Eject the Floppy Disk: How to Modernize the Computer Fraud and Abuse Act to Meet Cybersecurity Needs

Bailey McGowan[*]

When people think of computer hacking, they tend to think of some fictional character sitting in their parent's basement while they try to take down some website through various "evil" coding methods. Hacking, as covered by the Computer Fraud and Abuse Act ("CFAA"), is actually much more prevalent and could mean serious prison time for unsuspecting employees. The CFAA is a federal law that both criminalizes and holds people civilly liable when they "exceed[] authorized access." Due to poor drafting, circuits split on whether to read that language broadly and or narrowly, meaning some defendants walk free while others face up to ten years in prison. I argue the Supreme Court should have granted certiorari in Nosal v. United States, and should adopt a broad interpretation of the CFAA to hold people accountable for when they violate the intended-use of information. I make two suggestions on how to modernize the CFAA to keep up with the current pace of cybersecurity law. Finally, I propose some steps employers can take now to protect their information in the interim.

---

[*] J.D. Candidate, Texas Tech University School of Law 2018. Thank you to my parents for your love and support through this process. I could not have done this without you.

I. OFFLINE

In the thirty years since the Computer Fraud and Abuse Act ("CFAA") became law, the number of the technological advancements that have taken place is almost unquantifiable. Aimed at protecting people against white-collar crime and the rise of hackers, the CFAA made hacking and certain misuse of computers illegal.[1]

When the CFAA was introduced in the early 1980s, the federal government was using approximately 18,000 computers.[2] In contrast, in March 2014, the Washington Post estimated that the federal government now uses more than 4 million computers.[3] The difference in the number of computers alone shows the reliance on both the machines and the data those machines make possible.

The CFAA both criminalizes certain behaviors and makes people civilly liable for "exceeding authorized access" of a computer.[4] The issue came to Congress' attention in the early 1980s when a group of Milwaukee

---

[1] H. R. REP. NO. 98-894, at 4 (1984), *as reprinted in* 1984 U.S.C.C.A.N. 3689, 3690.

[2] S. REP. NO. 99-432 at 2 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 2479, 2479.

[3] Craig Timberg & Ellen Nakashima, *Government computers running Windows XP will be vulnerable to hackers after April 8*, WASHINGTON POST (Mar. 16, 2014), https://www.washingtonpost.com/business/technology/government-computers-running-windows-xp-will-be-vulnerable-to-hackers-after-april-8/2014/03/16/9a9c8c7c-a553-11e3-a5fa-55f0c77bf39c_story.html.

[4] *See generally* 18 U.S.C. § 1030 (West 1986). The cases surrounding this Act range from a police officer who improperly used a government database to a Major League Baseball recruiter who hacked into the Houston Astros email system; *See* United States v. Valle, 807 F.3d 508 (2d Cir. 2015); *See also* The Associated Press, *Christopher Correa, Former Cardinals Executive, Sentenced to Four Years for Hacking Astros' Database*, N.Y. TIMES (July 18, 2016), http://www.nytimes.com/2016/07/19/sports/baseball/christopher-correa-a-former-cardinals-executive-sentenced-to-four-years-for-hacking-astros-database.html?_r=0.

teenagers, known as the 414 Gang (after their area code), were able to hack into a cancer treatment center.[5] The teenagers gained access to records of some 6,000 cancer patients and even had the ability to change radiation treatment levels.[6] The incident took a small financial toll on the center, but the life-threatening nature of the hack caused the Senate Committee on the Judiciary concern and led to the modern-day language of the CFAA.[7]

The CFAA can be used to criminally prosecute someone or can be used in a civil lawsuit.[8] The Second, Fourth, and Ninth Circuits claim that the CFAA is much too vague to successfully prosecute or sue under, except in very limited circumstances.[9] Courts and scholars named this the "narrow" interpretation because these courts utilize a more literal interpretation of the CFAA language.[10] In contrast, the First, Fifth, Seventh, and Eleventh Circuits use a "broad" interpretation of the CFAA by construing the language as an intended-use analysis, making prosecution and lawsuits more judicially feasible.[11] This means that the First, Fifth, Seventh, and Eleventh Circuits, interpret improper use of data as actually exceeding authorized access.[12]

This Comment will analyze the purpose of the CFAA by quickly dissecting the House of Representatives' and the Senate's approach to the law in Part II. Then, this Comment will examine the circuit split, teasing out the two different interpretations of the law and how those interpretations create either a prosecution-friendly or plaintiff-friendly jurisdiction versus a defendant-friendly jurisdiction. Next, in Part III, this Comment will analyze the differing viewpoints of the varying interpretations. Part IV will suggest two options for how to handle the circuit split: an analysis of the current language and an explanation as to why the Supreme Court should have granted certiorari, and in doing so, why the Supreme Court should adopt the Fifth Circuit's interpretation of

---

[5] Will Storr, *The kid hackers who starred in a real-life WarGames*, TELEGRAPH (Sept. 16, 2015), http://www.telegraph.co.uk/film/the-414s/hackers-wargames-true-story/.

[6] S. REP. NO. 99-432, at 3.

[7] Storr, *supra* note 5; *See also* S. REP. NO. 99-432, at 3 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 2479, 2480 (describing how the 414 Gang was a concern for the Senate when deciding on the appropriate language for the CFAA).

[8] *See* § 1030.

[9] *See infra* Section II.C. *See also* § 1030. Specifically, the Second, Fourth, and Ninth Circuits operate under the assumption that improper data use is not exceeding authorized access if the person did in fact have authorized access to the computer.

[10] Am. Furukawa, Inc. v. Hossain, 103 F.Supp.3d 864, 872 (E.D. Mich. 2015).

[11] *See infra* Section II.D.

[12] *See infra* Section II.D. *See also Hossain*, 103 F.Supp.3d at 871. This "broad" interpretation is based on an intended-use analysis, meaning employees or competitors can be prosecuted for using data in a manner not intended by the original source.

the law. Alternatively, Part IV will put forth an argument that the CFAA should be repealed and replaced with two different statutes: one for criminal culpability with a separate section for offenders who are government operatives, and another concerning civil liability.

II. BOOTING UP: BACKGROUND ON CFAA

The original language of the CFAA prohibited "accessing a computer without authorization, or it [sic] authorized, abusing that authorization and obtaining what generically is considered to be classified."[13] An amendment switched that language to "exceeds authorized access."[14] The chairperson of the ABA Criminal Justice Section Task Force on Computer Crime suggested the switch after the original 1984 statute left many terms undefined and confusing.[15] This ambiguity, along with the evolving nature of hacking and the need to comprehensively cover employees' behavior, resulted in the language's change.[16] The switch caused a rift among the circuit courts in interpreting the Act.[17] For the past thirty years, federal courts battled with the language of "exceeds authorized access," dividing themselves into two distinct camps.[18]

A. How Do You Use This Thing? Congressional Action on Computer Security

In 1983, the House of Representatives introduced a bill that would eventually become the Computer Fraud and Abuse Act of 1986.[19] First, Congress passed the Comprehensive Crime Control Act of 1984.[20] The House Committee on the Judiciary found white-collar crimes were neglected on both a federal and a state level.[21] At the time, the only statutes remotely dealing with cybersecurity were mail fraud or wire fraud.[22]

---

[13] H.R. REP. NO. 98-894, at 21 (1984), *as reprinted in* 1984 U.S.C.C.A.N. 3689, 3707.

[14] Computer Fraud and Abuse Act of 1986, Pub. L. No. 99–474, 100 Stat. 1213 PL 99–474 (1986).

[15] Dodd S. Griffith, Note, *The Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem*, 43 VAND. L. REV. 453, 470 (1990). Examples of terms left undefined included: "access," "authorization," "affects" and "use".

[16] *Id.*

[17] *See infra* Part II.

[18] *See infra* Section II.C-D.

[19] H.R. REP. NO. 98-894 (1984), *as reprinted in* 1984 U.S.C.C.A.N. 3689.

[20] Scott Eltringham, *Prosecuting Computer Crimes*, OFFICE OF LEGAL EDUC., at 1 https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf (last visited Jan. 12, 2017).

[21] H. R. REP. NO. 98-894, at 4.

[22] *Id.* at 6. Even if mail fraud or wire fraud would cover the alleged conduct, because there was no specific framework of how to go about charging someone for a computer-related crime these cases were treated as an "untested basis for prosecution."

The Senate also expressed concerns over the rise of hackers.[23] After passing the Comprehensive Crime Control Act, Congress continued to investigate potential computer crimes and possible statutory solutions.[24] The Senate Committee on the Judiciary cited the 414 Gang incident as a serious concern over the effectiveness of the Comprehensive Crime Control Act.[25] After the Comprehensive Crime Control Act, the Justice Department criticized the scope of the act as being too narrow because the original version only protected a particular set of financial and credit information.[26]

The American Bar Association's ("ABA") Criminal Justice Section Task Force on Computer Crime suggested the Comprehensive Crime Control Act needed to define terms such as "access," "authorization," "affects," and "use."[27] The Task Force also noted that while the terms used in the Comprehensive Crime Control Act would cover hackers, the terms were still too vague when dealing with employees.[28] While Congress wanted to protect employees who were using data appropriately, the Comprehensive Crime Control Act provided almost no guidance on how to handle the idea that employees could have access to data and still "access without authorization," as the original language stated.[29] The Task Force also wanted the Federal Bureau of Investigations to have primary investigative jurisdiction because, at the time, the Comprehensive Crime Control Act mainly covered government computers.[30] Finally, the task force wanted a civil remedies option because the Comprehensive Crime Control Act did not have one.[31]

In 1986, the CFAA, as it is known today, passed with changes to definitions, the scope of the Act, and an attempt to fix some of the ambiguous language.[32] Specifically, the Act's language changed from "or having accessed a computer without authorization" in the Comprehensive

---

[23] S. REP. NO. 99-432, at 2 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 2479. Hackers are generally defined as "[a] person who writes in assembly language or in system-level languages, such as C." *Hacker*, PC MAG, https://www.pcmag.com/encyclopedia/term/44047/hacker. (last accessed Jan. 29, 2017). However, hacker in this context is referring to someone who conducts "computer sabotage." *Id.*

[24] Eltringham, *supra* note 20, at 1.

[25] S. REP. NO. 99-432, at 3

[26] Griffith, *supra* note 15, at 467.

[27] *Id.*at 470.

[28] *Id.*

[29] *Id.*

[30] *Id.* at 471.

[31] *Id.*

[32] Griffith, *supra* note 15, at 474.

Crime Control Act to "or exceeds authorized access," in the CFAA.[33] Congress aimed at making the "cumbersome" language of the Comprehensive Crime Control Act simpler.[34] The CFAA defines "exceeds authorized use" as "access[ing] a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled to obtain or alter[.]"[35] While this change attempted to fix some of the problems of the previous Act, it has not been enough to keep the courts from adopting drastically different interpretations.

B. Ctrl +: How Cases Arise Under the CFAA and Practical Examples

The Department of Justice identifies three types of cases that arise from the "exceeds authorized access" language.[36] Practitioners dealing with the CFAA would not know these "categories" as the Department of Justice has named them, but, for clarity's sake, this comment will refer to cases by their category to give a firm example of how the CFAA arises and how it is interpreted.[37] First, when a person is prohibited from accessing the information expressly; second, when a person has authorized access to the information and is expressly forbidden from using the information in certain ways, but the access of the information is not conditioned on obeying the restrictions; and third, when a person has not been commanded to avoid certain uses of the information but does so against the authorizing party's best interest.[38]

To better understand these three areas, consider the following: an employee enters information into a database for work. If the employee were to then access another program from another department, this would be an example of the first situation.[39] She was not given authorization and then gained access anyway. For the second category, suppose a person builds a program that will track the changes to a website and compiles that information into a spreadsheet.[40] Even though the website expressly prohibits people from doing this, the website did not condition the person's access of the information on not using the information in a certain way.[41] Finally, if an employee was given access to a certain database, and told to not research personal interests in the database (say a neighbor's billing

---

[33] *Id.*
[34] S. REP. NO. 99-432, at 9 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 2479, 2486.
[35] 18. U.S.C. § 1030 (e)(6) (West 1986).
[36] Eltringham, *supra,* at 9-10.
[37] *Id.* at 10.
[38] *Id.* at 9.
[39] *See generally id.*
[40] *Id.*
[41] *See* EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 578 (1st Cir. 2001).

statement,) but does so anyway, this is an example of the third category of cases.[42] The third category of cases is more controversial because the courts struggle with the narrow and broad interpretation of the CFAA regarding employee's access. A vast majority of cases used in this Comment will be from that third category.[43]

C. Right Click: Narrow Interpretations

In May of 2012, New York City police officer Gilberto Valle logged onto the Omnixx Force Mobile and searched for a woman he knew for years.[44] The program allows officers access to restricted databases, which include private information, such as home addresses and birthdates, as well as the federal National Crime Information Center database.[45] Valle used that information to discuss kidnapping the woman with another user of the Dark Fetish Network—an Internet site for the sex-fetish community.[46] Valle had access to the Omnixx Force Mobile program for his job as a New York City police officer.[47] Valle's misuse of the Omnixx Force Mobile resulted in prosecutors charging Valle under the CFAA.[48] A jury found Valle guilty of violating the CFAA, but the Second Circuit reversed this decision, calling the conviction "highly problematic" because, while Valle was authorized to access the information, he was using the information for unauthorized purposes.[49] The Second Circuit held the court should construe the statute narrowly so as not to "unintentionally turn ordinary citizens into criminals."[50] The Second Circuit also hinted a broad construction could turn seemingly innocent behavior, like checking one's Facebook at work, into a punishable offense.[51] While Valle's case may seem like an extreme use of the CFAA, other circuits have also found interpreting the language to be difficult and have followed the same narrow approach as the Second Circuit.

---

[42] *Id.*

[43] *See supra* Part II.C-D.

[44] United States v. Valle, 807 F.3d 508, 512 (2d Cir. 2015).

[45] *Id.; see also* "*Cannibal Cop" Gilberto Vale found guilty of plot to kidnap, kill and eat women*, CBS NEWS, (May 12, 2013) http://www.cbsnews.com/news/cannibal-cop-gilberto-valle-found-guilty-of-plot-to-kidnap-kill-and-eat-women/.

[46] *Valle*, 807 F.3d at 512.

[47] *Id.*

[48] *Id.*

[49] *Id.* at 523. In opening statements, Valle's attorney argued he did not violate the CFAA because, while Valle did violate the terms of his employment conducting the search, he did not "obtain any information he was not entitled to obtain.".

[50] *Id.* at 527.

[51] *Id.*

The Fourth Circuit wrestled with interpreting the CFAA in *WEC Carolina Energy Solutions v. Miller*.[52] In that case, the defendant, Mike Miller, and his assistant downloaded files from WEC Carolina Energy Solutions ("WEC") and then used those files at a new company to poach a potential client from WEC.[53] The Fourth Circuit held that while Miller may have misappropriated the information, he did not exceed his authorized access.[54] The court reached this conclusion by relying on WEC's complaint, which stated Miller had access to intranet, WEC servers, and confidential information.[55] In conceding these points, WEC essentially stated Miller had authorized access to confidential information, which led to the dismissal of the claim.[56]

The Ninth Circuit used the narrow approach with its opinion in *United States v. Nosal I*.[57] In *Nosal I*, an employee, David Nosal, convinced his coworkers to download confidential source lists for an executive search firm.[58] Nosal then left the company and started a competing business.[59] All of the employees at the firm were aware of the company's explicit policy forbidding use of the company's confidential information.[60] Nosal was charged with aiding and abetting his former coworkers to exceed their authorized access.[61] The count was dismissed by the district court after a motion for reconsideration.[62] The court reasoned "[t]here is simply no way" the definition of "exceeds authorized access" was meant to include company policies. [63]

The Ninth Circuit agreed, stating that the government's argument would make the CFAA too broad.[64] The court also agreed with Nosal, maintaining that the CFAA was only ever intended to be an anti-hacking

---

[52] 687 F.3d 199, 200 (4th Cir. 2012). WEC filed suit against Miller, claiming Miller had violated the CFAA and exceeded his authorized use of the data from the files.

[53] *Id.*

[54] *Id.* at 207.

[55] *Id.*

[56] *Id.* The court used a narrow approach, which concluded an employee exceeds authorized access by gaining access to information outside of his approved access; *see also Id.* at 204. This meant that the court did not find an employee exceeded authorized access when they improperly used such data.

[57] 676 F.3d 854, 856 (9th Cir. 2012). A judge in that opinion wrote: "Computers have become an indispensable part of our daily lives. We use them for work; we use them for play. Sometimes we use them for play at work"; *See also generally* LVRC Holdings LLC v. Brekka, 581 F.3d 1127 (9th Cir. 2009) (explaining how the Ninth Circuit also used a narrow interpretation in another employment case).

[58] *Nosal* 676 F.3d at 856.

[59] *Id.*

[60] *Id.*

[61] *Id.*

[62] *Id.*

[63] *Id.*

[64] *Nosal,* 676 F.3d at 857.

statute.[65] The court advocated that a broad interpretation would "make criminals of large groups of people who would have little reason to suspect they are committing a federal crime."[66] The court argued a broad construction of the CFAA would make seemingly innocent activities such as instant messenger chatting or checking social media punishable simply because those activities may be against company-wide computer-use policies.[67] Further, this could allow companies to improperly fire employees because the company could threaten the employee with FBI interference for misuse of company computers.[68] Thus, a broad construction could "invite arbitrary and discriminatory enforcement" because the employer-employee relationship would evolve from one governed by tort and contract law to one governed by criminal law.[69] On May 5, 2017, Nosal petitioned the Supreme Court to grant certiorari.[70]

D. Left Click: Broad Interpretations

In contrast, while the Second, Fourth, and Ninth Circuits have generally held the Act's language should be read narrowly, the First, Fifth, Seventh, and Eleventh Circuits have adopted a plain-language reading.[71] Instead, these four circuits use more of a reasonable-expectations test when describing acceptable behavior under the CFAA. This test, best described by the Fifth Circuit in *United States v. Phillips* and *United States v. John,* says that when a person exceeds the reasonable expectations of the intended-use of the data, the person has violated the CFAA.[72]

To better explain this, the first major case that depicted a broader interpretation of the CFAA and how it could affect data use comes from

---

[65] *Id.* at 858.
[66] *Id.* at 859.
[67] *Id.* at 860.
[68] *Id.*
[69] *Id*. In a subsequent proceeding regarding the prosecution of Nosal for conspiring with his former coworkers to violate company policy, the Ninth Circuit vacated in part and remanded the case to the district court because Nosal had by the "ordinary meaning" of "without authorization" violated the CFAA. *Id.* at 869. The Ninth Circuit still maintained that *Nosal I* was correctly decided because authorization was not an issue, as the coworkers had authorization from the company despite the fact that they had clearly and admittedly violated company policy. *Id.* at 874. The court reasoned that because Nosal instructed his coworkers to break that company policy, he satisfied the necessary element of intent and thus was a conspirator for violating the "without authorization" portion of the CFAA. *Id.* at 880.
[70] Aurora Barnes, *Petitions of the day*, SCOTUS BLOG (Jul. 11, 2017, 10:31 AM), http://www.scotusblog.com/2017/07/petitions-of-the-day-40/.
[71] *See infra* Part IV.
[72] *See infra* footnotes 82–97 and accompanying text (explaining the intended-use analysis and how these circuits derive their interpretations).

the First Circuit in *EF Cultural Travel BV v. Explorica, Inc*.[73] Explorica, a company founded in 2000, arranged global trips for students.[74] The company was a direct competitor to EF, which was the largest privately-owned teen travel company in the world.[75] Employees from EF left to join Explorica and sought to undercut EF's prices to take over the student travel market.[76] Part of Explorica's strategy was to build a "scraper" that would extensively search EF's website for pricing on tour codes.[77] Explorica then used the information to undercut EF's prices.[78] After finding out about the scraper during a separate lawsuit, EF was granted an injunction against Explorica from using the scraper, and filed a lawsuit claiming Explorica violated the CFAA.[79]

The First Circuit, in rendering its decision, did not decide whether the use of a scraper would satisfy the CFAA's language of "exceeds authorized use."[80] Instead, the court found that because there was a broad confidentiality agreement between the employee involved in this lawsuit and EF, the employee exceeded authorized use when he contributed to the development of the scraper and the subsequent use of the scraper on EF's website.[81]

This broad interpretation was better defined in *United States v. Phillips*, a case involving Christopher Andrew Phillips, a freshman at the University of Texas.[82] Phillips signed a computer-use policy upon matriculation, but shortly after starting school, Phillips began to steal data, including passwords.[83] Eventually, Phillips stole "a veritable informational goldmine," including bank account information, birth

---

[73] 274 F.3d 577, 578 (1st Cir. 2001).

[74] *Id.*

[75] *Id.* at 579.

[76] *Id.*

[77] *Id*. Scrapers are used on the Internet for search engines to filter content and find information. *Id.* The difference with Explorica's scraper is that the scraper only targeted EF's website, recording more than 30,000 inquiries and price information and then tunneling that information into a comprehensive spreadsheet for Explorica. *Id.* Explorica used the scraper twice, amassing 60,000 lines of data, which is equal to around eight telephone directories. *Id.* at 580.

[78] *Id.* at 579

[79] *Explorica, Inc.*, 274 F.3d at 580. The court found that, because the employee instructed a tech company how to decipher EF's website and find the tour codes, the employee had exceeded the authorized use of EF's website. *Id.* at 583. The employee attempted to argue that all of the information was available on EF's website; however, the court found the employee exceeded his authorized used because of the language of a contract he signed: "which might reasonably be construed to be contrary to the interests of EF." *Id.*

[80] *Id. at* 581.

[81] *Id.*

[82] 477 F.3d 215, 217 (5th Cir. 2007).

[83] *Id.*

records, and Social Security numbers.[84] Despite warnings, Phillips used a "'brute-force attack' program" to steal up to six Social Security numbers per second."[85] A jury convicted Phillips under the CFAA, and he received five years' probation, five-hundred community service hours, and restitution in the amount of $170,056, which he subsequently appealed.[86]

The Fifth Circuit used an intended-use test to determine if Phillips violated the CFAA when he used the university's computer system to gather data.[87] In doing so, the court stated that the CFAA should be read broadly to determine whether or not the access exceeded authorization.[88] To establish that, a court must first determine if a reasonable person would understand that what they were doing was outside of what the website's owner intended.[89]

The Fifth Circuit further clarified the aforementioned analysis in *United States v. John*.[90] In that case, the defendant, Dimetriace Eva-Lavon John, was an account manager at Citigroup.[91] Through her position, John had access to customer account information.[92] John gave her half-brother printouts of screenshots of customer information and eventually gathered the confidential information of at least seventy-six corporate customers.[93] John's half-brother used that information to incur fraudulent charges against four of those corporate customers.[94] John tried to argue that she did not violate the CFAA when she accessed the customer's data because she was authorized to use Citigroup's computers and accessing that data was a part of her job.[95] The First Circuit again used the intended-use analysis to reason that what John did was in fact a violation of the CFAA: To give but one example, an employer may "authorize" employees to

---

[84] *Id.*

[85] *Id.* at 218. The attack cost the university close to $200,000 to assess the damage and notify victims. *Id.* It was estimated over the fourteen-month attack that Phillips gained access to 45,000 people's information, but claimed he never intended to use or sell the information. *Id.*

[86] *Id.* at 218–19.

[87] *Id.* at 219. Phillips attempted to argue that because the university's website was a public application, he was an authorized user. *Id.* at 220. In making their decision, the court reasoned that, while anyone could type the URL for the university's website into the search bar, the university had to grant access for individual users and that created a contractual relationship that Phillips violated. *Id.*

[88] *Phillips*, 477 F.3d at 219.

[89] *Id.* at 219-220.

[90] 597 F.3d 263 (5th Cir. 2010).

[91] *Id.* at 269.

[92] *Id.*

[93] *Id.*

[94] *Id.*

[95] *Id.* at 271. In a parsing of the statute, John argued the CFAA does not cover the actual use of the information but instead only covers accessing, obtaining, or altering data she was not authorized to obtain. *Id.*

utilize computers for any lawful purpose but not for unlawful purposes and only in furtherance of the employer's business. An employee would "exceed [ ] authorized access" if he or she used that access to obtain or steal information as part of a criminal scheme.[96] The Fifth Circuit reasoned that because she was authorized to access the information for limited purposes only and understood that as a part of her job description, John thus exceeded authorized access when she used the information outside of the scope of her employment.[97]

Finally, the Eleventh Circuit furthered the implications of the intended-use analysis by finding that merely accessing the information would violate the CFAA.[98] In *United States v. Rodriguez*, Roberto Rodriguez worked for the Social Security Administration and had access to Social Security numbers, addresses, birthdates, and other information due to the nature of his job.[99] Rodriguez refused to sign acknowledgment forms about policies regarding the databases.[100] It was through this monitoring that the Administration flagged Rodriguez's access and told Rodriguez that the Administration was conducting a criminal investigation.[101] Rodriguez claimed he was conducting a whistleblowing expedition to see if the Administration would notice his unauthorized use.[102] Rodriguez was sentenced to one year in prison and one year of supervised release.[103] Rodriguez relied upon *United States v. John*, saying that only the use of the information would be a crime; the court, however, corrected Rodriguez, finding that because he conceded he had exceeded his authorized use, it did not matter what purpose Rodriguez had for the information.[104] The court also noted that it did not matter that Rodriguez did not use the information to defraud or for financial gain.[105] Simply exceeding his authorized use was enough to convict Rodriguez criminally.[106]

---

[96] *John*, 597 F.3d at 271.

[97] *Id.* at 272.

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

[99] *Id.* at 1260. On numerous occasions, Rodriguez accessed information of former girlfriends, family members, and random strangers, going as far as to use the information to wish someone a "happy half-birthday." *Id.* at 1261.

[100] *Id*. The Social Security Administration asserted that to make sure employees were following the policies, it gave individualized identification numbers and passwords and monitored the employee's access and compliance with policy. *Id.*

[101] *Id.* at 1260.

[102] *Id.* at 1262.

[103] *Id.*

[104] *Rodriguez*, 628 F.3d at 1263.

[105] *Id.*

[106] *Id.*

E. Force Quit: The Call for Reform

In 2010, Aaron Swartz, a co-founder of the popular website Reddit, was indicted for "attempting to download all of the electronically archived materials maintained by JSTOR while accessing them through a computer network operated by the Massachusetts Institute of Technology ("MIT")."[107] Swartz allegedly downloaded millions of articles from JSTOR, a digital library boasting more than 2,300 academic journals and historical information, and then released the documents so that anyone could read and interpret them.[108] On January 11, 2013, Swartz committed suicide.[109] If Swartz had been convicted, he could have faced up to thirty-five years in prison.[110]

Some called Swartz's actions political activism and used the indictment and subsequent suicide as proof that the reach of the CFAA needs curtailing.[111] As a result, in June 2013, Representative Zoe Lofgren of California introduced H.R. 2454, commonly known as "Aaron's Law."[112] The law would amend the CFAA to strike the phrase "exceeds authorized access" and instead replace it with the phrase "access without authorization."[113]

The amended CFAA would define "access without authorization" as: "(A) to obtain information on a protected computer; (B) that the accesser lacks authorization to obtain; and (C) by knowingly circumventing one or more technological or physical measures that are designed to exclude or prevent unauthorized individuals from obtaining that information."[114] These amendments would imply that violations of terms of service or acceptable use policies would not qualify as exceeding authorized

---

[107] United States v. Swartz, 945 F.Supp.2d 216, 217 (D. Mass. 2013); *See also* Josephine Wolff, *The Hacking Law That Can't Hack It*, SLATE (Sept. 27, 2016, 11:15 AM), http://www.slate.com/articles/technology/future_tense/2016/09/the_computer_fraud_and_abuse_act_turns_30_years_old.html.

[108] Peter Eckersley, *Farewell to Aaron Swartz, an Extraordinary Hacker and Activist*, ELECTRONIC FRONTIER FOUND (Jan. 12, 2013), https://www.eff.org/deeplinks/2013/01/farewell-aaron-swartz. *See also New to JSTOR? Learn More About Us*, JSTOR http://about.jstor.org/10things.

[109] *Id.*

[110] Eckersley, *supra* note 107.

[111] *Id.*

[112] Aaron's Law Act of 2013, H.R. 2454, 113th Cong. (2013).

[113] *Id.*

[114] *Id.*

access.[115] The law did not pass in 2013 and failed to become codified law when reintroduced in 2015.[116]

Senator Sheldon Whitehouse, who has also proposed an amendment to the CFAA, criticized Aaron's Law, claiming it would decriminalize insider hacking.[117] Major technology and software companies, such as Oracle, Adobe, and the Software and Information Industry Association, oppose changing the CFAA with such mechanisms as Aaron's Law.[118] Oracle alone spent $1.5 million for each quarter in 2013 for lobbying efforts to stop Congress from passing Aaron's Law because the broad language makes litigation more favorable to companies.[119]

F. Restart: Texas' Version of the CFAA

On December 31, 1984, Texas State Senator Ray Farabee introduced Senate Bill No. 72, a bill "relating to the creation of offenses involving breach of computer security."[120] The bill later passed on May 25, 1985, following administrative and substantive changes.[121] Senator Farabee recognized the importance of computers, citing the difference between personal computer sales in 1976 and 1982: none and $1 billion, respectively.[122] At the time the bill was introduced, thirty-five states had computer crime bills on the books. [123]

---

[115] *See* Wolff, *supra* note 107. Terms of service is described by PC Magazine as rules a person or organization must follow in order to use a service. *See also Terms of Service*, PC MAG, http://www.pcmag.com/encyclopedia/term/62682/terms-of-service. They are legally binding unless the terms violate federal or local law. *Id*. Websites that store personal data for the user have terms of services like social media sites or "financial transaction sites." *Id.* In contrast, an acceptable use policy is a policy that describes prohibited behaviors, like spamming. *Acceptable use policy*, PC MAG, http://www.pcmag.com/encyclopedia/term/37376/acceptable-use-policy. These policies can also be found at schools or universities for access to a computer lab or database, for example. *Id.*

[116] *See Id.* Due to the manner in which Swartz downloaded the files from JSTOR, the proposed language may not have protected Swartz. *Id.*

[117] Sheldon Whitehouse, *Hacking into the Computer Fraud and Abuse Act: The CFAA at 30: Keynote*, 84 GEO. WASH. L. REV. 1437, 1440 (2016). By using a terms of service approach for breaching authorization, Aaron's Law would still make behaviors like logging into your spouse's Facebook or getting around a paying for access to an Internet site by clearing your cookies illegal behavior, Whitehouse claims. *Id.*

[118] Fruzsina Eördögh, *Silicon Valley is Stonewalling Efforts to Amend the Law Imprisoning Hacktivists*, VICE (July 16, 2014 3:51 PM), http://motherboard.vice.com/read/silicon-valley-is-stonewalling-efforts-to-amend-the-law-imprisoning-hacktivists.

[119] *Id.*

[120] S.B. No. 72, 69th R.S. (Tx. 1985), 1-2.

[121] *See generally* S.B. NO. 72, *supra* note 120.

[122] *Id.* at 5.

[123] *Id.* These states included: Alaska, Arizona, California, Colorado, Connecticut, Delaware, Georgia, Hawaii, Idaho, Illinois, Iowa, Kentucky, Louisiana, Maine, Maryland,

The current language of Texas Penal Code § 33.02 "Breach of Computer Security" reads as follows: "(a) A person commits an offense if the person knowingly accesses a computer, computer network, or computer system without the effective consent of the owner.[124] Part (b-1) makes the scope of the offense very clear:

A person commits an offense if, with the intent to defraud or harm another or alter, damage, or delete property, the person knowingly accesses: (1) a computer, computer network, or computer system without the effective consent of the owner; or (2) a computer, computer network, or computer system: (A) that is owned by: (i) the government; or (ii) a business or other commercial entity engaged in a business activity; (B) in violation of: (i) a clear and conspicuous prohibition by the owner of the computer, computer network, or computer system; or (ii) a contractual agreement to which the person has expressly agreed; and (C) with the intent to obtain or use a file, data, or proprietary information stored in the computer, network, or system to defraud or harm another or alter, damage, or delete property.[125]

There are only two defenses within the Texas Penal Code § 33.02: legitimate law enforcement purposes and when someone contracts to provide computer security.[126] Texas has also codified the same law as a civil claim in Section 143.001 of the Texas Civil Practices and Remedies Code.[127]

Massachusetts, Michigan, Minnesota, Missouri, Montana, New Mexico, Nevada, North Carolina, North Dakota, Ohio, Oklahoma, Pennsylvania, Rhode Island, South Dakota, Tennessee, Utah, Virginia, Washington, Wisconsin, and Wyoming.

[124] TEX. PENAL CODE ANN. § 33.02(a) (West 1985).

[125] *Id.*

[126] *Id.*

[127] TEX. CIV. PRAC. & REM. CODE ANN. § 143.001 (West 1989). "A person who is injured or whose property has been injured as a result of a violation under Chapter 33, Penal Code, has a civil cause of action if the conduct constituting the violation was committed knowingly or intentionally." *Id.* The definitions for the Texas statute define access as "approach[ing], instruct[ing], communicat[ing] with, stor[ing] data in, retriev[ing] or intercept[ing] data from, alter[ing] data or computer software in, or otherwise mak[ing] use of any resource of a computer, computer network, computer program, or computer system." TEX. PEN. CODE ANN. § 33.01(1) (West 1985). The statute also defines the terms computer, computer network, computer program, or computer system. Ann. § 33.01(4)(5)(6)(8) (West 1985). Computer is defined as "an electronic, magnetic, optical, electrochemical, or other high-speed data processing device that performs logical, arithmetic, or memory functions by the manipulations of electronic or magnetic impulses and includes all input, output, processing, storage, or communication facilities that are connected or related to the device." *Id.*; TEX. PENAL CODE ANN. § 33.01 (4) (West 1985). Computer network is "the interconnection of two or more computers or computer systems by satellite, microwave, line, or other communication medium with the capability to transmit information among the computers." *Id.*; Ann. § 33.01 (5) (West 1985). A computer program is defined as "means an ordered set of data representing coded instructions or statements that when executed by a computer cause the computer to process

III. FROM DIALUP TO WIFI: POTENTIAL SOLUTIONS FOR THE CFAA IN THE MODERN AGE

With a variety of interpretations from seven circuits, it is difficult to see how a company or a prosecutor should handle an allegation of a violation of the CFAA.[128] Mere miles across a state line can mean the difference between jail time and walking free due to broad interpretations.[129] This growing strife between interpretations and the dire consequences created a variety of opinions and options of where the CFAA may go next.

A. Password Required: A Look at the Different Opinions on the CFAA

In an interview with *Slate.com*, Former New Jersey Representative William J. Hughes stated that Congress was trying to create a law that would help solve future problems when it developed the CFAA.[130] He stated that, "We were attempting to anticipate the problems that surely would evolve over time . . . ."[131] Representative Hughes analogized that since there were laws on the books that protect breaking into a home, Congress should also try to prevent theft of information stored on computers.[132] As the use of the CFAA has transitioned over the years, it is clear that some courts favor a broad interpretation of the law while others favor a narrower one.[133] Opponents of the CFAA point to the inconsistencies with interpretations and the range in punishments as support for reform.[134] Specifically, opponents are looking for "narrower definitions, gentler punishments, and clearer exceptions carved out for security researchers."[135] Meanwhile, Representative Hughes is calling for the exact opposite: "I suspect that we may have to go back and broaden the statute even more to make sure that we're catching everything and everyone we should be."[136] He cites the CFAA as essential for protecting property in the age of cyber attacks.[137]

---

data or perform specific functions." *Id.;* § 33.01 (6) (West 1985). Finally, a computer system is "any combination of a computer or computer network with the documentation, computer software, or physical facilities supporting the computer or computer network." § 33.01 (8) (West 1985).

[128] *See supra* Part II B-C.

[129] Michael L. Levy, *A Proposed Amendment to 18 U.S.C. § 1030 – The Problem of Employee Theft*, 84 GEO. WASH. L. REV. 1591, 1593 (2016).

[130] Wolff, *supra* note 107.

[131] *Id.*

[132] *Id.*

[133] *Id.*

[134] *Id.*

[135] *Id*.

[136] Wolff, *supra* note 107.

[137] *Id.*

A group of academic researchers and journalists attempted to reform the second category of cases in the summer of 2016.[138] With the help of the American Civil Liberties Union, the researchers filed a complaint for declaratory and injunctive relief against Attorney General Loretta Lynch, alleging that the CFAA makes violating a terms of service agreement a crime.[139] The plaintiffs in the case claim that they pose online as people of different races to research potential discrimination in hiring and housing practices.[140] By claiming to be people they are not, the plaintiffs are violating the terms of service and could be prosecuted under the CFAA.[141] The complaint points out that even the Justice Department's manual on the CFAA states that "exceeds authorized access" is: [R]elatively easy to prove that a defendant had only limited authority to access a computer in cases where the defendant's access was limited by restrictions that were memorialized in writing, such as terms of service [or] a website notice . . . .[142]

Reform efforts are also underway in the third category of cases with the sentencing of Matthew Keys. Keys was a former Reuters employee who gave members of the hacker group "Anonymous" login information for the Tribune Media.[143] Upon obtaining this information, Anonymous altered a headline on a story on the *LA Times* website, which was live on the Tribune Media website for about forty minutes.[144] Those forty minutes turned into a two-year sentence for Keys, who was convicted of violating the CFAA for giving his information to Anonymous.[145] Again, Keys did not post the headline himself, but merely shared his login information.[146] The eight-word headline allegedly cost Tribune Media $929,977 in defacement.[147] When convicted, Keys tweeted out, "That was bullsh**."[148]

---

[138] Complaint at 1, Sandvig v. Lynch, No. 1:16-cv-1368 (JDB) (D.D.C. June 29, 2016).
[139] *Id.*
[140] *Id.* at 4.
[141] *Id.*
[142] *Id.* at 8.
[143] Kate Conger, *Journalist Matthew Keys sentenced to 2 years in hacking case*, TECH CRUNCH (Apr. 13, 2016), https://techcrunch.com/2016/04/13/matthew-keys-sentenced-under-cfaa/.
[144] Conger, *supra* note 143.
[145] *Id.*
[146] *Id.*
[147] *Id.*
[148] Cat Zakrzewski, *Journalist Mathew Keys Found Guilty on Hacking Charges*, Tech Crunch (Oct. 7, 2015), https://techcrunch.com/2015/10/07/journalist-matthew-keys-found-guilty-on-hacking-charges/.

B. Do You Wish to Debug? Ideas on What Happens Next

The American Bar Association suggested that repealing the CFAA would not be a total blow to either the criminal or civil realms.[149] For example, if the CFAA were repealed, Prosecutors could continue to look to the federal trade-secrets statute in 18 U.S.C. § 1832.[150] That trade-secret statute was critical in cases like *WEC Carolina Energy Solutions LLC v. Miller*.[151] Trade secret charges may be the best alternative route for prosecutors to charge defendants with, as it is more narrowly tailored to target people who "knowingly [and] without authorization cop[y], duplicate . . . download, upload, destroy, . . . transmit, deliver, . . . or convey such information . . . " for an economic benefit.[152] If someone violates the statute, they can be convicted for up to ten years in prison.[153] A violation of the federal trade secret law covers at least in part what legislators set out to do with the CFAA.

In terms of civil alternatives, employers have other avenues available through a variety of claims.[154] Employers could easily bring claims of "breach of contract, breach of fiduciary duty, conversion, tortious interference with an economic advantage, unfair competition, or misappropriation of trade secrets."[155]

In 2011, Professor Michael Risch from Villanova University's Charles Widger School of Law posted in a blog about the "scary" implications of the CFAA and interpretations.[156] In dissecting the 2011 ruling in *United States v. Nosal*, Risch suggested that the CFAA could be fixed by requiring a two-part standard for the CFAA.[157] First, an action under the CFAA must be tied to an independent wrongful action; for example, trade secret misappropriation.[158] Second, that wrongful action would need to be tied to exceeding authorized access.[159]

---

[149] Aaron M. Danzig & Matthew A.S. Esworthy, *Glitches Within the CFAA's "Exceeds Authorized Access" Language*, A.B.A. (Oct. 9, 2013) http://apps.americanbar.org/litigation/committees/criminal/articles/summer2013-1013-glitches-within-cfaas-exceeds-authorized-access-language.html.

[150] *Id.*

[151] *See* 687 F.3d 199 (4th Cir. 2012).

[152] 18 U.S.C § 1832(a)(2) (1996).

[153] § 1832(a).

[154] Danzig & Esworthy, *supra* note 149, at 21.

[155] *Id.*

[156] Michael Risch, *When the Right Interpretation of the Law is a Scary One (CFAA Edition),* Madisonian (Apr. 18, 2011) http://madisonian.net/2011/04/28/when-the-right-interpretation-of-the-law-is-a-scary-one-cfaa-edition/.

[157] *Id.*

[158] *Id*.

[159] *Id.* Risch put it best when he wrote: "In other words, lying about your age shouldn't affect access rights generally, but lying about your age might very well be a problem if the reason you did so was to prey on young children." *Id.*

Another suggestion would be to reject both of the circuits analyses and instead akin authorization to a physical trespass with similar elements.[160] This would require a prosecutor or a plaintiff to prove three elements to be successful: (1) access violating an express or implied prohibition; (2) the alleged violator knew or should have known about the prohibition; (3) and, the prohibition would be "material or related to the underlying policy of trespass."[161] The second element breaks down into three subcategories to prove knowledge of the prohibition: a code-based approach, a notification approach, and a social norm approach.[162] A code-based approach, like a password, would be required if the computer's owner had some sort of program to stop access and the user knew they were exceeding their authorization.[163] Another approach could be a notification that certain access is unauthorized, like a disclaimer or a terms of service post.[164] The last type of knowledge to show a user knew or should have known they violated their terms of access would be a social norm approach.[165] An example would be a hacker continuously accessing a website with a program that shuts down the website's server.[166] While the hacker was authorized to visit the site, social norms would suggest the hacker was not authorized to visit the site in such an aggressive manner to shut the site down.[167]

There are inherent problems with this physical trespass approach. While a code-based approach to understanding whether or not the user should have known their access exceeded authorization would seem to be a simple solution, consider the following scenario from Michael L. Levy, the Chief of Computer Crimes for the United States Attorney's office in the Eastern District of Pennsylvania.[168] One employee asks another to login to his computer at work while he is away so she can relay some information.[169] From a code-based approach, the second employee would not know or have reason to know that they had exceeded authorized access.[170] If that same employee then guessed the first employee's

---

[160] Josh Goldfoot & Aditya Bamzai, *A Trespass Framework for the Crime of Hacking*, 84 GEO. WASH. L. REV. 1477, 1483 (2016).

[161] *Id.* at 1483.

[162] *Id.* at 1487–94.

[163] *Id.* at 1487.

[164] *Id.* at 1490.

[165] *Id.* at 1493. This approach suggests the user would know their access was prohibited because "social norms, or conventions, with which the defendant was familiar, demand the conclusion." *Id.*

[166] Goldfoot & Bamzai *supra* note 160, at 1493.

[167] *Id.*

[168] Levy, *supra* note 129, at 1603.

[169] *Id.*

[170] *Id.*

password and used it, they would still not have violated a code-based approach.[171] This is because they were able to overcome the code of the program and still access the information.[172] Thus, there was nothing impeding the second employee's access.[173]

Also, the notification approach poses an issue to the physical trespass approach. Lawyers spend hundreds of hours drafting terms of service agreements that are rarely read or contemplated until someone has a problem with the website.[174] Therefore, the notification is not actually effective because the user does not have actual notice, just constructive notice. For example, if a person tweaks his or her dating profile to make his or herself seem more interesting by saying he or she has traveled to Paris but does not qualify that statement as Paris, Texas, that person has violated a notification approach.[175] Another example of a violation of a notification approach would be providing the wrong phone number or email address to avoid unwanted marketing.[176] These seemingly harmless activities would violate a notification approach even though they are not malicious or criminal in society's view.[177]

Lastly, the social-norm approach toward determining knowledge proves difficult in the changing way people use technology.[178] In Judge Reinhart's *Nosal II* dissent, he pointed out that today password sharing is the norm.[179] In fact, Judge Reinhart said the CFAA "does not make the millions of people who engage in this ubiquitous, useful, and generally harmless conduct into unwitting federal criminals."[180] Instead, he concluded that the CFAA was not meant to cover the everyday sharing of passwords such as with Netflix.[181] Because so many people engage in password sharing, it is hard for people to conceptualize that they are violating a social norm in the process. Although parents of adolescents everywhere may hate it, the excuse "everyone's doing it" makes sense for a social-norm approach. While perhaps one of the other two notification approaches would cover this type of behavior, the social-norm approach is problematic when certain behaviors become commonplace.

---

171 *Id.* at 1603–04.
172 *Id.* at 1604.
173 *Id.*
174 Whitehouse, *supra* note 117, at 1438.
175 *Id.*
176 *Id.*
177 *Id.*
178 *See infra* Part II.C.
179 United States v. Nosal (*Nosal II)*, 828 F.3d 865, 888 (9th Cir. 2016), *opinion amended, reh'g denied*, 016 WL 7190670 (9th Cir. 2016).
180 *Id.*
181 *Id.* at 889.

Another approach to fixing the problems with the CFAA includes amending the language, like that of Senator Sheldon Whitehouse and Senator Lindsey Graham's July 2015 proposal.[182] The amendment would replace the language of the CFAA to "intentionally access[ing] a protected computer without authorization and thereby obtain[ing] information from or caus[ing] damage to any such protected computer."[183] However, the proposed amendment uses "protected computer," and calls for the same definition currently in the CFAA.[184] That definition is narrow and would only protect government computers or those used for interstate or foreign commerce.[185] For example, unless an employer is the United States government, a financial institution, or affecting interstate or foreign commerce, the amendment does not cover a situation in which someone stole information from their employer.[186] While the phrase interstate commerce could be stretched to almost any situation, without a more clear definition of the type of information this amendment would protect, this amendment leaves the CFAA weaker, rather than stronger than before.

IV. CLICK HERE TO AGREE: POTENTIAL SOLUTIONS TO THE CFAA CRISIS

In order to fix the CFAA to provide a more uniform approach, the Supreme Court could grant certiorari and give courts a uniform interpretation, or Congress could pass an amendment to the CFAA, providing better definitions and context on how the CFAA should be used.

A. System Override: The Supreme Court Option

The Supreme Court should have granted certiorari in *Nosal v. United States* to answer the question concerning whether the CFAA should be

---

[182] Levy, *supra* note 129, at 1607.

[183] *Id*. The rest of the amendment reads: "(B) accesses a protected computer with authorization and thereby knowingly obtains information from such computer that the accessor is not entitled to obtain, or knowingly obtains any information from such computer for a purpose that the accessor knows is prohibited by the computer owner, if - (i) the value of the information obtained exceeds [$ 10,000]; (ii) [the conduct was undertaken in furtherance of any felony violation of the laws of the United States or of any State, unless an element of such violation would require proof that the information was obtained without authorization or in excess of authorization;] or (iii) the protected computer is owned or operated by or on behalf of a State or local governmental entity responsible for the administration of justice, public health, or safety, or of the United States Government; and (C) the limitation on access to or use of the information is not based solely on the terms of a contractual obligation or agreement, such as an acceptable use policy or terms of service agreement, between a provider of online service and a customer or subscriber thereof." *Id.*

[184] *Id*.

[185] 18 U.S.C. § 1030 (e)(2) (West 1986).

[186] *See supra* Section II.D.

interpreted in a broad or a narrow manner.[187] Unfortunately, on October 7, 2017, the Supreme Court denied certiorari.[188] *Nosal* was ideal because it fit into the third category in which the CFAA normally arises; when an employee takes data from their employer and then uses that data for their own gain.[189] The first category, when someone is hacking or stealing information, would cause less of a controversy under the current language of the CFAA because that type of behavior would fall into the unauthorized access portion of the CFAA.[190] Alternatively, the second category, essentially exceeding the terms of service or an acceptable use policy, would benefit from a more definitive answer, but since those types of cases rarely arise, an interpretation for the third category would cover this second category.[191]

United States v. Nosal, was a perfect example of the type of case the Supreme Court should grant certiorari for, as it involves an employee who took his work-granted privileges and used them in a manner not intended by their employer.[192] Nosal took confidential information from his employer so he could start his own firm in the same business.[193] A Supreme Court decision would have been helpful because deciding an interpretation for the CFAA should be all-encompassing. Then, the Supreme Court should interpret the CFAA in a broad sense like the First, Fifth, Seventh, and Eleventh Circuits.[194]

The CFAA was passed as a way to combat a new type of crime in an age when the impact of computers and the data they could create and store was not fully comprehensible.[195] Even so, the principle behind the CFAA remains the same: to protect information stored electronically.[196] Under a broad interpretation, the CFAA can do just that. By looking at the individual circumstance, a court should answer just one question: would a reasonable person understand that what the accused was doing was outside of the intended-use of the access granted?[197] This would allow the government and companies to protect their information, which is at the

---

[187] Aurora Barnes, *Petitions of the day*, SCOTUSBLOG (Jul. 11, 2017, 10:31 AM), http://www.scotusblog.com/2017/07/petitions-of-the-day-40.

[188] Docket, *United States v. Nosal*, https://www.supremecourt.gov/search.aspx?filename=/docket/docketfiles/html/public/16-1344.html (last visited Oct. 16, 2017).

[189] *See supra* Section II.B.

[190] *See Id.*

[191] *See Id.*

[192] *See supra* Section II.D.

[193] *See Id.*

[194] *See Id.*

[195] *See supra* Section II.A.

[196] *See Id.*

[197] *See supra* Section II.D.

heart of the CFAA. By following this analysis, a court would almost always come down in favor of the government or a company. While this may seem harsh, the purpose of the CFAA is clear.[198] Congress intended to protect data and, in a digital age, there can be no loopholes.

B. Rewiring the CFAA: A Suggested New Approach

If the Supreme Court does not eventually grant certiorari and Congress instead decides to amend the CFAA, there are three major considerations. First, Congress should emphasize data rather than computers in any amendment. Second, Congress should seek to fully define all aspects of an amendment, creating one interpretation of the law for courts to follow. Finally, Congress should consider bifurcating the civil and criminal aspects of any amendment.

First, Congress should amend the CFAA in title and scope to focus on what they are actually trying to protect: data. The CFAA is not truly concerned with the desktop or laptop computer on every employee's desk.[199] Nor is the CFAA aimed at the cellphone in the pocket of almost every American with a smartphone.[200] The CFAA is aimed at protecting data.[201] This slight tweak covers the information stored electronically and is a better descriptor at the root of the litigation. If an employee were to walk out of the office with the intent to steal their work computer, it would be theft. If the employee were to take the information from the computer, they are only stealing the data. This data is the root of the three categories of cases involving the CFAA. Hackers do not hack computers to steal equipment; they do so to steal data. One potential definition of data comes from Texas' version of the CFAA.[202] While not the most updated version, this definition does encompass the purpose of the law rather than computer.

"Data" means a representation of information, knowledge, facts, concepts, or instructions that is being prepared or has been prepared in a formalized manner and is intended to be stored or processed, is being stored or processed, or has been stored or processed in a computer. Data may be embodied in any form, including but not limited to computer

---

198 *See supra* Section II.A.

199 *See supra* Section II.A.

200 *Mobile Fact Sheet*, Pew Research Center, PEW INTERNET (Jan. 12, 2017), http://www.pewinternet.org/fact-sheet/mobile/. The Pew Research Center found seventy-seven percent of Americans own a smartphone. *Id.* In 2011, that number was just thirty-five percent in 2011. *Id.*

201 *See supra* Section II.A.

202 Tex. Pen. Code Ann. § 33.02 (West 1985).

printouts, magnetic storage media, laser storage media, and punchcards, or may be stored internally in the memory of the computer.[203]

Second, Congress should amend the CFAA with a new definition of "exceeds authorized access." Alternatively, Congress should adopt a version of the CFAA similar to Texas's law since Texas' law fully encompasses all three categories of CFAA cases.[204] If Congress were to re-define "exceeds authorized access," using the broad interpretation of "whether a reasonable person would understand what the accused was doing was outside of the intended-use of the access granted," courts could apply a more uniform approach to CFAA cases across all three categories. This would still come with the problems under the second category mentioned above.[205] Alternatively, by adopting a statute similar to Texas', all three categories would be managed in a more uniform manner. Texas' law is focused on both hackers and employees, both private and government, who use information in an unintended way.[206] Specifically, section (b-1) covers the first and third category of cases completely, making it a crime to both hack and take information from an employer.[207] By further describing what the person intended to do in (b-1)(C), employees who accidentally access information would not be subject to prosecution.[208] This interpretation would also limit the second category of cases because of the narrow intent definition. With this definition, researchers, like those of the ACLU tracking possible discriminatory practices, would not be subject to prosecution.[209] Instead, Texas' language sets out narrow parameters that would encompass the purpose the CFAA is trying to protect in a way that would favor a more uniform interpretation.

Finally, the CFAA currently has the same standard for both a criminal and civil application. In Texas, the civil component of the CFAA law lowers the mens rea standard to knowingly or intentionally. This allows those who want to sue under Texas's version of the CFAA an opportunity to recover if the conduct does not rise to the same level as the intent under (b-1)(2)(C). Congress should consider bifurcation of the criminal and civil standard in any future amendments to offer protection of the same conduct that does not rise to the level of criminal culpability. This would further Congress' justification for the statute while still

---

[203] Tex. Pen. Code Ann. § 33.01(11) (West 1985).

[204] *See supra* Section II.B.

[205] *See Explorica, Inc.*, 274 F.3d 577; Eltringham, *supra* note 20, at 9-10 (explaining how cases involving the CFAA arise).

[206] Tex. Pen. Code Ann. § 33.02 (West 1985).

[207] *Id.*

[208] Tex. Pen. Code Ann. § 33.02 (West 1985).

[209] *See supra* Section III.A.

delineating the difference between conduct that should be penalized with prison time or not.

C. Error Message: Authority not Found

Even without a definitive answer as to which analysis courts should use or what amendments should be adopted, there are steps employers can take to protect themselves against litigation.[210] First, employers can draft comprehensive polices that explicitly delineate the appropriate access standards for employees to avoid litigation.[211] Next, employers could invest in computer systems that allow access to be broken down to different levels.[212] This would allow employers to keep employees from gaining access to data that they do not need to complete their tasks.[213] Employers also need plans in place for when employees leave.[214] This would include terminating remote access and making sure employees return all work-issued devices with access to any employer-related network.[215] Finally, employers should reiterate that employees are not to continue to access the work networks after their work is complete and they leave the company.[216]

V. UNPLUGGING

The issues with the CFAA will not disappear or become any less relevant. Instead, the differences between the interpretations will only continue to increase as technology continues to advance. While the parsing of words and individual circumstances make the CFAA tedious, the CFAA was intended to protect Americans in a way that no other law can do. The CFAA will only continue to become more important. Congress needs to amend the law as quickly as possible so the unbalanced prosecution of citizens can be leveled. If Congress does not act, eventually the Supreme Court needs to grant certiorari to determine an interpretation. The law needs to be used as it was intended instead of resulting in an

---

[210] Barbara A. Neider & Joseph S. Diedrich, *Not Authorized! Employees and Computer Fraud*, 89 WIS. LAW. 22 (2016).

[211] *Id.*

[212] *Id.* For example, there are different levels of security clearances for the Federal Bureau of Investigations. *Security Clearances for Law Enforcement*, FBI.gov https://www.fbi.gov/resources/law-enforcement/security-clearances-for-law-enforcement (last accessed Jan. 29, 2017). These clearance levels keep people from being able to access certain information, something employers may want to look into for all employees. *Id.*

[213] *Id.*

[214] *Id.*

[215] *Id.*

[216] Neider & Diedrich, *supra* note 210 at 22.

unequal playing field that defendants are currently a victim of — some courts punishing the same acts other deem acceptable.