CFAA and Van Buren: A Half-Measure for a Whole-ly Ineffective Statute

*Samantha Hourican**

I. INTRODUCTION

As computers became widely available and utilized throughout society, there was a clear need to propel government regulation of computer conduct.[1] While Congressional interest in computer legislation can be traced to the 1970s,[2] the major federal statute governing computer usage and crimes, the Computer Fraud and Abuse Act ("CFAA"),[3] was not passed until 1986.[4] Congress passed the first federal computer crime statute two years before passing the more

*Samantha Hourican, J.D. Class of 2023, Seton Hall University School of Law. I would like to thank Professor Jacob Elberg for his support and guidance throughout the writing process. A special thanks to the *Seton Hall Legislative Journal* members for their suggestions and dedication throughout the publication process, and to my parents, Donna and Thomas Hourican, and my sister, Kristina Hourican, for their love and encouragement.

1 *See* PETER G. BERRIS, CONG. RSCH. SERV., R46536, CYBERCRIME AND THE LAW: COMPUTER FRAUD AND ABUSE ACT (CFAA) AND THE 116TH CONGRESS 8–20 (2020) [*hereinafter* Berris, CYBERCRIME AND THE LAW].

2 *See* John K. Taber, On Computer Crime (Senate Bill S. 240), 1 Computer L. J. 517 (1978).

3 Off. of Legal Educ., *Prosecuting Computer Crimes*, U.S. DEP'T OF JUST. (2010), http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf.

4 *CFAA Background*, NACDL, https://www.nacdl.org/Content/CFAABackground (last visited Mar. 28, 2023).

expansive CFAA.[5] The inspiration for this legislation is often traced not to the years of Congressional interest in legislating in this area, but to *WarGames*, the 1983 thriller starring Matthew Broderick.[6] The movie's depiction of the vast dangers of the computer age is said to have sparked conversation amongst President Reagan and his advisors and factored into the intent behind Congress' passing of the CFAA.[7] Despite many Congressional amendments to the CFAA since its passage thirty years ago, the United States Supreme Court only addressed it for the first time in 2021 in *Van Buren v. United States*.[8]

In *Van Buren*, the Supreme Court reviewed 18 U.S.C. § 1030, the Computer Fraud and Abuse Act.[9] Under the CFAA, it is illegal to "access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter."[10] In *Van Buren*, the Court reversed the judgment of the Eleventh Circuit and held that while 18 U.S.C. § 1030(e)(6) covers those who "obtain information from particular areas in the computer [that] . . . their access does not extend," the act "does not cover those who . . . [had] improper motives for obtaining information that is otherwise available to them."[11] To support its ruling, the Court turned to the interpretation of the statutory language, specifically, "is not entitled so to obtain," the history of the statute, particularly Congress's choice to remove any reference to purpose in the statute, and policy considerations, that the government's argument would criminalize commonplace computer activity.[12]

Even after the Supreme Court's *Van Buren* decision, there is still uncertainty regarding the implementation and impact of the CFAA.[13]

---

5 *Id.*

6 WARGAMES (Metro-Goldwyn-Mayer Studios 1983); *see* Fred Kaplan, *'WarGames' and Cybersecurity's Debt to a Hollywood Hack*, N.Y. TIMES (Feb. 19, 2016), https://www.nytimes.com/2016/02/21/movies/wargames-and-cybersecuritys-debt-to-a-hollywood-hack.html (describing the popular tale that the birth of federal cybersecurity laws stems from President Ronald Reagan's concern over the movie "WarGames") [*hereinafter* Kaplan].

7 H.R. REP. NO. 98-894, at 10 (1984) (referencing *WarGames* in discussion of the necessity for computer fraud legislation); Kaplan, *supra* note 6.

8 Koray Bulut, *Supreme Court Ruling Narrows Scope of Computer Fraud and Abuse Act*, JD SUPRA, https://www.jdsupra.com/legalnews/supreme-court-ruling-narrows-scope-of-4163500/ (last visited Mar. 28, 2023).

9 Van Buren v. United States, 141 S. Ct. 1648, 1652 (2021).

10 18 U.S.C. § 1030(e)(6).

11 *Van Buren*, 141 S. Ct. at 1652.

12 *Id.* at 1655–61.

13 Scott L. Lashway & Matthew M.K. Stein, *Signs Inscribed on a Gate: The Impact of* Van Buren v. United States *on Civil Claims Under the Computer Fraud and Abuse Act*, 44 W. NEW ENG. L. REV. 109, 114 (2022).

First, there remains a lack of clarity as to what is considered a gate and what constitutes exceeding authorized access. Second, the fact that the statute is both criminal and civil and failed attempts to interpret the statute have caused problems in both civil and criminal cases. This Comment argues that the *Van Buren* decision does not go far enough to resolve the ambiguities of the CFAA and highlights the importance of reforming this outdated and overbroad statute. Part II of this Comment discusses the background and history of the CFAA. Part III then provides an analysis of the *Van Buren* decision to detail the two main problems with the CFAA mentioned above and proposes a two-factor statutory reform of the statute.

II. HISTORY OF THE CFAA AND THE *VAN BUREN* DECISION

The Computer Fraud and Abuse Act is the principal federal statute through which the unauthorized access and use of computers and networks of computers is prosecuted.[14] The CFAA covers seven different categories of prohibited conduct that "rang[e] from certain acts of computer trespass to unauthorized computer access with an intent to defraud".[15] As technology developed and computer usage became more mainstream, the CFAA has been amended to address emerging legal issues. Congress has broadened the CFAA's coverage through several amendments made in 1996, 2001, 2002, and 2008.[16] In its modern state, the CFAA prohibits: (1) sharing or retaining national security information obtained through unauthorized computer access;[17] (2) obtaining information through unauthorized computer access;[18] (3) trespassing on government computers;[19] (4) committing computer fraud;[20] (5) damaging a computer;[21] (6) trafficking passwords;[22] and (7) making extortionate threats to harm a computer based on information obtained through accessing a computer without authorization.[23]

---

14 Off. of Legal Educ., *Prosecuting Computer Crimes*, U.S. DEP'T OF JUST. (2010), http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf.

15 Berris, CYBERCRIME AND THE LAW, *supra* note 1, at 8.

16 *CFAA Background*, NAT'L ASS'N OF CRIM. DEF. LAWS, https://www.nacdl.org/Content/CFAABackground (last visited Mar. 28, 2023).

17 18 U.S.C. § 1030(a)(1).

18 18 U.S.C. § 1030(a)(2) (listing examples of information obtained in accordance with the statute such as information contained in a finical record of a financial institution, information from any department or agency of the United States, or information from any protected computer).

19 18 U.S.C. § 1030(a)(3).

20 18 U.S.C. § 1030(a)(4).

21 18 U.S.C. § 1030(a)(5).

22 18 U.S.C. § 1030(a)(6).

23 18 U.S.C. § 1030(a)(7).

Congress first drafted this statute in 1986 to specifically address computer-related hacking offenses rather than amend preexisting criminal statutes.[24] The CFAA covers two different types of hacking: (1) outside hacking, where an individual "access[es] a computer without authorization;" and (2) inside hacking, where an individual accesses a computer "with authorization" but obtains information that the individual is "not entitled *so* to obtain."[25] By doing so, this individual "exceeds authorized access."[26] While initially drafted as a hacking statute, the CFAA is both a civil and a criminal cybercrime law that has become much broader in scope since its initial drafting, prohibiting a wide range of computer-related conduct.[27] As a dual-use statute, the CFAA authorizes both the Department of Justice to criminally prosecute violators and the victims of cybercrime to civilly sue against perpetrators.[28] The CFAA's dual-use status is significant because even though the CFAA is a criminal statute, the majority of cases brought under the statute have been civil lawsuits between alleged victims and alleged perpetrators.[29] CFAA cases typically fall into one of two categories: (1) the employer-employee scenario where an employee, former or current, improperly accesses data with the intention of using said data to compete with the employer; and (2) the competitor scenario where companies violate the Terms of Service of a competitor's public-facing website by "scraping data" with the intent of using the scraped data for competitive purposes.[30]

---

24 Charles Doyle, CONG. RSCH. SERV., LSB97-1025, CYBERCRIME: AN OVERVIEW OF THE FEDERAL COMPUTER FRAUD AND ABUSE STATUTE AND RELATED FEDERAL CRIMINAL LAWS 1 (Oct. 15, 2014), https://www.everycrsreport.com/files/20141015_97-1025_31056cd16cc55cc39047e24e327a15875045157f.pdf.

25 18 U.S.C. § 1030(a)(1); 18 U.S.C. § 1030(e)(6) (emphasis added); *see* Melanie Assad, *Van Buren v. United States: An Employer Defeat or Hacker's Victory – Or Something in Between*, 21 UIC REV. INTELL. PROP. L. 166, 181 (2022).

26 18 U.S.C. § 1030(e)(6).

27 Berris, CYBERCRIME AND THE LAW, *supra* note 1, at 1–4.

28 Lawrence L. Muir, Jr.*, Revising the CFAA: How Stronger Domestic Cybercrime Law Can Improve International Cybersecurity*, GEO. J. INT'L AFFS. (May 7, 2015), https://web.archive.org/web/20201201151406/https://www.georgetownjournalofinternationalaffairs.org/online-edition/revising-the-cfaa-how-stronger-domestic-cybercrime-law-can-improve-international-cybersecurity [https://www.georgetownjournalofinternationalaffairs.org/online-edition/revising-the-cfaa-how-stronger-domestic-cybercrime-law-can-improve-international-cybersecurity].

29 Mark Rasch, *After Van Buren, Are Data Scraping Cases Barred*?, SEC. BOULEVARD (June 25, 2021), https://securityboulevard.com/2021/06/after-van-buren-are-data-scraping-cases-barred/.

30 *Id*.

The CFAA was enacted over three decades ago at a time when very "few people had access to computers, let alone had one of their own."[31] While the CFAA has developed and adapted over time, it is a notoriously broad and controversial statute[32] that many have described as poorly drafted.[33] In the decades following its passage, however, as detailed below, courts have not only interpreted the CFAA broadly, effectively slowing the development of computer security and undermining the law's purpose,[34] but have also interpreted the CFAA inconsistently, resulting in a long-standing circuit split.[35]

Critics argue that this unclear and vast statute threatens researchers and other individuals who utilize information that is freely accessible in ways that may be unapproved.[36] Legal scholars have argued for years that the language of this statute is not only too broad but also encompasses far too many computer-related activities.[37] Many of the activities covered by the CFAA are not even considered malicious hacking, which is the crime that the statute was designed to address.[38] This is especially dangerous when considering the spectrum of penalties available under the CFAA. Those who violate this statute, depending on the subsection at issue, can be subject to penalties ranging from fines to up to five, ten, or twenty years in prison.[39] It is also commonly argued

31 Dennis Fisher, *Supreme Court to Review CFAA for the First Time*, DECIPHER, (Apr. 20, 2020), https://duo.com/decipher/supreme-court-to-review-cfaa-for-first-time.

32 Adi Robertson, *The Supreme Court Pared Down a Controversial Anti-Hacking Law*, THE VERGE, (June 5, 2021, 9:00 AM), https://www.theverge.com/2021/6/5/22491859/supreme-court-van-buren-cfaa-hacking-law-scope-narrowed.

33 Grant Burningham, *The Most Hated Law on the Internet and Its Many Problems*, NEWSWEEK (Apr. 16. 2016, 2:20 PM), https://www.newsweek.com/most-hated-law-internet-and-its-many-problems-cfaa-448567; Justin Peters, *Congress Has a Chance to Fix Its Bad "Internet Crime" Law*, SLATE (Apr. 24, 2015, 5:47 PM), https://slate.com/technology/2015/04/aarons-law-why-its-needed-to-fix-the-horrendously-bad-cfaa.html; Press Release, Ron Wyden, U.S. Senate, Wyden Statement on SCOTUS Van Buren v. United States Decision, (June 3, 2021), https://www.wyden.senate.gov/news/press-releases/wyden-statement-on-scotus-van-buren-v-united-states-decision.

34 Brief for the EFF as Amicus Curiae Supporting Petitioners at 4, Van Buren v. US, 141 S. Ct. 1648 (2021), https://www.eff.org/files/2020/07/08/19-783_eff_security_researchers_amici_brief_.pdf.

35 *See, e.g.*, Zoe Lofgren & Ron Wyden, *Introducing Aaron's Law, A Desperately Needed Reform of the Computer Fraud and Abuse Act*, WIRED (June 20, 2013, 9:30 AM), https://www.wired.com/2013/06/aarons-law-is-finally-here/.

36 Robertson, *supra* note 32.

37 Fisher, *supra* note 31.

38 Fisher, *supra* note 31.

39 Berris, CYBERCRIME AND THE LAW, *supra* note 1, at 20–22.

that the breadth and vagueness of the CFAA, exasperated by the statute's lack of adequate definitions, allows for prosecutorial abuse.[40] Along with allowing for abusive prosecution tactics, many argue that the CFAA violates the Due Process Clause of the Fifth Amendment, which requires that defendants are put on notice that the actions they choose to engage in are illegal and that the statute that governs those actions provides clear guidance regarding enforcement to law enforcement officials.[41]

While there are several key points of the statute that elicit controversy, the clause at issue in this Comment is the statement in the first category, 18 U.S.C. § 1030(a)(2), that anyone who "intentionally accesses a computer without authorization or exceeds authorized access" to obtain information is in violation of the CFAA.[42]

The exact meaning and correct interpretation of this aspect of the statute has long been debated. In fact, *Van Buren v. United States* was the first instance where the Supreme Court conducted a review of the CFAA.[43] In *Van Buren*, a former police sergeant, Nathan Van Buren, utilized a law enforcement computer database to run a license plate search.[44] While Officer Van Buren had the required authorization to access and use this database, he did so for improper purposes, in exchange for money, and therefore not in furtherance of his role as a law enforcement officer.[45] While his conduct blatantly violated police department policy, the issue presented to the Court was whether or not Officer Van Buren also violated the CFAA under § 100(e)(6), which prohibits exceeding authorized access to a computer or computer network.[46] The CFAA does not clearly define "exceeding authorized access" and courts at all levels have disagreed for years over how narrowly or broadly to construe the phrase "exceeding authorized access."[47]

---

40 *See, e.g.*, Lofgren & Wyden, *supra* note 35.

41 Tor Eckland, *How to Reform the Outdated Federal Anti-Hacking Law*, THE CHRISTIAN SCI. MONITOR (March 24, 2017), https://www.csmonitor.com/World/Passcode/Passcode-Voices/2017/0324/How-to-reform-the-outdated-federal-anti-hacking-law.

42 18 U.S.C. § 1030(a)(2).

43 Sehseh Sanan, *Implications of* Van Buren v. United States *and the Reach of the CFAA*, N.Y. STATE SCI. & TECH. L. CTR. (Jan. 6, 2021), https://nysstlc.syr.edu/implications-of-van-buren-v-united-states-and-the-reach-of-the-cfaa/.

44 Van Buren v. United States, 141 S. Ct. 1648, 1652 (2021).

45 *Id.* at 1652–53.

46 *Id*. at 1653.

47 Raymond Cooper et al., *SCOTUS Decision Significantly Impacts Data Operations for U.S. Businesses*, JD SUPRA (June 8, 2021), https://www.jdsupra.com/legalnews/scotus-decision-significantly-impacts-1583064/; *see* 18 U.S.C. § 1030(e)(6) ("[T]he term 'exceeds authorized access' means to access a computer with authorization and to use

Varied judicial interpretations, along with extensive case law, clearly illustrate the problematic construction of the CFAA and the need for clarification that effectively addresses modern issues in cybercrime.[48] The First, Fifth, Seventh, and Eleventh Circuits have interpreted the CFAA to cover both Terms of Service violations and acceptable use policies set by employers on company computers, while other circuits, particularly the Second, Fourth, Sixth, and Ninth view these interpretations of the CFAA as overbroad.[49] The narrow view taken by these courts interprets the CFAA as not imposing criminal liability on a person who is authorized to access information on a computer but then uses the information they access for an improper purpose.[50]

such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter."); *see also* S. REP. NO. 104-357, at 11 (1996) ("In sum, under the bill, insiders, who are authorized to access a computer, face criminal liability only if they intend to cause damage to the computer, not for recklessly or negligently causing damage. By contrast, outside hackers who break into a computer could be punished for any intentional, reckless, or other damage they cause by their trespass.").

48 *See* Lofgren & Wyden, *supra* note 35; *see also* Katherine M. Field, *Agency, Code, or Contract: Determining Employees' Authorization Under the Computer Fraud and Abuse Act*, 107 MICH. L. REV. 819, 821 (2009).

49 *Compare* United States v. John, 597 F.3d 263, 271 (5th Cir. 2010) (finding that the defendant exceeded authorized access when she accessed company data for a purpose other than that for which she was given access to the information), United States v. Rodriguez, 628 F.3d 1258, 1260 (11th Cir. 2010) (determining that a Social Security Administration employee exceeded authorized access by viewing the personal records of his ex-wife and other acquaintances), Int'l Airport Ctrs., L.C.C. v. Citrin, 440 F.3d 418, 419-20 (7th Cir. 2006) (finding a user exceeded authorized access when he permanently deleted company files from his work laptop after breaching his employment contract), *and* EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 581-83 (1st Cir. 2001) (finding former employees exceeded authorized access when they disclosed proprietary information in violation of their former employer's broad confidentiality agreement), *with* Royal Truck & Trailer Sales and Servs., Inc. v. Kraft, 974 F.3d 756, 761 (6th Cir. 2020) (holding that "one who is authorized to access a computer does not exceed her authorized access by violating an employer's restrictions on the *use* of information once it is validly accessed"); Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1066-67 (9th Cir. 2016), *cert. denied*, 138 S. Ct. 313 (2017) (holding that a person can exceed authorized access if permission to access a computer has been revoked but "a violation of the terms of use of a website—without more—cannot establish liability under the CFAA"), United States v. Valle, 807 F.3d 508, 523 (2d Cir. 2015) (finding that defendant did not exceed his authorized access when he used his access to law enforcement databases to do a search that had no law enforcement purpose), WEC Carolina Energy Sols. v. Miller, 687 F.3d 199, 206 (4th Cir. 2012) (determining that the CFAA does not cover violations of employee use policies or related misappropriation), *and* LVRC Holdings LLC v. Brekka, 581 F.3d 1127 (9th Cir. 2009).

50 Brian F. McEvoy et al., *SCOTUS Set to Resolve Circuit Split and Decide Scope of Computer Fraud and Abuse Act Prosecutions*, 10 NAT. L. REV. 119 (2020).

In its *Van Buren* holding, the Supreme Court resolved this split.[51] The Court adopted the narrow view, holding that while 18 U.S.C. § 1030(e)(6) covers those who obtain information from areas of the computer that their access does not extend, it does not cover those who had improper motives for obtaining information to which that they otherwise had access.[52] The focal point for the Court was how and by what means the employer prohibited its employees from accessing particular information that was stored electronically on the employer's computers.[53] The Court found that, "if a person has access to information stored in a computer—e.g., in 'Folder Y,' from which the person could permissibly pull information—then he does not violate the CFAA by obtaining such information, regardless of whether he pulled the information for a prohibited purpose."[54] Van Buren argued that the phrase "is not entitled *so* to obtain" in the statute refers solely to information that an individual is not allowed to obtain by means of using a computer that they already have authorization to access.[55] The Government, however, argued that the phrase refers to information one was not allowed to "obtain in the particular manner or circumstances in which he obtained it."[56] Under the Government's more expansive interpretation, people may be punished if they have improper motives for obtaining information that they have authorized access to.[57]

The *Van Buren* Court rejected the Government's argument and adopted a gates-up-or-down inquiry.[58] A gates-up-or-down inquiry means that an individual is either authorized to access something or is not.[59] If gates are up, the individual does not have access to that computer or to that area of the computer, and accessing it would be a

51 Nathan Conway et. al., *U.S. Supreme Court Resolves Circuit Split on Meaning of "Exceeds Authorized Access" in Computer Fraud and Abuse Act*, JD SUPRA (June 8, 2021), https://www.jdsupra.com/legalnews/u-s-supreme-court-resolves-circuit-8118018/#2.

52 *Van Buren*, 141 S. Ct. at 1662.

53 Brent Crossrow & Usama Kahf, *SCOTUS Decision Ushers in the "Gates Up or Down" Era for Employers Seeking to Protect Workplace Computers and ESI - The Post-Van Buren Workplace and the Computer Fraud and Abuse Act*, JD SUPRA (July 6, 2021), https://www.jdsupra.com/legalnews/scotus-decision-ushers-in-the-gates-up-9387318/.

54 *Id*.

55 *Van Buren*, 141 S. Ct. at 1654.

56 *Id*.

57 *See* Raymond Cooper et al., *SCOTUS Decision Significantly Impacts Data Operations for U.S. Businesses*, JD SUPRA (June 8, 2021), https://www.jdsupra.com/legalnews/scotus-decision-significantly-impacts-1583064/.

58 *Van Buren*, 141 S. Ct. at 1658.

59 *Id.* at 1658–59.

violation of the CFAA.[60] However, if gates are down, the individual can access that computer or that area of the computer without fear of penalty under the CFAA.[61] In the words of the *Van Buren* Court, a person would have to enter "particular areas of the computer—such as files, folders, or databases—that are off-limits to him."[62] While the *Van Buren* Court discusses a gates-up-or-down inquiry, therefore clarifying the scope of the definition of "exceeding authorized access," it fails to clarify what constitutes a gate.[63] A gate is a restriction that would keep an individual from having authorized access to a computer or an area of a computer.[64] Some restrictions, such as username and password, are definitively considered gates, but it is unclear whether other restrictions, such as Terms of Service or IP address blocks, would also be considered gates under the CFAA.[65]

While *Van Buren* states a person needs to bypass a gate to violate the CFAA, the Court punts on what type of gates are covered under the CFAA, therefore failing to clarify what it means to have "authorized access."[66] In a footnote, the *Van Buren* Court explained that "[for] present purposes, we need not address whether this inquiry turns only on technological (or 'code-based') limitations on access, or instead also looks to limits contained in contracts or policies."[67] While footnote eight states that choosing a preferable form of authorization is not necessary in this case, the Court still discussed that there are two different potential theories of authorization to choose from: the contract-based approach and the code-based approach.[68] Each of these approaches portrays a different view of the type of gates that are covered by the CFAA. The contract-based approach to determining whether information is considered *gates-down* or not allows for the creation of

60 *See* Orin Kerr, *The Supreme Court Reins in the CFAA in Van Buren*, LAWFARE (June 9, 2021, 9:04 PM), https://www.lawfareblog.com/supreme-court-reins-cfaa-van-buren.

61 *Id.*

62 *Van Buren*, 141 S. Ct. at 1662.

63 *Id.* at 1659 n. 8.

64 Kerr, *supra* note 60.

65 James X. Dempsey, *Cybersecurity Law Fundamentals: Updates to Chapter 2 Criminal Law*, THE INT'L ASS'N OF PRIV. PROFESSIONALS (Oct. 25, 2021), https://cybersecuritylawfundamentals.com/chapter-2.

66 Kerr, *supra* note 60.

67 *Van Buren*, 141 S. Ct. at 1659 n. 8.

68 *Id.*; Peter Pizzi, *United States: Resolving a Circuit Split, Van Buren Reduces CFAA's Scope, But Leaves Options for Pursuing Disloyal Employees, Less so for Victims of Web-Scraping*, MONDAQ (Aug. 17, 2021), https://www.mondaq.com/unitedstates/contracts-and-commercial-law/1102228/resolving-a-circuit-split-van-buren-reduces-cfaa39s-scope-but-leaves-options-for-pursuing-disloyal-employees-less-so-for-victims-of-web-scraping.

authorization limitations through company or contract policies, or even verbal or written restrictions regarding how a computer can be used.[69] The code-based approach, on the other hand, hinges on the use of computer codes, such as passwords, to bring *gates down* on particular information, therefore "making access to that data 'unauthorized' under the CFAA, along the lines of traditional hacking."[70]

The contract-based approach considers conduct to be unauthorized whenever a user violates a relevant contract.[71] This approach, therefore, requires a contract to exist, whether implicitly or explicitly, that defines and often limits the authorization of an individual user.[72] This approach is often applied in cases where there is a Terms of Service contract or agreement between internet providers and computer users and in cases where there is an employee handbook or contract between employers and employees.[73] The code-based approach would only attach liability when someone circumvents a technological measure, whether it be a password or some other technological or physical security measure.[74] While no courts had adopted the code-based approach prior to the Ninth Circuit's 2019 decision in *HiQ Labs, Inc. v. LinkedIn Corp.*, it has gained more support and legislative attention in recent years.[75]

One particular instance of this attention is the proposed Aaron's Law Act of 2013, which was a bill named for internet activist Aaron Swartz, who committed suicide while he was facing CFFA charges totaling fifty years in prison for violating an academic repository's Terms of Service by downloading articles he was authorized to access, but not to download and share.[76] Aaron's Law aimed to address

69 Pizzi, *supra* note 68.

70 Pizzi, *supra* note 68.

71 Katherine Mesenbring Field, *Agency, Code, or Contract: Determining Employees' Authorization Under the Computer Fraud and Abuse Act*, 107 MICH. L. REV. 819, 827 (2009).

72 *Id.*

73 *Id.*

74 *The Computer Fraud and Abuse Act: Circuit Split and Efforts to Amend*, BERKLEY TECH. L. J. (Mar. 31, 2014), https://btlj.org/2014/03/the-computer-fraud-and-abuse-act-circuit-split-and-efforts-to-amend/.

75 Michael J. O'Connor, *Standing Under the Computer Fraud and Abuse Act*, 124:3 PENN STATE L. REV. 743, 753 (2020); *see* HiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985, 1001 (9th Cir. Sept. 9, 2019) (suggesting that "authorization is only required for password-protected sites or sites that otherwise prevent the general public from viewing the information"); *see, e.g.*, Patricia L. Bellia, *A Code-Based Approach to Unauthorized Access Under the Computer Fraud Abuse Act*, 84 GEO. WASH. L. REV. 1442 (2016).

76 *The Computer Fraud and Abuse Act: Circuit Split and Efforts to Amend*, *supra* note 74.

fundamental issues with the CFAA by proposing several fixes, most notably clarifying the language of the statute to ensure that exceeding authorized access would refer only to individuals who circumvent technological or physical controls.[77] Because Aaron never bypassed any technological barriers, under a code-based approach as proposed by Aaron's Law rather than a contract-based approach, his conduct would not have been actionable.[78] The approach that is applied determines what the definition of "authorized access" under the CFAA is and therefore greatly impacts the type and nature of conduct to which liability attaches under the CFAA. The uncertainty fostered by a lack of clarity regarding which approach is proper makes this statute ineffective.

III. ANALYSIS

A. Importance of Adopting a Narrower Approach

Until the *Van Buren* Supreme Court decision, "[y]ou could indict a ham sandwich with the CFAA," as Jeff Moss, the founder of the Black Hat and DEF CON security conferences, once stated.[79] While the *Van Buren* decision clarifies some of the ambiguities of the CFAA, it fails to resolve issues that make the Act incredibly difficult to implement effectively. For example, the *Van Buren* Court clarified that the purpose behind the action is irrelevant when determining if an individual has exceeded authorized access or not,[80] but actively refused to clarify what constitutes "authorized access."[81] The Court's failure to determine whether the contract-based approach or the code-based approach is appropriate to apply when determining what "authorized access" means under the CFAA guarantees that post-*Van Buren* decision applications of the CFAA will remain unclear and disjointed. Although *Van Buren* was a step in the right direction, without a clear definition for "authorized access" or clarification on what types of gates are covered by the statute's gates-up-gates-down framework, the application of the CFAA will continue to be unsettled and inconsistent.

---

77 Aaron's Law Act, H.R. 2454, 113th Cong. § 1 (2013).

78 *See* Thomas Brewster, *Aaron's Law is Doomed Leaving US Hacking Law 'Broken'*, FORBES (Aug. 6, 2014, 9:39 AM), https://www.forbes.com/sites/thomasbrewster/2014/08/06/aarons-law-is-doomed-leaving-us-hacking-law-broken/.

79 Riana Pfefferkorn*, America's Anti-Hacking Laws pose a Risk to National Security*, THE BROOKINGS INST. (Sept. 7, 2021), https://www.brookings.edu/techstream/americas-anti-hacking-laws-pose-a-risk-to-national-security/.

80 Van Buren v. United States, 141 S. Ct. 1648, 1662 (2021).

81 *Id.* at 1659 n. 8.

To support its decision, however incomplete it turned out to be, the *Van Buren* Court turned to policy considerations.[82] While some argue that the CFAA has been a useful litigation tool for employers when sensitive information accessed via computer is misappropriated or compromised,[83] the Court argued that failing to adopt this narrow approach would criminalize commonplace computer activity.[84] Others agree with this notion, such as Esha Bhandari, the American Civil Liberties Union's Speech, Privacy, and Technology Project deputy director, who stated that the *Van Buren* decision "is an important victory for civil liberties and civil rights enforcement in the digital age."[85] Electronic Frontier Foundation staff members Aaron Mackey and Kurt Opsahl also characterized the *Van Buren* decision as a victory, by stating that the Court "provided good language that should help protect researchers, investigative journalists, and others."[86] While this is a genuine concern, failing to determine whether the *Van Buren* Court's gates-up-gates-down approach is code-based or contract-based leaves both researchers and common computer users at risk. Federal courts are split on whether someone who violates a contract-based gate, such as a Terms of Service agreement, is subject to liability under the CFAA.[87] Failing to limit this approach to code-based gates permits courts to criminalize contract law.[88]

This failure to define authorization further emphasizes that while the *Van Buren* decision provides some clarity, it does not go nearly far enough to allow for consistent application of this problematic statute. One aspect of *Van Buren* that will require further clarification relates to

---

82 *Id*. at 1661.

83 Aime Dempsey, *SCOTUS Favors Narrower Reading of CFAA "So" It Does Not Cover Misuse of Authorized Access*, EPSTEIN BECKER GREEN: TRADE SECRETS AND CONFIDENTIAL INFORMATION (June 17, 2021), https://www.tradesecretsandemployeemobility.com/2021/06/articles/trade-secrets-and-confidential-information/scotus-favors-narrower-reading-of-cfaa-so-it-does-not-cover-misuse-of-authorized-access/.

84 *Van Buren*, 141 S. Ct. at 1661 (stating that failing to narrow the approach could lead to criminalization of commonplace computer activity such as sending a personal email or reading the news from a work computer).

85 *Statement on Supreme Court Decision Removes Hurdles to Online Civil Rights Testing and Research*, ACLU (June 3, 2021, 12:30 PM), https://www.aclu.org/press-releases/statement-supreme-court-decision-removing-hurdles-online-civil-rights-testing-and.

86 Robertson, *supra* note 32.

87 PETER BERRIS, CONG. RSCH. SERV., LSB10423, FROM CLICKWRAP TO RAP SHEET: CRIMINAL LIABILITY UNDER THE CONSUMER FRAUD AND ABUSE ACT FOR TERMS OF SERVICE VIOLATIONS 2 (Dec. 21, 2020) [*hereinafter* Berris, FROM CLICKWRAP TO RAP SHEET], https://crsreports.congress.gov/product/pdf/LSB/LSB10423/6s.

88 Eckland, *supra* note 41.

its holding that there is a "gates-up-or-down inquiry" involved in examining both what "exceeds authorization" and what is "without authorization."[89] While the Court stated that the inquiry applies in both situations, it does not address what qualifies as a gate.[90] Even though *Van Buren* does not resolve it, there is a case from the Ninth Circuit that is on point for helping to resolve this issue: *HiQ Labs, Inc. v. LinkedIn Corp*.[91]

On June 14, 2020, about two weeks after the *Van Buren* decision, the Supreme Court issued a summary disposition in the *HiQ Labs,* vacating the prior judgment and remanding the case to be reassessed in light of the *Van Buren* decision.[92] The Supreme Court's decision not to address this case is problematic as it provided the Court the perfect opportunity to further clarify the CFAA and address what constitutes a gate when attempting to interpret the "without authorization" statutory language.[93] Also, a Supreme Court decision would be binding precedent for lower courts and therefore would be a further step towards clarifying the CFAA and promoting consistent application.[94]

B. Proposed Statutory Reform

The shortcomings of the *Van Buren* decision highlight the great need for reform within the CFAA statute. The statutory reform this Comment proposes is two-fold: (1) establish that mere breaches of Terms of Service or contracts are not automatic violations of the CFAA, and (2) decouple the civil and criminal aspects of the CFAA by clarifying the language and providing some supplemental definitions of the statutory language.

1. Resolving the Circuit Split Regarding the Definition of "Authorization" by Adopting a Code-Based Approach

In the cybersecurity industry, one of the most prolific complaints about the CFAA is that it criminalizes normal, everyday behavior.[95] One

89 Sarah Rippy & Nicole Sakin, *Van Buren: The Implications of What is Left Unsaid*, IAPP (June 18, 2021), https://iapp.org/news/a/van-buren-the-implications-of-what-is-left-unsaid/.

90 *Id*.

91 HiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985 (9th Cir. 2019).

92 Mark P. Kesslen, et. al, *Supreme Court Grants Certiorari in Web Scraping Case HiQ v. LinkedIn*, LOWENSTEIN SANDLER: CLIENT ALERT, (June 15, 2021), https://www.lowenstein.com/news-insights/publications/client-alerts/supreme-court-grants-certiorari-in-web-scraping-case-hiq-v-linkedin-tech-groupwhite-collar.

93 Rippy & Sakin, *supra* note 89.

94 Kesslen, *supra* note 92.

95 Eckland, *supra* note 41.

clear example of this is the criminalization of simply looking for vulnerabilities in publicly accessible servers.[96] Along the lines of that complaint, some Department of Justice CFAA prosecutions have frightening implications for all Americans, regardless of their level of hacking skill.[97] In its current state, "[l]ying about one's age on Facebook, or checking personal email on a work computer, could violate this felony statute."[98] Many view the *Van Buren* decision as a step towards assuaging the fears of some citizens in this context.[99] Particularly, the *Van Buren* decision is great news for journalists, researchers, bug bounty hunters, and various other individuals who could access information in a myriad of legitimate ways but were still at risk of criminal prosecution under the broader interpretation of the CFAA.[100] However, the *Van Buren* decision still leaves open questions on whether contractual limits, such as Terms of Service, are covered under the CFAA, which will likely be addressed and settled via litigation in coming years.[101] If the CFAA decided to criminalize Terms of Service violations, it would "turn[] each website into its own criminal jurisdiction and each webmaster into his own legislature"—and each website's Terms of Service into "a law unto itself."[102]

The CFAA provision in question, "exceeds authorized access," has been interpreted to prevent an individual from visiting or using a website in such a way that violates the website's Terms of Service.[103] Allowing a simple violation of a website's Terms of Service to be prosecuted under the CFAA has detrimental consequences in several areas. One clear example of this is audit testing to uncover racial discrimination. The Federal Government has long encouraged the use of audit testing to expose racial discrimination, and this process has

96 Eckland, *supra* note 41.

97 Eckland, *supra* note 41.

98 *See, e.g.*, Zoe Lofgren & Ron Wyden, Opinion, *Introducing Aaron's Law, A Desperately Needed Reform of the Computer Fraud and Abuse Act*, Wired (June 20, 2013, 9:30 AM), https://www.wired.com/2013/06/aarons-law-is-finally-here/.

99 *See, e.g.*, Udbhav Tiwari, *The Van Buren Decision is a Strong Step Forward for Public Interest Research Online*, MOZILLA: OPEN POL'Y & ADVOC. BLOG (Jun. 4, 2021), https://blog.mozilla.org/netpolicy/2021/06/04/the-van-buren-decision-is-a-strong-step-forward-for-public-interest-research-online/.

100 *Id.*

101 *Id*.

102 Sandvig v. Barr, 451 F. Supp. 3d 73, 88 (D.D.C. 2020) (citing Emp. Div., Dep't of Hum. Res. of Or. v. Smith, 494 U.S. 872 (1990)).

103 *Sandvig v. Barr—Challenge to CFAA Prohibition on Uncovering Racial Discrimination Online*, ACLU (May 22, 2019), https://www.aclu.org/cases/sandvig-v-barr-challenge-cfaa-prohibition-uncovering-racial-discrimination-online.

proven to be crucial in offline areas such as housing and employment.[104] However, when it comes to online sources, uncovering discrimination requires audit testing, which is often in violation of the Terms of Service agreements of many websites.[105] Therefore, allowing a criminal penalty for violating Terms of Service may hamper crucial anti-discrimination efforts across a vast array of online platforms. This is just one example that highlights the importance of interpreting the CFAA narrowly and applying it only to code-based authorization.

Allowing CFAA actions for Terms of Service violations presents issues for both the civil and criminal aspects of the statute. The danger of allowing parties to bring civil actions for violations of Terms of Service under the CFAA is that it does not align with the goals of the statute. This is evident in the Court's choice to reject the Government's argument that the "exceeds authorized access" clause in the CFAA "incorporate[s] purpose-based limits contained in contracts and workplace policies."[106] The Court rejected this proposition because it recognized a "structural problem" in relation to the civil remedies available under the CFAA.[107] Justice Barrett expanded on this structural issue by discussing how the terms "damage" and "loss," which are prerequisites to civil actions under the CFAA, "focus on technological harms—such as the corruption of files of the type unauthorized users cause to computer systems and data."[108] If the statute was limited to the technological harms described by the definition of these terms, it would "make[] sense in a scheme 'aimed at preventing the typical consequences of hacking.'"[109] The definitions of "damage" and "loss" under the CFAA, however, are "ill-fitted . . . to remediating 'misuse' of sensitive information that employees may permissibly access using their computers."[110] By preventing actions based on Terms of Service violations, the statute maintains its legislative intent of addressing hacking crimes.

In terms of the criminal aspect of the CFAA, there is also an issue regarding notice. The public must be put on notice regarding actions that would violate criminal laws.[111] As the Court recognized, Terms of

104 *Id.*

105 *Id*.

106 *US Supreme Court Narrows Scope of Computer Fraud and Abuse Act in Van Buren*, COOLEY (Jun. 9, 2021), https://www.cooley.com/news/insight/2021/2021-06-09-us-supreme-court-computer-fraud-abuse-act-van-buren.

107 *Id.*

108 Van Buren v. United States, 141 S. Ct. 1648, 1660 (2021).

109 *Id*. at 1651.

110 *Id*.

111 U.S. CONST. amend. VI.

Service or Terms of Use agreements on websites do not provide notice sufficient to meet this requirement because these agreements are "often long, dense, and subject to change," and are often inconspicuous in smaller print and found at the bottom of webpages.[112] Users' lack of awareness that their activity is criminal unfairly leaves them vulnerable to prosecution. The Federal Government has argued that this is not a concern because it has promised not to pursue "garden-variety violations" of the CFAA.[113] By making this promise, the Government has admitted that it has the power and discretion to arrest nearly anyone under this statute, but that we should trust it to prosecute only the serious and harmful cases.[114] Expecting citizens to rely on the government to not execute its prosecutorial power is not sufficient to protect citizens' rights.

Along with the concern of overcriminalization and over-prosecution, imposing liability for terms of use violations has caused a significant chilling effect on security research that is highly innovative and socially useful.[115] This is because the CFAA imposes liability on actions that are not clearly tracking or hacking.[116] There is also a concern about businesses seeking criminal sanctions under the statute. If liability includes violations of Terms of Service agreements, businesses that seek criminal sanctions under the CFAA will likely be incentivized to put more time, money, and effort into protecting information behind various digital, code-based protections and through contracts such as explicit employment agreements.[117] This process results in additional effort and costs on behalf of businesses in the wake of fear of liability. The adverse effects this has on average citizens, researchers, and businesses could be remedied by clarifying and narrowing the CFAA by adopting a code-based rather than a contract-based approach.

For both the civil and criminal aspects of the CFAA, allowing actions for violations of Terms of Service presents significant concerns. While

112 Naomi Glens & Jamie Williams, *Federal Judge Rules It Is Not a Crime to Violate a Website's Terms of Service*, ELEC. FRONTIER FOUND. (Apr. 6, 2020), https://www.eff.org/deeplinks/2020/04/federal-judge-rules-it-not-crime-violate-websites-terms-service.

113 Peter J. Toren, *Supreme Court Needs to Clarify the Scope of the CFAA*, THE HILL: CONG. BLOG (Dec. 24, 2015, 3:00 PM), https://thehill.com/blogs/congress-blog/judicial/264061-supreme-court-needs-to-clarify-the-scope-of-the-cfaa.

114 *Id.*

115 Jonathan Keim, *Updating the Computer Fraud and Abuse Act*, FEDERALIST SOC'Y (Oct. 28, 2015), https://fedsoc.org/commentary/publications/updating-the-computer-fraud-and-abuse-act-1.

116 *Id.*

117 Muir, *supra* note 28.

the *Van Buren* Court addressed and interpreted the CFAA, it failed to take action that would resolve these issues. In rejecting one policy gate, but explicitly refraining from generally adopting a code-based approach to access restrictions, the ruling leaves much work for future courts, which will have to determine which, if any, policy gates are backed by the CFAA.[118] Under the contract-based approach, the employer or individual gives someone a login and password, granting them access to a computer database, but then tells them their access is limited to certain areas or publishes a policy restricting access to certain sites or files.[119] If courts adopt a contract-based model for "exceeds authorized access," then it is hard to distinguish between telling Officer Van Buren that he can access the GCIC database solely for law enforcement purposes (authorized access, but improper use) and, "if you do not intend to use the data for law enforcement purposes, you are not authorized to access the database or this computer at all" (permissions-based or contract-based restrictions).[120] The dichotomy of these scenarios shows the blurry lines that are created when adopting a contract-based approach.

> What the court is saying is that you can tell someone that they can be in (virtual) place A, or (virtual) place B, and if they are granted permission to be in place A but not B, their access to place B is in "excess" of their authorization, but you *can't* say that you can be in (virtual) place A, but only for specific purposes.[121]

Ultimately, by failing to adopt a code-based approach, everything becomes contract-based restrictions, and the problem that the *Van Buren* Court identifies and footnote eight mentions about Terms of Service remains unsolved.[122]

2. Decoupling the Civil and Criminal Aspects of the Statute and Altering the Language and Explanatory Definitions of Terms Used in the CFAA

The CFAA's dual-use nature exacerbates problems of inconsistent and questionable statutory interpretation. This is evidenced by the fact that the CFAA allows prosecution, with sentences that can be quite extensive, for acts as innocent or benign as violating a website or

118 Will Duffield, *Van Buren Decision is a Step in the Right Direction*, CATO INST.: CATO AT LIBERTY BLOG (June 14, 2021, 9:07 AM), https://www.cato.org/blog/van-buren-decision-step-right-direction.

119 Rasch, *supra* note 29.

120 Rasch, *supra* note 29.

121 Rasch, *supra* note 29.

122 Rasch, *supra* note 29.

vendor's Terms of Service agreement, to those as harmful or malicious as breaking into computers to steal credit card numbers.[123] The CFAA's dual-use nature has even resulted in a circuit split among the Federal Circuit Courts of Appeals. This divide originates from courts' use of criminal statutory interpretation in civil actions, which is applied when the statute is both criminal and civil and the interpretation of a singular statute has to be consistent.[124] As a result, while the intention was that the statute is construed consistently, inconsistent and inefficient interpretation of the statute has run rampant in both civil and criminal cases.[125] This section argues that problems would be alleviated by decoupling the statute and creating separate criminal and civil statutes with distinct language and definitions of key terms.

While the CFAA is currently a joint civil and criminal statute, by decoupling the causes of action and applying a narrower interpretation to criminal sanctions and a broader interpretation to civil-only sanctions, both categories of cases can be dealt with more effectively, and fear of overcriminalization can be greatly reduced. Because sanctions that are associated with criminal convictions are more severe than those associated with civil convictions, the procedural rules and interpretive norms that govern criminal causes of action are more favorable to defendants.[126] Presumptively, Congress is aware that civil and criminal cases are different.[127] Along with this, Congress explicitly and intentionally gives a provision of both civil and criminal significance and therefore intends it to be read in both circumstances.[128] There is an argument that since criminal and civil are separate scenarios, with different procedures and requirements, the statute was meant to be applied differently in each scenario.[129] However, allowing for the same statute to be interpreted in multiple different ways in different contexts

123 James Hendler, *It's Time to Reform the Computer Fraud and Abuse Act,* SCIENTIFIC AM. (Aug. 6, 2013), https://www.scientificamerican.com/article/its-times-reform-computer-fraud-abuse-act/.

124 Muir, *supra* note 28.

125 Muir, *supra* note 28.

126 Ryan D. Doerfler, *Can a Statute Have More Than One Meaning?*, 94 N.Y.U. L. REV. 213, 243–44 (2019).

127 *See* Daniel Epps, *The Consequences of Error in Criminal Justice*, 128 HARV. L. REV. 1065, 1067–68 (2015) ("'[B]etter that ten guilty persons escape, than that one innocent suffer' is perhaps the most revered adage in the criminal law, exalted by judges and scholars alike as a cardinal principle of Anglo-American jurisprudence.").

128 *See, e.g.*, 15 U.S.C. § 77(b), (d) (2012) (providing criminal and civil remedies, respectively, for Securities Act violations); 18 U.S.C. §§ 1963–64 (2012) (providing civil and criminal remedies, respectively, for RICO violations); 33 U.S.C. §§ 1319(b)–(c) (2012) (providing civil and criminal remedies, respectively, for Clean Water Act violations).

129 Doerfler, *supra* note 126, at 244.

would come dangerously close to statutory "invent[ion]" rather than statutory "interpretat[ion]."[130] While language is often not used uniformly across different statutes,[131] courts have more rigid standards for language within the same statute, as "a statute is not a chameleon," and "its meaning does not change from case to case."[132]

Courts' attempts to construe this language and the differing rules they must use to do so for criminal and civil cases make it difficult for the CFAA to be effective. One rule that presents an interpretation problem for the CFAA is the rule of lenity.[133] The rule of lenity states that for criminal statutes, any ambiguities relating to the scope of the statute are to be resolved in favor of lenity, meaning that all ambiguities are to be read in a light most favorable to the defendant.[134] Because the CFAA is a criminal statute, the rule of lenity applies.[135] Therefore, not only do all of the statute's many ambiguities have to be resolved in favor of defendants, but also the application of this rule provides forceful support for the argument that the CFAA should be interpreted more narrowly.[136] The impact of the rule of lenity calls for a more narrow interpretation of the CFAA, especially since the statute has both criminal and civil components.[137] Since it is a dual-use statute, the breadth or

130 Clark v. Martinez, 543 U.S. 371, 378 (2005).

131 *See, e.g.*, Util. Air Regulatory Grp. v. EPA, 134 S. Ct. 2427, 2441–42 (2014) (noting that "air pollutant" has different meanings in different parts of the Clean Air Act); Wachovia Bank, N.A. v. Schmidt, 546 U.S. 303, 313–14 (2006) (noting that "located" has different meanings in different parts of the National Bank Act); Gen. Dynamics Land Sys., Inc. v. Cline, 540 U.S. 581, 595–97 (2004) (noting that "age" has different meanings in different parts of the ADEA); United States v. Cleveland Indians Baseball Co., 532 U.S. 200, 212–13 (2001) (noting that "wages paid" has different meanings in different parts of Title 26); Robinson v. Shell Oil Co., 519 U.S. 337, 343–44 (1997) (noting that "employee" has different meanings in different parts of Title VII); District of Columbia v. Carter, 409 U.S. 418, 420–21 (1973) (noting that "state or territory" has different meanings in different parts of Title 42).

132 Carter v. Welles-Bowen Realty, Inc., 736 F.3d 722, 730 (6th Cir. 2013) (Sutton, J., concurring); *see, e.g.*, United States v. Santos, 553 U.S. 507, 522 (2008) (plurality opinion) ("[T]he proposition that one undefined word, repeated in different statutory provisions, can have different meanings in each provision . . . is worlds apart from giving the same word, *in the same statutory provision*, different meanings *in different factual contexts*."), *superseded by statute*, 18 U.S.C. § 1956 (2009); Leocal v. Ashcroft, 543 U.S. 1, 12 n.8 (2004) ("[W]e must interpret the statute consistently . . . .").

133 Derek Borchardt & Michael F. Buchanan, *The Supreme Court Punts on Clarifying the Computer Fraud and Abuse Act*, PATTERSON BELKNAP: DATA SECURITY LAW BLOG (Oct. 16, 2017), https://www.pbwt.com/data-security-law-blog/the-supreme-court-punts-on-clarifying-the-computer-fraud-and-abuse-act.

134 *See* United States v. Bass, 404 U.S. 336, 347 (1971); United States v. Santos, 553 U.S. 507, 514 (2008).

135 Borchardt & Buchanan, *supra* note 133.

136 Borchardt & Buchanan, *supra* note 133.

137 *See* Berris, CYBERCRIME AND THE LAW, *supra* note 1, at 25.

narrowness of interpretation in the criminal component directly impacts the civil component as well.[138] This is because, while the rule of lenity typically only applies to criminal laws, where the civil and criminal counterparts of the CFAA have identical statutory language, the language has to be interpreted in the same way.[139] The Ninth Circuit reasoned:

> [t]he government's construction of the statute 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 1984, meant to criminalize conduct beyond that which is inherently wrongful, such as breaking into a computer.[140]

This brings up a "path dependence" problem, meaning that there is a concern that identical language could be given different constructions and interpreted differently depending on whether a particular case is in a civil or criminal context.[141] A very similar issue arises when considering the impact of a court that first interprets the statute in a civil case and chooses to adopt a broader construction in line with the remedial purpose of the statute.[142] If this broad construction does not bind future criminal CFAA cases, the problematic result of dual construction of the same statute is likely.[143] Alternatively, if the broad civil precedent does in fact bind the interpretation of the statute in preceding criminal cases, the purpose and effect of the rule of lenity will be impacted, and the broad judicial construction will likely lead to increased criminal liability.[144] This "criminalization-by-remedial-construction," which is often referred to as "statutory inflation," raises concerning questions about the law's devotion to the principle of legality: "the notion that criminal conduct should be legislatively defined with the greatest possible specificity."[145]

While the *Van Buren* decision takes a step towards preventing the attachment of criminal penalties to an excessive amount of

138 *See* Borchardt & Buchanan, *supra* note 133.

139 Borchardt & Buchanan, *supra* note 133.

140 United States v. Nosal, 676 F.3d 854, 859 (9th Cir. 2012) (en banc).

141 Johnathan Marx, *How to Construe a Hybrid Statute*, 93 VA. L. REV. 235, 236 (2013).

142 *Id*.

143 *Id*.

144 *Id*.

145 *Id*.; *see also* Lawrence M. Solan, *Statutory Inflation and Institutional Choice*, 44 WM. & MARY L. REV. 2209, 2213 (2003).

commonplace computer activity,[146] restructuring the statute would be a more effective and definitive solution. The statute intended to prevent hacking crimes, and it would better address this goal by decoupling the criminal and civil law aspects of this statute. In its current form, interpretation of the statute requires consistency with both the rule of lenity and the doctrine of consistent interpretation. The result of this is that the rule of lenity's requirement that statutory ambiguities must be understood in a light most favorable to the criminal defendant, also applies to civil defendants. By applying strict rules of construction to "exceeding authorized access," an ambiguous and controversial term in the statute, a person with the proper credentials required to access information on a business's network cannot be prosecuted under the CFAA even if the information they had access to was subsequently used in an improper manner.[147] This favorable reading of the statute in a civil context makes it incredibly difficult for companies to pursue any judicial recourse, especially when the theft of items such as intellectual property occurs.[148] Even in courts that prioritize property rights over a focus on strict construction, the dual-use nature of the CFAA presents a problem. These courts analyze the way in which an individual uses the information they have access to and determine whether the individual's actions were in opposition to the interests of the company.[149] In these cases, the court will hold defendants civilly liable even though there is clear language stating that the court's inquiry should not focus on the defendant's intent but on the defendant's access status at the time they removed the information.[150] Neither of these interpretations provide an adequate result.

Separating the civil and criminal aspects of the CFAA would eliminate the fear of everyday computer users being criminalized while simultaneously allowing employers and businesses to still enjoy the broad coverage of the CFAA pre-*Van Buren.* Allowing the civil aspect of the CFAA to be broad while the criminal remains narrowed maintains the benefits the CFAA offers civil claimants.[151] For example, the CFAA provides an avenue to federal court when the only other claims available to the individual do not meet the requirements for diversity jurisdiction

146 *US Supreme Court Narrows Scope of Computer Fraud and Abuse Act in Van Buren*, COOLEY (June 9, 2021), https://www.cooley.com/news/insight/2021/2021-06-09-us-supreme-court-computer-fraud-abuse-act-van-buren.

147 Muir, *supra* note 28.

148 Muir, *supra* note 28.

149 Muir, *supra* note 28.

150 Muir, *supra* note 28.

151 Muir, *supra* note 28, at 57–58.

and arise under state law.[152] Also, CFAA claims tend to be easier for plaintiffs to prove than other related causes of action.[153]

By separating the civil and criminal causes of action, the statute's language could be interpreted differently in civil and criminal cases since the causes of action will no longer be coupled together. This allows for a broader application to civil cases where the notice requirements and lenity rules do not apply, and the consequences are less severe. Additionally, decoupling the statute also limits the impact of the *Van Buren* decision on civil CFAA cases. The *Van Buren* holding, by failing to acknowledge purpose beyond a litigant's actions, stifles the effectiveness of the CFAA in the civil context where an individual misuses information they have access to without necessarily exceeding their access rights.[154] While this interpretation is helpful in a criminal case, for civil claims where the bar for liability is arguably lower, allowing evidence regarding purpose would provide more protections, particularly in an employer-employee context.

To ensure that this decoupled statute is interpreted differently in its respective civil and criminal arenas, Congress should also alter the language and definitions of the now separated statutes. For the civil aspect, Congress should define the term "authorization" by providing guidance that the CFAA is applicable in scenarios where "initial permitted access to information is later rescinded or abused."[155] Providing this guidance would be a clear indication that mere or even accidental violations of employment agreements, Terms of Service agreements, or other contracts do not automatically violate the CFAA.[156] This would further ensure that every day, unsuspecting computer users are not penalized for unintentional violations while still giving employers the ability to seek justice or compensation from employees who exceed their access maliciously. Also, this definition would not prevent malware, phishing, or viruses from being penalized because they would still be considered unauthorized access achieved by circumventing a code-based technological gate under the CFAA.[157]

152 Muir, *supra* note 28, at 52.

153 Muir, *supra* note 28, at 52–53.

154 Barnard, Eidson, et. al., *Justices Clarify Scope of Anti-Hacking Law*, STINSON LLP, https://www.stinson.com/newsroom-publications-Justices-Clarify-Scope-of-Anti-Hacking-Law (last visited Aug. 4, 2022).

155 Mark L. Krotoski, *Time to Reform the Computer Fraud and Abuse Act*, LAW.COM: THE RECORDER (Nov. 18, 2015, 3:44 PM), *reprinted in* MORGAN LEWIS: PUBLICATIONS, https://www.morganlewis.com/pubs/time-to-reform-the-computer-fraud-and-abuse-act.

156 *See, e.g.*, Lofgren & Wyden, *supra* note 35.

157 *See, e.g.*, Lofgren & Wyden, *supra* note 35.

Along with clearly defining authorization, the definition of damage under the CFAA should be limited solely to real damage, whether that be damage to data or damage to the method used to access data.[158] Harmless instances where employees delete emails from their inbox as they leave the company, or delete backup files when there are various other accessible copies of them, should not be actionable under the CFAA.[159] In allowing this broadened civil interpretation, Congress could also set a standard for the "exceeds authorization" equivalent by specifically focusing on employees and criminalizing the access only if it is a clear violation of an employment agreement.[160] This change could allow for an essential function of the statute, maintaining liability for the misappropriation of information an employee has access to without the risk of liability beyond the CFAA's intended scope.[161]

For the criminal aspect, Congress can create clear criminal liability, successfully addressing notice concerns, by replacing "exceeds authorized access" with a term capturing its limitation to code-based restrictions.[162] Specifically, Congress should replace "exceeds authorized access" with "access without authorization," and define it as obtaining "information on a protected computer . . . that the accessor lacks authorization to obtain" by "knowingly circumventing one or more technological or physical measures that are designed to exclude or prevent unauthorized individuals from obtaining that information."[163] Aaron's Law proposed this language change in 2013 to apply to both the civil and criminal aspects of the CFAA.[164] However, applying this solely to the criminal aspect limits the scope of the CFAA in a manner more consistent with how courts have construed the narrow view of this statute.[165] This change focuses criminal liability on the technological act, such as bypassing a code-based restriction, ensuring that bypassing firewalls, hacking passwords, or other similar actions will give rise to criminal liability.[166]

Along with these specific changes, as discussed in the previous section, individuals who violate Terms of Service should not be liable under the CFAA, whether in a civil or criminal context. To achieve this goal, Congress could provide courts with clear guidance by altering the

158 Eckland, *supra* note 41.
159 Eckland, *supra* note 41.
160 Muir, *supra* note 28.
161 *See* Muir, *supra* note 28.
162 Berris, FROM CLICKWRAP TO RAP SHEET, *supra* note 87.
163 Berris, FROM CLICKWRAP TO RAP SHEET, *supra* note 87.
164 Aaron's Law Act, H.R. 2454, 113th Cong. § 1 (2013).
165 Berris, FROM CLICKWRAP TO RAP SHEET, *supra* note 87.
166 Muir, *supra* note 28.

access status terms and basing them on technology and how the retrieved information is accessed.[167] While separating the civil and criminal causes of action does not address every privacy issue, it allows the statute to address hacking crimes, both criminally and civilly, which was CFAA's original intent. In terms of other computer-related crimes, the CFAA was not enacted to be the sole vehicle to protect privacy interests, nor was it drafted by Congress with the level of complexity, detail, or foresight required to address the vast array of modern-day privacy concerns.[168] Thus, while the CFAA can and should have a role in shaping privacy policy, its role should be specialized and relate to its initial purpose, addressing hacking, as it does not artfully or effectively address other areas of privacy policy.[169] In essence, "if privacy regulation requires the nuanced approach of a scalpel, the CFAA acts as a hammer."[170] In reference to the *Van Buren* case, for example, other laws and routes are already in place to protect against this behavior.[171] Some preexisting laws that address privacy policy are the Defend Trade Secrets Act, state trade secret laws, state trespass laws, and business torts such as the breach of the duty of care.[172] In conjunction with these laws, confidentiality, non-disclosure, and non-compete agreements with express provisions for unauthorized access or disclosure of information can aid in protecting employers and also provide additional grounds for civil lawsuits.[173]

IV. CONCLUSION

The purpose of a statute is to prohibit problematic or dangerous behavior and therefore put the public on notice that engaging in such behavior would result in liability, whether criminal or civil.[174] This Comment sets forth the position that in its current form, the CFAA is

167 Muir, *supra* note 28.

168 Nicole Sakin & Sarah Rippy, *How the Lack of a Federal Privacy Law is Resulting in a Problematic Application of the CFAA*, IAPP (Feb. 5, 2021), https://iapp.org/news/a/how-the-lack-of-a-federal-privacy-law-is-resulting-in-a-problematic-application-of-the-cffa/.

169 *Id*.

170 *Id*.

171 *The Computer Fraud and Abuse Act now Provides Less Protection from Insider Threats. Here's What Employers Need to be Doing*, CONSTANGY, BROOKS, SMITH & PROPHETE LLP (June 6, 2021), https://www.constangy.com/newsroom-newsletters-1078.

172 *Id*.

173 *Id*.

174 Mark L. Krotoski, *Time to Reform the Computer Fraud and Abuse Act*, LAW.COM: THE RECORDER (Nov. 18, 2015, 3:44 PM), *reprinted in* MORGAN LEWIS: PUBLICATIONS, https://www.morganlewis.com/pubs/time-to-reform-the-computer-fraud-and-abuse-act.

unworkable and does not effectively achieve the goals for which it was created. The dual-use nature of the statute prevents it from effectively addressing civil and criminal aspects. Since a single statute cannot be interpreted in multiple ways, the differing standards and procedures of civil and criminal causes of action clash, resulting in an unideal application of the statute in various areas. Also, the *Van Buren* decision does not go far enough to resolve the ambiguities of this historically controversial, overbroad, and outdated statute.

This Comment proposes a two-fold statutory reform of the CFAA. The first prong addresses the aspects of the statute that *Van Buren* failed to address and proposes adopting a code-based approach when defining "authorization." The second prong discusses the importance of decoupling the statute's civil and criminal causes of action to allow for more adequate application. Along with decoupling the statute, this prong discusses proposed language changes and clarifications on the definitions of certain terms for the respective civil and criminal aspects of the statute. By continuing the process of narrowing the statute that was begun in *Van Buren*, decoupling the civil and criminal aspects of it, and clarifying the cause of action specific language, Congress can make the CFAA more effective as a true hacking statute and avoid fear of criminal liability for everyday computer users and researchers alike.