpretation of the 'exceeds authorized access' provision[.] . . . Some circuits . . . have interpreted the [CFAA] more broadly and upheld convictions for violations of consumer or employee terms of service. Accordingly, by defining 'cybersecurity threat' as excluding the violation of a consumer term of service, the [CSA] does not provide carte blanche to private entities to disclose or monitor information merely because of the relatively common occurrence of a consumer violating terms of service."). *See also* S. REP. NO. 114-32, *supra* note 126, at 4 ("Many terms of service agreements prohibit activities that would also meet the 'cybersecurity threat' definition; such activities would still be considered a 'cybersecurity threat' because they were not 'solely' violations of consumer agreements. The [Select Committee on Intelligence] intends this definition to include activities that may have unauthorized and negative results, but to exclude authorized activities, such as extensive use of bandwidth that may incidentally cause adverse effects. However, this definition clearly does not permit hackers to cloak their criminal actions like theft of information or destruction of property under the ambit of First Amendment protected activities.").

157 S. REP. NO. 114-32, *supra* note 126, at 4.

158 Gardner & Broder, *supra* note 112, at 21.

The scope of the CSA depends on how courts interpret "authorization" under the CSA through construing the phrases "cybersecurity purpose," "cybersecurity threat," "defensive measure," and "cyber threat indicator." Put simply, the CSA defines a "cybersecurity threat" as anything that *may* harm a network.[159] A lot of things could fall into this broad definition, which would then cause "cybersecurity purpose," "defensive measures," and "cyber threat indicators" to also be broadly interpreted. The concept of "authorization" within the CSA matters because whether entities are protected from liability depends on whether they are complying with the CSA's standards—entities are protected from liability only if they are taking actions prescribed by the CSA for a "cybersecurity purpose," not other, potentially nefarious or non-cybersecurity purposes.[160] Given the broad definition of "cybersecurity purpose" and how broadly courts could construe it, there seems to be little for which entities would be liable. Thus, it is important for Congress to clarify what these terms mean, as well as define "unauthorized effort" and "unauthorized access" so the CSA does not become a broad surveillance law with serious privacy implications.[161]

---

159 *See supra* note 137.

160 CSA, *supra* note 11, § 106(b).

161 Under the CSA, the federal government clearly has more authorization to share and receive "cyber threat indicators" than private entities. *See* CSA, *supra* note 11, §§ 103, 105(d)(5). Some believe that this is unfair and that this makes the CSA seem more like a surveillance bill than a cybersecurity law. *See* Jessica Beyer, *The Cybersecurity Information Sharing Act (CISA)*, HENRY M. JACKSON SCH. INT'L STUD., U. WASH. (Oct. 30, 2015), https://jsis.washington.edu/news/the-cybersecurity-information-sharing-act-cisa/ ("Critics of the CISA are concerned about four major elements of the bill. First, critics are concerned that the definitions included in the bill are overly broad. . . . Second, critics are concerned that the protections for companies are overly vast. . . . Third, critics are concerned about the surveillance permission granted to U.S. security agencies, in general, beyond the purpose of the bill. . . . Fourth, critics are concerned that the bill will not do anything to address present day cybersecurity challenges."). *See also* Russell Brandom, *Congress snuck a surveillance bill into the federal budget last night*, VERGE (Dec. 16, 2015, 10:51 AM), http://www.theverge.com/2015/12/16/10288182/cisa-surveillance-cybersecurity-budget-pro posal ("[The CSA] make[s] it easier for private sector companies to share user information with the government and other companies, removing privacy and liability protections in the name of better cybersecurity. . . . In many ways, the [CSA] . . . is even more invasive than previous versions, stripping out crucial provisions that prevented direct information-sharing with the NSA and mandated that data be anonymized before being widely distributed. 'It's clear now that this bill was never intended to prevent cyber attacks,' said Evan Greer, campaign director of Fight for the Future, which has campaigned vigorously against the bill. 'It's a disingenuous attempt to quietly expand the US government's surveillance programs.'"). As mentioned, however, a detailed look at the CSA's privacy implications is beyond the scope of this Comment.

B. *The Unclear Scope of "Authorization" Under the CSA*

Key phrases in the CSA are "unauthorized effort" and "unauthorized access," neither of which are defined in the CSA, and both of which sound very similar to the phrases "without authorization" and "exceeds authorized access" in the CFAA. What constitutes an "unauthorized effort" or "unauthorized access"? Do these phrases mean the same as "without authorization" or "exceeds authorized access"? As the CSA is currently written, it is unclear.

Section 104 of the CSA partially explains "authorization." Notwithstanding any other law, section 104 authorizes private entities—for "cybersecurity purpose[s]" only—to monitor information systems; operate defensive measures on their own information systems, as well as other private or government entities' information systems provided they have the others' authorization and written consent; and share or receive "cyber threat indicators" or "defensive measures."[162] Section 104 explicitly states that "[n]othing in this subsection shall be construed to authorize the monitoring of an information system [or "authorize the use of a defensive measure"] . . . other than as provided in this subsection[] or to limit otherwise lawful activity."[163]

The legislative history reveals that Congress intended "authorization" in the CSA to refer to actions undertaken for "cybersecurity purpose[s]" only.[164] Interestingly, the legislative history also reveals that Congress stated the authorization for entities to take "defensive measures" "does not include activities that are generally considered 'offensive' in nature, such as unauthorized access of, or execution of computer code on, another entity's information systems, . . . or any actions that would substantially harm another private entity's information systems, such as violations of [the CFAA]."[165] But there are two problems with this partial explanation of "authorization" for the CSA. First, this guidance addresses only "defensive measures," not monitoring or sharing information, all of which entities can do, provided it is for a "cybersecurity purpose," which is itself a broad term, as explained above. Second, this guidance does not define "unauthorized access," but instead references CFAA violations as examples of actions that would not be authorized by the CSA. Given the current split of interpretation on what constitutes a CFAA violation with regard to unauthorized actions, however, this gives minimal (if any) guidance as to the scope of "authorization" under the CSA. Thus, the CSA's legislative history does not

162 CSA, *supra* note 11, § 104(a)–(c).

163 *Id.* § 104(a)(2), (b)(2).

164 161 CONG. REC. S8848 (2015), https://www.gpo.gov/fdsys/pkg/CREC-2015-12-18/pdf/CREC-2015-12-18-pt1-PgS8844.pdf.

165 *Id.*

elucidate Congress's intent as to the scope of "authorization" under the Act. In other words, anything that could result in an "unauthorized effort" would constitute a "cybersecurity threat." This would, in turn, constitute a "cybersecurity purpose," which would permit entities to take action—i.e., monitor networks, operate "defensive measures," or share and receive "cyber threat indicators" with the government—pursuant to the CSA and without fear of reprisal.[166] This will inevitably occur because of the broad definitions of these ambiguous phrases and the lack of clarification as to the scope of "authorization" under the CSA.

How courts interpret "cybersecurity purpose" is important because this will determine the scope of "authorization" under the CSA, i.e., the limits on how entities can monitor information systems, operate defensive measures, and share and receive "cyber threat indicators."[167] Depending on how broadly courts interpret "unauthorized effort" and "unauthorized access," courts could also broadly interpret "cybersecurity purpose," "cybersecurity threat," "defensive measures," and "cyber threat indicator."[168] If courts broadly interpret these troublesome phrases, this could have serious privacy implications for what entities are legally permitted to do under the CSA, particularly because as long as the private entity can show its actions were for a "cybersecurity purpose," it can take advantage of the liability protections the CSA affords.[169]

Senator Ron Wyden opined that the definition of "cybersecurity threat" in the CSA is too broad and will incentivize sharing information even when the information is not affiliated with (or even unlikely to relate to) an actual cybersecurity threat.[170] He suggests that Congress should have a more

166 CSA, *supra* note 11, § 106.

167 *See* S. REP. NO. 114-32, *supra* note 126, at 3.

168 Gardner & Broder, *supra* note 112, at 26 (citing CSA, *supra* note 11, § 105(d)(5)(A)(i)).

169 *See* Johnson, *supra* note 126, at 580–81 (citing John D. McKinnon, *Congress Poised to Pass Cybersecurity Measure*, WALL ST. J. (Dec. 16, 2015, 5:48 PM), http://www.wsj.com/articles/congress-poised-to-pass-cybersecurity-measure-1450284622) ("Critics of the Cybersecurity Information Sharing Act contend that the statute grants broad powers of surveillance and fails to incorporate appropriate privacy protections. Market participants express concern regarding the government's ability to safeguard proprietary and confidential information. Government warehousing of shared data is only as safe as the government's capacity to prevent cyber intrusions. After recent cyberattacks breaching government agency defenses, many express concerns that shared information may be more vulnerable in the hands of government agencies.").

170 S. REP. NO. 114-32, *supra* note 126, at 21 (Senator Ron Wyden stated "I opposed this bill because I believe its insufficient privacy protections will lead to large amounts of personal information being shared with the government even when that information is not needed for cybersecurity. This could include email content, financial records, and a wide variety of other personal information. . . . This excessively broad collection may not be the intent of this bill, but the language is clearly drafted broadly enough to permit it. Most notably, the bill defines a cybersecurity threat as anything that 'may result' in harm to a network. This broad definition

narrowly focused definition of a "cybersecurity threat"—limited to actions that are "reasonably likely" to affect or harm a network—to ensure that information-sharing is tailored to actual threats.[171] Senator Wyden stated that the CSA's language as a whole permits an "excessively broad" collection of information.[172] Thus, he opposed the CSA because he said the bill does very little to secure America's networks, yet significantly increases the government's collection of people's personal and private information.[173] This Comment similarly argues that Congress should amend the CSA to not only clarify and tailor the definition and/or scope of "cybersecurity threat," but also to define the ambiguous phrases "unauthorized effort" and "unauthorized access" on which the scope of "cybersecurity threat" relies.[174]

C. *Congress Should Amend the CSA, but Absent Any Amendments, Courts Should Follow the Narrow Interpretation of "Authorization" Used by the Second, Fourth, and Ninth Circuit Courts*

As noted above, Congress should amend the CSA to clarify its ambiguous language. Absent any amendments, however, courts should follow the Second, Fourth, and Ninth Circuits' lead and interpret "authorization" in the CSA narrowly. As previously stated, "cybersecurity purpose" and "cybersecurity threat" both have broad definitions, which form the basis of authorization for what entities are permitted to do under the CSA. Entities receive liability protections under the CSA so long as they are undertaking actions for a "cybersecurity purpose," which is meant to protect against cybersecurity threats or anything that could harm an information system.[175] This broad definition can include conduct that does not actually lead to any harm, as well as actions that are maliciously or unknowingly harmful (such as a botnet attack that overtakes someone else's computer and then uses that computer to harm others).

Scholar Orin Kerr argues that courts should not adopt "contract-based notions of authorization," but rather should limit statutes involving unauthorized access to cases that involve the "circumvention of code-based restrictions."[176] Analogous to the narrower interpretation side of the CFAA

will incentivize the sharing of information even when it is unlikely to pertain to an actual cybersecurity threat. A more tailored definition, limited to actions that are *reasonably likely* to harm or interfere with a network, would ensure that information-sharing is more narrowly focused on actual threats.").

171 *Id.*

172 *Id.*

173 *Id.* at 22.

174 CSA, *supra* note 11, §§ 102(5), 203.

175 *See id.* § 102(4)–(5).

176 Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in*

circuit split, Kerr states that simply violating a contractual restriction on computer use should not constitute unauthorized access.[177] Kerr contends that bypassing code-based restrictions, such as password protections, should be required to trigger criminal liability, "such that hacking into a computer could be an unauthorized access, but violating Terms of Service would not be."[178]

This Comment similarly argues that courts should not interpret "authorization" in the CSA to mean violating restrictions on *use* of information,[179] but rather should be limited to violating restrictions on *access* to information.[180] The legislative history of the CSA implies that it was not necessarily enacted to prevent restrictions on use, but rather was enacted to prevent actions "including cyber attacks, theft, and data breaches."[181] As noted above, the CSA permits entities to monitor networks, operate "defensive measures," and share and receive "cyber threat indicators" as long as these actions are taken for a "cybersecurity purpose." This is to protect information or information systems from a "cybersecurity threat," which is anything that may result in an "unauthorized effort."[182] A broad interpretation of "authorization" under the CSA would lead to broad interpretations of "cybersecurity purpose," "cybersecurity threat," "defensive measure," and "cyber threat indicator." The scope of "defensive measure" and "cyber threat indicator" depends on how broadly courts interpret "cybersecurity purpose." This depends on how broadly courts interpret "cybersecurity threat," which rests on how courts interpret "unauthorized effort." If courts construe "authorization" under the CSA broadly, then violations of use restrictions or misappropriation of information would constitute "unauthorized efforts." These violations would thus constitute "cybersecurity threats" for which entities could monitor their networks, operate "defensive measures," or share or receive "cyber threat indicators." This expansive interpretation contradicts Congress's intent for the CSA to promote voluntary sharing of information to prevent things like "cyber attacks, theft, and data breaches."[183] Therefore, courts should instead interpret the concept of authorization under the CSA narrowly, following the Second, Fourth, and Ninth Circuits on that side of the CFAA circuit split. They should interpret "unauthorized effort" as a

Computer Misuse Statutes, 78 N.Y.U. L. REV. 1596, 1600 (2003).

177 *Id.*

178 *Id.*

179 United States v. Nosal, 676 F.3d 854, 863 (9th Cir. 2012).

180 *See id.*

181 S. REP. No. 114-32, *supra* note 126, at 15.

182 *See supra* Part III.B.

183 *See* S. REP. No. 114-32, *supra* note 126, at 15; House of Representatives, *supra* note 116.

violation of a restriction against access to information, i.e., accessing or attempting to access information one does not have permission to obtain on a device that one is otherwise permitted to use. Otherwise, this could create potential liability for millions of people who might unknowingly become a "cybersecurity threat" or "cyber threat indicator."

The scope of CSA provisions containing the following phrases—"cybersecurity purpose," "cybersecurity threat," "defensive measure," and "cyber threat indicator"—depends on how courts interpret "unauthorized" or "authorization." Recall that a cybersecurity threat is anything that *may* result in an unauthorized effort to harm information or information systems.[184] The concept of "authorization" underlying the CSA's ambiguous phrases "cybersecurity purpose" and "cybersecurity threat" could be interpreted both broadly (based on the broad definitions of those phrases) and narrowly (if courts so choose in their discretion). This Comment argues that if Congress does not amend the CSA, courts construing its ambiguous language will inevitably arrive at different interpretations, which could result in a circuit split similar to the one that exists with the CFAA. This would also cause entities attempting to address cybersecurity threats to dissimilarly use and apply the CSA. Some entities will be allowed to more closely monitor information systems than other entities for things that *may* result in an "unauthorized effort" to harm information or information systems. The potential harm of a non-uniform application of the CSA is that entities in jurisdictions where courts broadly interpret the CSA's ambiguous language will be able to do more monitoring, employ more "defensive measures," or share and receive more "cyber threat indicators" than entities in jurisdictions where courts narrowly interpret the CSA's language—all while being shielded by the CSA's liability protections. This will not only lead to a circuit split similar to the CFAA's, but will also have serious privacy implications and could lead to constitutional challenges in the near future.[185]

IV. THE CSA SHOULD BE AMENDED RATHER THAN REPEALED

Some critics of the CSA would prefer to repeal and replace the CSA rather than amend it, because of the difficulties in amending federal legislation.[186] The United States Constitution sets forth specific procedural requirements for creating binding federal legislation.[187] Under this

184 *See* CSA, *supra* note 11, § 102(4)–(5).

185 *See supra* note 132.

186 *See, e.g.*, Daniel Wilson, *Voices Grow Against 'Hastily' Passed Cybersecurity Law*, LAW360 (Jan. 26, 2016, 2:46 PM), http://www.law360.com/articles/750690/voices-grow-against-hastily-passed-cybersecurity-law; Cory Bennett, *Amash Bill Would Repeal New Cybersecurity Law*, THE HILL (Jan. 14, 2016, 9:08 AM), http://thehill.com/policy/cybersecurity/265852-amash-bill-would-repeal-new-cybersecurity-law.

187 U.S. CONST. art. I, § 7.

framework, a bill becomes law after a majority in both the House and the Senate pass it, and after the President signs it.[188] This process "makes federal legislation exceedingly difficult to enact and to amend."[189] On January 28, 2016, shortly after Congress passed the CSA, Republican House Representative Justin Amash introduced a bill to repeal the CSA,[190] stating it was "the worst anti-privacy law since the USA Patriot Act."[191] Congressman Amash claimed that most representatives likely did not even vote on the CSA because they did not notice it being included as part of such an omnibus bill.[192] Civil liberties advocates, government accountability groups, and tech industry members similarly expressed a strong desire to repeal the CSA, arguing "it was 'hastily' included in a broader government funding bill and deserves open debate."[193] These groups also believe that the CSA likely will not prevent cyberattacks and, rather, will allow for "broad and undefined data collection"[194] in contravention of privacy rights.[195]

188 *Id.* § 7, cl. 2. *See also* Michael D. Shumsky, *Severability, Inseverability, and the Rule of Law*, 41 HARV. J. ON LEGIS. 227, 247 (2004) (describing the "arduous legislative process" in America for how a bill becomes "a legally binding statutory enactment subject only to *substantive* constitutional constraints").

189 Shumsky, *supra* note 188, at 264.

190 *See* To Repeal the Cybersecurity Act of 2015, H.R. 4350, (114th Cong. Jan. 28, 2016), https://www.congress.gov/bill/114th-congress/house-bill/4350/text.

191 Bennett, *supra* note 186.

192 *See id.*

193 Wilson, *supra* note 186; Sam Thielman, *Apple, Google and Twitter among 22 tech companies opposing Cisa bill*, GUARDIAN (Oct. 21, 2015), https://www.theguardian.com/technology/2015/oct/21/apple-google-and-twitter-among-22-tech-companies-opposing-cisa-bill ("Twenty-two of the world's top technology companies are firmly against the controversial Cybersecurity Information Sharing Act . . . [including] Apple, Google, Twitter and Wikipedia[.] . . . [CISA] is aimed at tightening online security but has been criticised as infringing on civil liberties and privacy. . . . The bill would allow private industry to share user information with the Department of Homeland Security, which would be compelled to share it across 'relevant government agencies', presumably including the Federal Bureau of Investigation (FBI) and the National Security Agency (NSA). The bill has been touted by its supporters, notably the US Chamber of Commerce, as entirely voluntary, but in fact, as Wired points out, other such 'voluntary' programs mandate the kind of data reported and the frequency of the reports."). *See also* Heidenreich, *supra* note 132, at 407 (citing Tom Risen, *Obama Signs Cybersecurity Law In Spending Package,* U.S. NEWS AND WORLD REP. (Dec. 18, 2015, 5:49 PM), http://www.usnews.com/news/articles/2015-12-18/obama-signs-cybersecurity-law-in-spending-package) ("This change in standards is one reason that some privacy experts and some legislators are upset about the fact that CISA was tacked on to the budget bill and passed with no real debate.").

194 Wilson, *supra* note 186. *See also* Heidenreich, *supra* note 132, at 410 ("The information that CISA authorizes the government to collect is too broad. There are too few controls on what information the government collects and on how it uses that information. In fact, CISA specifically authorizes the government to use the information for non-cybersecurity purposes. The information is collected without a warrant or probable cause, yet CISA authorizes the government to use that information in order to prosecute certain crimes.").

195 Wilson, *supra* note 186. *See also* Tran, *supra* note 112, at 497 ("[S]haring information

Others have argued that the CSA's information-sharing framework creates new opportunities for would-be cyber attackers.[196]

If Congress amends the CSA to clarify the meaning and scope of "authorization" as it relates to "cybersecurity purpose," "cybersecurity threat," "defensive measure," and "cyber threat indicator," this would eliminate the need for a possible repeal. Additionally, amending the CSA would quell some of the privacy advocates' fears about the government having too much power to collect and/or share information under the guise of a "cybersecurity purpose" or "cybersecurity threat" because it would ideally narrow and limit the potential scope of its ambiguous provisions, as well as give legislators the chance to debate these provisions.

V. STATE CYBERSECURITY LAWS INVOLVING "AUTHORIZATION"

A number of state legislatures have passed cybersecurity laws.[197] Solely with regard to online privacy and data security, states have enacted statutes covering a wide array of issues.[198] A detailed examination of all of these state cybersecurity laws is beyond the scope of this Comment. This section will, however, briefly discuss some of these state cybersecurity laws that define concepts related to authorization as an example of the kind of language Congress could use to amend the CSA to clarify its ambiguous language centered on the concept of "authorization."

---

does little to prevent successful cyberattacks, given that there have been many already in place. For instance, in 2003, DHS established its U.S. Computer Emergency Readiness Team to collect and analyze data, but its results have been unclear. . . . [The CSA] will very likely face constitutional challenges in courts; the battle of right to privacy in the realm of cybersecurity is far from over.").

196 *See* Tran, *supra* note 112, at 497.

197 *See generally* National Conference of State Legislatures, *Cybersecurity Legislation 2016*, Dec. 8, 2016, http://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2016.aspx (summarizing state cybersecurity laws that were proposed (and in some cases, enacted) in 2016); National Conference of State Legislatures, *Cybersecurity Legislation 2015*, Dec. 31, 2015, http://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2015.aspx (summarizing state cybersecurity laws that were proposed (and in some cases, enacted) in 2015).

198 Examples of such issues include cyberstalking, privacy-related issues, privacy policies, employer access to employees' social media accounts, unsolicited commercial communications, data disposal, electronic solicitation of children, and security breach notifications, to name a few. Alan Charles Raul, Tasha D. Manoranjan, & Vivek K. Mohan, *United States*, *in* THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW 268, 279 (Alan Charles Raul ed., 2014), http://www.sidley.com/~/media/files/publications/2014/11/the-privacy-data-protection-and-cybersecurity-la__/files/united-states/fileattachment/united-states.pdf (internal citations omitted). For state cybersecurity laws that have been enacted in 2016, see National Conference of State Legislatures, *Cybersecurity Legislation 2016*, Oct. 27, 2016, http://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2016.aspx.

For instance, New York's penal code states that "[a] person is guilty of unauthorized use of a computer when he or she knowingly uses, causes to be used, or accesses a computer, computer service, or computer network without authorization."[199] Unlike the CFAA, the New York law defines "without authorization."[200] It states that "without authorization" means "to use or to access a computer, computer service or computer network without the permission of the owner or lessor or someone licensed or privileged by the owner or lessor"[201] and "where such person knew that his or her use or access was without permission or after actual notice to such person that such use or access was without permission."[202] The law further provides that proof that a person accessed or used "a computer, computer service or computer network through the knowing use of a set of instructions, code or computer program that bypasses, defrauds or otherwise circumvents a security measure installed . . . shall be presumptive evidence that such person used or accessed [such a device or network] . . . without authorization."[203]

Similar to New York, Colorado also defines "authorization" in its penal code as "the express consent of a person which may include an employee's job description to use said person's computer, computer network, computer program, computer software, computer system, property, or services as those terms are defined in this section."[204] Similar to the CFAA, Colorado defines "exceed authorized access" as "to access a computer with authorization and to use such access to obtain or alter information, data, computer program, or computer software that the person is not entitled to so obtain or alter."[205]

Virginia's Computer Crimes Act also discusses authorization.[206] It states that "[a] person is 'without authority' when he knows or reasonably should know that he has no right, agreement, or permission or acts in a manner knowingly exceeding such right, agreement, or permission."[207]

---

199 N.Y. PENAL LAW § 156.05 (McKinney 2006). *But see* MD. CODE ANN., CRIM. LAW § 7-302 (West 2010) (a law discussing unauthorized access to computers but not defining "unauthorized access").

200 N.Y. PENAL LAW § 156.00(8).

201 *Id.*

202 *Id. See also id.* (further stating that without authorization "shall also mean the access of a computer service by a person without permission where such person knew that such access was without permission or after actual notice to such person, that such access was without permission").

203 *Id.*

204 COLO. REV. STAT. ANN. § 18-5.5-101(1) (West 2000).

205 *Id.* § 18-5.5-101(6.7).

206 *See* VA. CODE ANN. § 18.2-152.2 (West 2010).

207 *Id.*

More recently, in 2016, Utah adopted a cybersecurity law with provisions related to "unauthorized access" to information technology, specifically unauthorized access of a protected computer.[208] Like the CFAA, the Utah law includes the term "protected computer," which it defines as "a computer that is used in connection with the operation of a business, state government entity, or political subdivision and requires a technological access barrier for an individual to access the computer."[209] To help determine what constitutes unauthorized access, the law defines "authorized user" as "the protected computer's owner; or an individual who has permission to access the protected computer[.]"[210] The law also defines "unauthorized user" as an individual who "is not an authorized user of the protected computer; and accesses the protected computer by: obtaining, without an authorized user's permission, the authorized user's technological access barrier; or circumventing, without the permission of the protected computer's owner, a technological access barrier on the protected computer."[211] The law prohibits unauthorized users from knowingly and intentionally causing harm or damage by obtaining information from a protected computer; transmitting "a program, code, or command to the protected computer;" or using a "technological access barrier" to access the protected computer.[212] By defining which computers this law applies to and what constitutes authorized and unauthorized users, the Utah law is more narrow and limited in application than the CFAA or the CSA.

Congress should amend the CSA to both provide a clear definition of "authorization" and limit the scope of "authorization" in the CSA, similar to what is found in these state statutes. A clear and limiting definition of "authorization" is necessary because other critical phrases in the CSA depend on how the phrases "unauthorized effort" and "unauthorized access" are defined and interpreted. As these phrases stand now, courts could broadly interpret these provisions and provisions that rely on these phrases, so an amendment is necessary to narrow the scope of "authorization" in the CSA. For example, Congress could define "unauthorized effort" as something akin to Utah's definition of "unauthorized access," New York's definition of "without authorization," or Virginia's definition of "without authority."[213] The specificity in these definitions would limit the scope of

---

208 UTAH CODE ANN. §§ 63D-3-101–06 (2016), http://le.utah.gov/~2016/bills/static/hb0241.html. *See also* National Conference of State Legislatures, *Cybersecurity Legislation 2016*, Dec. 8, 2016, http://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2016.aspx.

209 UTAH CODE ANN. § 63D-3-101–06(a).

210 *Id.* § 63D-3-102(1).

211 *Id.* § 63D-3-102(9).

212 *Id.* § 63D-3-104(1).

213 *See id.* § 63D-3-102(9); VA. CODE ANN. § 18.2-152.2; N.Y. PENAL LAW § 156.00(8).

"authorization" in the CSA, thus making the courts' task of interpreting the CSA much easier. Congress could also add a definition of a computer or information system that the CSA applies to in order to further limit the application of the CSA so that it applies to specific devices rather than just *any* computer or electronic device that could connect to the Internet and pose a "cybersecurity threat." Congress could also include examples of what it means by "unauthorized effort" or a "cybersecurity threat," which could give more context to the intended scope of authorization in the CSA. By amending the CSA to incorporate a definition of authorization or examples of unauthorized efforts and cybersecurity threats, Congress could guide courts in interpreting the CSA when questions of liability, monitoring, operating "defensive measures," information sharing, and privacy problems inevitably arise.

VI. CONCLUSION

Perhaps Congress intended the ambiguities in the CSA. Or, perhaps Congress inadvertently included the ambiguities. Either way, ambiguous language exists with respect to the concept of authorization in the CSA, which will create interpretive problems for the judiciary and will have large privacy and security implications if it is not amended, or interpreted narrowly in the absence of any amendments. This Comment recommends that Congress amend the CSA to clarify its scope of authorization, which impacts how courts will interpret "cybersecurity purpose," "cybersecurity threat," "defensive measure," and "cyber threat indicator" under the CSA when questions of liability, monitoring, operating "defensive measures," information sharing, and privacy problems inevitably arise. This clarification would help guide courts in interpreting the CSA and help prevent a potential circuit split of interpretation down the road, similar to that which currently exists with the CFAA. In the absence of any amendments (or a Supreme Court resolution of the CFAA circuit split), however, courts should narrowly interpret the CSA's provisions centering around the concept of authorization, just as the Second, Fourth, and Ninth Circuits have done in the CFAA context.