UIC
REVIEW OF INTELLECTUAL PROPERTY LAW

VAN BUREN V. UNITED STATES: AN EMPLOYER DEFEAT OR HACKERS' VICTORY – OR SOMETHING IN BETWEEN?

MELANIE ASSAD

ORCID: 0000-0002-3435-8807

ABSTRACT

The Supreme Court decision in *Van Buren v. United States* significantly impacts the scope of the Computer Fraud and Abuse Act (CFAA). In its current form, the CFAA imposes criminal and civil liability onto anyone who "intentionally access a computer without authorization or exceeds authorized access." For many years, the federal circuit courts had difficulty determining what conduct triggers liability under the "exceeds authorized access" clause of the CFAA. The Supreme Court resolved this dispute by narrowly interpreting the phrase to apply to only individuals who access information they are not otherwise authorized to access. In *Van Buren,* the Court found that a police officer, who used his authorized police database to access information for a personal reason, did not violate the CFAA. This case note will explore how the Court reached its conclusion in *Van Buren.* It will further examine the policy implications of this decision and discuss how a narrow interpretation of the CFAA will impact future litigation.

Cite as 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 (2022).

VAN BUREN V. UNITED STATES: AN EMPLOYER DEFEAT OR HACKERS' VICTORY – OR SOMETHING IN BETWEEN?

MELANIE ASSAD

VAN BUREN V. UNITED STATES: AN EMPLOYER DEFEAT OR HACKERS' VICTORY – OR SOMETHING IN BETWEEN?

MELANIE ASSAD*

I. INTRODUCTION

Imagine you are an attorney at a large law firm. You go to work one morning and realize that you forgot to answer some personal emails from the night before. You quickly log into your personal email, respond, and check Facebook before exiting out of the browsers. You disregard the company policy that prevents employees from using their work computers for personal matters because everybody does it. Three days later, you return to work, and the FBI is waiting for you–you have just been charged with committing computer fraud under the Computer Fraud and Abuse Act of 1986 (CFAA).[1]

According to the Government's argument in *Van Buren v. United States,* you–and nearly every American–would be guilty of committing computer fraud by "exceeding authorized access" if you accessed information on a computer for an "improper purpose."[2] Fortunately, for computer users across the country,[3] the Supreme Court rejected the Government's interpretation of what it means to "exceed authorized access" under the CFAA.[4] However, this hypothetical could have been reality if the Supreme Court did not come to its decision in *Van Buren.*[5]

So, what does it mean to "exceed authorized access" under the CFAA? And, in what situations is an employee subject to liability under the statute? These questions have been the subject of a decades long split between the federal circuit courts.[6]

---

* © ORCID 0000-0002-3435-8807. Melanie Assad, J.D. Candidate, May 2022, University of Illinois Chicago School of Law; B.A. in Criminal Justice, Michigan State University (2019). I would like to dedicate this article and achievement to my father, David Assad, who always encourages me to be the best version of myself. I would also like to thank my friends, family, and RIPL editors - I could not have done it without you.

[1] 18 U.S.C. § 1030(a)(2) (2022).

[2] *See* Van Buren v. United States, 141 S. Ct. 1648, 1649 (2021) (arguing that the original 1984 Act's precursor to the "extends authorized access" language which covered any person whom, "having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend" supports its reading).

[3] *See* Joseph Johnson*, United States: Digital Populations as of January 2021*, STATISTA (Mar. 9, 2022), https://www.statista.com/statistics/1044012/usa-digital-platform-audience/. As of January 2021, there were approximately 269.5 million internet users in the United States, representing over 90 percent of all active internet users nationwide. *Id.*

[4] *See Van Buren*, 141 S. Ct. at 1649. When Congress amended the CFAA in 1984, it removed any reference to "purpose." Accordingly, the Supreme Court noted this "cuts against reading the statute to cover purpose-based limitations." *Id.* at 1651.

[5] *See* Musacchio v. United States, 577 U.S. 237, 237 (2016). The Supreme Court had the opportunity to address the ongoing dispute over how to interpret the "exceeds authorized access" clause of the CFAA in 2016. The Court, however, did not provide any insight on how to properly interpret the clause. *Id.*

[6] *See* Tonia O. Klausner, Nomi Conway & Johnathan S. Francis, *U.S. Supreme Court Resolves Circuit Split on Meaning of "Exceeds Authorized Access" in Computer Fraud and Abuse Act*, WILSON SONSINI (June 7, 2021), https://www.wsgr.com/print/v2/content/208377/U.S.-Supreme-Court-Resolves-Circuit-Split-on-Meaning-of-%E2%80%9CExceeds-Authorized-Access%E2%80%9D-in-

Accordingly, Part II will introduce the Computer Fraud and Abuse Act and explain the competing interpretations of what it means to "exceed authorized access" under the statute. Part III will explain how the Supreme Court answered this decades-long debate in *Van Buren v. United States*. Part IV will analyze the Supreme Court's "gates-up-and-down" approach,[7] argue that it was correct in its interpretation, and discuss the legal ambiguities that *Van Buren* did not address. Lastly, Part V will conclude this case note and briefly recap how the Supreme Court's interpretation of the CFAA will affect future litigation.[8]

II. BACKGROUND

This Part will discuss the history behind the CFAA and explain the circuit courts' disagreement over the "exceeds authorized access" clause, with an emphasis on Eleventh Circuit precedent. The Eleventh Circuit plays an integral role in the discussion of the CFAA because two important cases emerged from the this circuit– *United States v. Rodriguez* and *Van Buren v. United States.*

A. The Emergence of the Computer Fraud and Abuse Act

In the early 1980s,[9] law enforcement agencies were concerned with the lack of criminal laws available[10] to fight emerging computer crimes.[11] In response, Congress added provisions to the Comprehensive Crime Control Act[12] (CCCA) of 1984 to address

---

Computer-Fraud-and-Abuse-Act.pdf. (stating that "[o]n June 3, 2021, the U.S. Supreme Court issued its decision in *Van Buren* . . . resolv[ed] a decades-old circuit split").

[7] *See Van Buren*, 141 S. Ct. at 1658. "[Under the] gates-up-or-down inquiry-one either can or cannot access a computer system, and one either can or cannot access certain areas within the system." *Id.* at 1658–59.

[8] *See* Mark P. Kesslen, Kathleen A. McGree & Bryan Sterba, *Supreme Court Grants Certiorari in Web Scaping Case HiQ v. Linkedin*, LOWENSTEIN SANDLER (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. The *Van Buren* decision has implications on a future case currently on the Supreme Court's docket, *HiQ Labs, Inc. v. LinkedIn Corp*. *Id.*

[9] *See* H.R. REP. NO. 98-894, at 20 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3659. "Traditional theft/larceny statutes are not the proper vehicle to control the spate of computer abuse and computer assisted crimes." *Id.* As reliance on computers increased in the 1980s, it became clear to the government that unauthorized access to data could become catastrophic. *Id.*

[10] *See Van Buren*, 141 S. Ct. at 1652. "After a series of highly publicized hackings captured the public's attention, it became clear that traditional theft and trespass statutes were ill suited to address cybercrimes that did not deprive computer owners of property in the traditional sense." *Id.*; Orin S. Kerr, *Cybercrimes Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, N.Y.U. L. REV. 1596, 1605–13 (2003); Seymour Bosworth, Michael E. Kabay & Eric Whyne, *History of Computer Crime*, *in* COMPUTER SECURITY HANDBOOK 23, 24 (6th ed., 2012) ("Physical damage to computer systems was a prominent threat until the 1980s.).

[11] H. Marshall Jarett & Michael W. Bailie, *Prosecuting Computer Crimes*, DEP'T OF JUSTICE, https://www.justice.gov/criminal/file/442156/download (last visited Apr. 18, 2022).

[12] *See* The Comprehensive Crime Control Act of 1984, 18 U.S.C. § 1030 (2022). The CCCA was the first federal computer fraud law designed to address hacking in cases involving a compelling "federal interest" (involving situations where computers of the federal government or certain financial institutions were involved where the crime itself was interstate in nature). *Id.*

problems associated with the unauthorized use of computers and computer networks.[13] These newly added provisions made it a felony to access classified information in a computer without authorization.[14] It also made it a misdemeanor offense to access financial records, access credit histories stored in financial institutions, and trespass into government computers without authorization.[15]

Even after Congress amended the CCCA,[16] it continued to investigate problems associated with computer crimes and held several hearings[17] to determine whether federal criminal laws required further revision.[18] Two years later, Congress enacted the Computer Fraud and Abuse Act in order to address computer hacking.[19] Today, the CFAA is the main federal computer fraud statute[20] and has been described as "the most important piece of U.S. legislation used to combat computer crime."[21]

---

[13] Jarett, *supra* note 11.

[14] 18 U.S.C. § 1030 (2022).

[15] *Id.*

[16] H.R. REP. NO. 98-894, at 12 (1984). The 1984 Amendments to the Counterfeit Access Device and Computer Fraud and Abuse Act made it a federal offense to use a computer without authorization with the intent to execute a scheme to defraud. It also prohibited the unauthorized use of a computer when such conduct modifies or discloses information. *Id.* Additionally, it amended the language to prevent the use of a computer to obtain anything of value or to create a loss of another of a value of $5,000 or more during anyone one year. *Id.*

[17] *Id.* at 28. As the potential for abuse of computer networks became clearer, the Judiciary Committee held hearings to establish criminal penalties under the Counterfeit Access Device and Computer Fraud Act of 1983. It expanded the Act to protect computers owned or used by the federal government, financial institutions, and/or businesses engaged in interstate commerce.

[18] *Id.*

[19] H.R. REP. NO. 98-894. In 1983, President Ronald Regan watched the movie *WarGames,* a movie in which a computer hacks into a military system. *Id.* Intrigued by the movie, Regan consulted with the Chairman of the Joint Chief of Staff who voiced concerns of computer hacking. *Id.* Later that year, six anti-hacking bills made their way through Congress. *Id.* In the 1984 House Report, Congress references the 1983 film for its inspiration on the CFAA. *Id. See generally Where Did The CFAA Come From, and Where is it Going*?, THE PARALLAX VIEW (Mar. 16, 2016), https://www.the-parallax.com/where-cfaa-going-timeline-history/ (explaining the legislative history); Ronald Sarian, *The Computer Fraud and Abuse Act Now Provides Less Protection From Insider Threats. Here's What Employers Need to be Doing*, CONSTANGY, BROOKS, SMITH & PROPHET (June 30, 2021), https://www.constangy.com/newsroom-newsletters-1078; *Computer Fraud and Abuse Act (CFAA),* NACDL, https://www.nacdl.org/Landing/ComputerFraudandAbuseAct.

[20] *See* Ivan Evtimov et al., *Is Tricking A Robot Hacking*?, 34 BERKELEY TECH. L.J. 891, 904 (2019). "Since its implementation, the CFAA has been the nation's predominant anti-hacking law." *Id. See A Review of State Computer Crime Law*, NAT'L GOVERNORS ASSOC. (Nov. 1, 2016), https://www.nga.org/center/publications/a-review-of-state-computer-crime-law/ ("Today, virtually all computer crime statutes regulate the following behavior: (1) using, accessing, or damaging a computer with criminal intent or for a criminal purpose; (2) using, accessing, or damaging a computer without authorization; (3) using, access, or damaging computerized data without permission.").

[21] Daniel Etcovich & Thyla Van Der Merwe, *Coming In From the Cold: A Safe Harbor from the CFAA and the DMCA § 1201 For Security Researchers*, BERKMAN KLEIN CTR. HARV. UNIV. 1, 7 (2018), https://dash.harvard.edu/bitstream/handle/1/37135306/ComingOutoftheCold_FINAL.pdf?sequence=1&isAllowed=y.

As computer crimes have continued to grow over the years,[22] Congress[23] has broadened the scope and coverage of the CFAA beyond its original intent.[24] The current version of the CFAA subjects criminal and civil liability[25] to anyone who "intentionally[26] accesses a computer without authorization[27] or exceeds authorized

---

[22] *See* Steve Morgan, *Cybercrime To Cost The World $10.5 Trillion Annually By 2025*, CYBERCRIME MAG. (Nov. 13, 2020), https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

("Cybersecurity Ventures expects global cybercrime costs to grow by 15 percent per year over the next five years, reaching $10.5 trillion USD annually by 2025, up from $3 trillion USD in 2015.").

[23] Christopher P. Hotaling & Krithika Rajumar, *SCOTUS Narrows The Computer Fraud And Abuse Act in* Van Buren v. United States, NIXON PEABODY (June 10, 2021), https://www.nixonpeabody.com/en/ideas/articles/2021/06/10/van-buren-cfaa-ruling. It is not clear if Congress will amend the CFAA pursuant to the Supreme Court's decision in *Van Buren*. *Id.*

[24] *See What is the Computer Fraud and Abuse Act?,* FLEESON GOOING (Feb. 10, 2017), https://www.fleeson.com/what-is-the-computer-fraud-and-abuse-act/#:~:text=The%20Computer%20Fraud%20and%20Abuse%20Act%20(CFAA)%2C18%20U.S.C.,be%20brought%20by%20private%20litigants. "Prosecutors need only prove a general intent to cause damage, rather than a specific intent to cause a predefined type of damage." *Id.* Congress has amended the CFAA on eight separation occasions: in 1988, 1989, 1990, 1994, 1996, 2001, 2002, and 2008. *Id.* Originally, Section 1030(a)(2) protected individual privacy by criminalizing unauthorized access to computerized information and credit records. *Id.* However, in 1996, Congress expanded the scope of this section by adding two subsections that also protected information on government computers, § 1030(a)(2)(B) and computers used in interstate or foreign communication, § 1030(a)(2)(C). *See* 18 U.S.C. § 1030 (2022). Now, the prohibition applies, at a minimum, to any information from any computer that is connected to the internet. *See* §§ 1030(a)(2)(C) and (e)(2)(B) (2022). Additionally, the Patriot Act further amended the CFAA in 2001. *Id.* The Patriot Act expanded the CFAA, increasing both its penalties and its effectiveness as a prosecution tool by changing the "intent" requirement. *Id.*

[25] *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws*, CONGRESSIONAL RSCH. SERVS. (Oct. 15, 2014), https://www.everycrsreport.com/reports/97-1025.html. Section 1030(a)(2) of the CFAA has a three-tier sentencing structure. Simple violations are punished as misdemeanors, imprisonment up to one year, and/or a fine up to $100,000 or $200,000 for organizations. *See* 18 U.S.C. § 1030(c)(2)(A)-(B) (2022). The second tier carries penalties of imprisonment for up to five years and/or a fine of up to $250,000 or $500,000 for organizations. *Id.* These penalties are reserved for cases in which: "(i) the offense was committed for purposes of commercial advantage of private financial gain; (ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or (iii) the value of the information obtained exceeds $5,000." *Id. See* 18 U.S.C. § 1030(c)(2)(B) (2022). The third tier is for repeat offenders. These offenders may face imprisonment of up to 10 years and/or a fine of up to $250,000 or $500,000 for organizations. *Id.*

[26] *See* S. REP. NO. 104-357, at 11 (1986). "[I]nsiders, 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 intruders who break into a computer could be punished for any intentional, reckless, or other damage they cause by their trespass." *Id.*

[27] *See "Authorized Access": The Supreme Court's First Foray into the Computer Fraud and Abuse Act*, CROWELL & MORING (Apr. 22, 2020), https://www.crowell.com/NewsEvents/AlertsNewsletters/all/Authorized-Access-The-Supreme-Courts-First-Foray-Into-The-Computer-Fraud-And-Abuse-Act (noting the term "without authorization" is undefined by the CFAA).

access, and thereby obtains information[28] from any protected computer.[29]"[30] While the CFAA does not define the phrase "without authorization," it does define the phrase "exceeds authorized access" to mean 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."[31] The most commonly litigated issue about exceeding authorized access has resulted from a disagreement over what conduct falls under this category.[32]

Even though the language under § 1030(a)(2) is unclear, legislative history indicates that the two phrases were intended to correspond to different categories of unauthorized computer use.[33] A senate report indicates that persons who access computers "without authorization" will typically be outsiders such as hackers.[34] In contrast, persons who "exceed authorized access" will be insiders such as employees using a victims corporate computer network.[35] Congress intended for these provisions to provide computer owners and the law enforcement community a "clearer statement of proscribed activity."[36] However, over the past few decades, the CFAA has remained the subject of significant legal challenges, and the federal circuit courts have remained divided on how to interpret certain areas of the law.[37]

B. The Circuit Split

Every day, millions of Americans across the country use computers for work and personal matters.[38] Accessing information on those computers is almost always

---

[28] *See* United States v. Drew, 259 F.R.D. 449, 457 (C.D. Cal. 2009). "[T]he term 'obtaining information includes merely reading it." (quoting S. REP. NO. 103-357, at 7 (1996)). The phrase "obtain information" has been broadly interpreted by courts to include "mere observation of the data" such as reading information on a screen. *Id.*

[29] *See* 18 U.S.C. § 1030(e)(2) (2022). The term "protected computer" is broadly interpreted to include (1) United States' government computers; (2) financial institution computers; or (3) computers used in interstate or foreign commerce. *Id.* Examples include cellphones, cell towers, websites, restricted databases, iPads, Kindles, Nooks, video game systems, and any stations that submit wireless signals. *See also* Brenda R. Sharton, Gabrielle L. Gould & Justin C. Pierce, *Key Issues in Computer Fraud and Abuse Act (CFAA) Civil Litigation*, GOODWIN LAW, https://www.goodwinlaw.com/-/media/files/publications/10_01-aa-key-issues-in-computer-fraud-and-abuse.pdf (last visited Apr. 19, 2022).

[30] 18 U.S.C. § 1030(a)(2) (2022).

[31] 18 U.S.C. § 1030(e)(6) (2022).

[32] *See* Jarett, *supra* note 11, at 9. "[T]he most commonly litigated issue about 'exceeding authorized access' in reported opinions is whether a particular defendant exceeded authorized access by accessing the computer for an improper purpose."

[33] *Id.*

[34] *See* S. REP. NO. 99-432, at 8 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479 (discussing the legislative history).

[35] *Id.*

[36] H.R. REP. NO. 98-894, at 6; Jarett, *supra* note 11, at 1.

[37] *See* Jesse R. Taylor & Peter Watt-Morse, *Reexamining the Computer Fraud and Abuse Act*, MORGAN LEWIS (May 27, 2020), https://www.morganlewis.com/blogs/sourcingatmorganlewis/2020/05/reexamining-the-computer-fraud-and-abuse-act. ("[I]n the employment context, courts are split on whether an employee's violation of company policy constitutes a CFAA violation.").

[38] Andrew Kopsidas & Eda Stark, *From WarGames to Terms of Service: How the Supreme Court's Review of Computer Fraud Abuse Act Will Impact Your Trade Secrets*, FISH & RICHARDSON (Aug. 7, 2020), https://www.jdsupra.com/post/contentViewerEmbed.aspx?fid=3e009a6d-9cc4-4391-b29f-c22a25d114b7.

subject to employers' policies, websites' terms of service, and other third-party restrictions.[39] Should the court subject CFAA liability onto an individual who violates an employment policy or a condition on a website's terms of service?

As briefly discussed above, litigation over what conduct is subject to liability under the "exceeds authorized access" clause[40] has created disagreement between the federal circuit courts.[41] Accordingly, this Part will examine that split and discuss the competing authority that led the Supreme Court to grant certiorari in *Van Buren v. United States*.

Since the CFAA was enacted in 1986, it has been widely used by prosecutors[42] and civil litigants[43] to reach conduct that does not resemble traditional hacking techniques.[44] Consider the following hypothetical: an employee is authorized to download confidential information from his employer's database but there is a company policy that prevents employees from disclosing confidential information to third-party sources. Before the employee quits his job, he downloads information from his employer's database and gives the information to a competing business. Did this employee "exceed authorized access" under the CFAA?

---

[39] *Id.*

[40] *See* Peter G. Berris, *Cybercrime and the Law: Computer Fraud and Abuse Act (CFAA) and the 116th Congress*, CONGRESSIONAL RSCH. SERV. (Sept. 21, 2020), https://sgp.fas.org/crs/misc/R46536.pdf ("Whatever the legislative intent, judicial interpretations of "without authorization" and "exceeds authorized access" have not been entirely consistent.").

[41] *See* Alden Anderson, *The Computer Fraud And Abuse Act: Hacking Into The Authorization Debate*, 53 JURIMETRICS J. 447, 447 (2013) ("This has created a split among the Circuit Courts over whether an employee who misuses employer information pursuant to authorized physical computer access 'accessing a computer without authorization or 'exceeds authorized' access' and can thus be prosecuted or held liable for civil damages under the Act.").

[42] *Id.*; *see also* Andrea Peterson, *This 80's-Era Criminal Hacking Law Scares Cybersecurity Researchers*, THE WASH. POST (Aug. 5, 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/08/05/this-80s-era-criminal-hacking-law-scares-cybersecurity-researchers/. One of the most high-profile prosecutions under the CFAA was Aaron Swartz, a Reddit co-founder and online activist. *Id.* Swartz committed suicide in 2013 while facing felony charges for illegally downloading millions of documents after he illegally accessed a computer network at the Massachusetts Institute of Technology. *Id.* The CFAA was also used to prosecute and convict Andrew Auernheimer, a notorious Internet troll, who obtained more than 100,000 e-mail addresses of iPad users from AT&T's website. *Id.*

[43] *See* Matthew J. Hank & Rachel Fendell Satinsky, *Supreme Court Narrows the Scope of Claims Available Under the Computer Fraud and Abuse Act*, LITTLER MENDELSON (June 8, 2021), https://www.littler.com/publication-press/publication/supreme-court-narrows-scope-claims-available-under-computer-fraud-and ("Employers typically allege CFAA violations after, for example, an employee downloads or emails confidential information to benefit a computer.").

[44] *See* Jessica Heim, Jennifer Freel, Meghan Natenson & Evan Seeder, *Hacking the Computer Fraud and Abuse Act: The Supreme Court Narrows the Reach of the CFAA's "Exceeds Authorized Access" Provision*, VINSON & ELKINS (June 8, 2021), https://www.velaw.com/insights/hacking-the-computer-fraud-and-abuse-act-the-supreme-court-narrows-the-reach-of-the-cfaas-exceeds-authorized-access-provision/ ("[The CFAA] has been widely used . . . to reach conduct that does not resemble traditional hacking techniques, such as installing malicious software on a computer to gain system access and obtaining information from a computer network.").

Prior to the *Van Buren* decision, some circuits would find this conduct in violation of the CFAA. For example, the First,[45] Fifth,[46] Seventh,[47] and Eleventh[48] circuits have all held that employees "exceed authorized access" if they use their authorized access to obtain information from a computer for an improper purpose. Under this approach, it does not matter if the individual is granted general permission to access the computer. An employee exceeds their authorized access if they use their general permission for non-business purposes.[49]

In the First Circuit, the court interpreted this clause to apply to situations in which a user who was authorized to access information did so with the intent of disclosing the information in violation of a confidentiality agreement.[50] The Fifth Circuit interpreted this clause to apply to a user who was authorized to access information but did so with the intent of committing fraud in violation of an employment policy.[51] In addition, the Seventh Circuit has held that an employee exceeds authorized access when he accesses information with the intent of deleting information to harm a former employer.[52] All of these examples express the general principle that an employee's motive for obtaining information can determine whether one exceeds authorized access under the CFAA.

In contrast, other circuit courts including the Second,[53] Fourth,[54] Sixth,[55] and Ninth,[56] circuits would find that the conduct articulated in the hypothetical above, does

---

[45] *See* United States v. Czubinski, 106 F.3d 1069, 1071 (1st Cir. 1997). "[IRS] employees may not use any Service computer system for other than official purposes." *Id.* at 1079 n.1; EF Cultural Travel BV v. Explorica, 274 F.3d 577, 582–83 (1st Cir. 2001) (holding that defendant exceeded its authorized access by disclosing computer data in violation of a confidentiality agreement).

[46] *See* United States v. John, 597 F.3d 263, 272 (5th Cir. 2010). "Access to a computer and data that can be obtained from that access may be exceeded if the purposes for which the access has been given are exceeded." *Id.*

[47] *See* Int'l Airport Ctr., LLC v. Citrin, 440 F.3d 418, 420 (7th Cir. 2006) (applying the CFAA to employee misconduct).

[48] *See* Cont'l Grp., Inc. v. KW Prop. Mgmt., LLC, 622 F. Supp. 2d 1357, 1372 (S.D. Fla. 2009). Computer access policies stated that computers were provided "for business use" and were "to be used solely for the authorizing party's purposes." *Id.*; United States v. Salum, 257 F. App'x. 225, 227 (11th Cir. 2007) (holding that officers could access NCIC system only for official business for the criminal justice agency).

[49] *See* United States v. Rodriguez, 628 F.3d 1258, 1264 (11th Cir. 2010) (holding an employee liable under the CFAA for using its employer's database for a non-business reason).

[50] *See EF Cultural Travel BV*, 274 F.3d at 581–82.

[51] *John,* 597 F.3d 271–72.

[52] *Int'l Airport Ctr., LLC*, 440 F.3d at 420.

[53] *See* United States v. Valle, 807 F.3d 508, 528 (2d Cir. 2015) (holding that a New York City Police Officer did not violate the CFAA when he used his access to law enforcement databases to view information about a woman, even though NYPD policies limited database access to law enforcement purposes).

[54] *See* WEC Carolina Energy Sols., LLC v. Miller, 687 F.3d 199, 203–04 (4th Cir. 2012) ("limiting [Section 1030(a)(2)'s] terms application to situations where an individual accesses a computer or information on a computer without permission") (citing United States v. Nosal, 676 F.3d 854, 863 (9th Cir. 2012)).

[55] *See* Royal Truck & Trailer Sales & Serv., Inc. v. Kraft, 974 F.3d 756, 761–62 (6th Cir. 2020) (adopting the Second, Fourth, and Ninth Circuits' narrow approach to find that the CFAA does not bar employees from misusing company information that they are authorized to access).

[56] *See* LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1135 n.7 (9th Cir. 2009). The defendant does not "exceed authorized access" under the CFAA when he breaches a duty of loyalty to an authorizing party. *Id.*

not exceed authorized access within the meaning of § 1030(e)(6). These circuits have favored a more narrow approach, holding that an employee violates the CFAA only when he accesses other areas of the computer that he is not authorized to access.[57] This inquiry limits the application of "exceeding authorized access" to situations in which an employee has authorization to access a computer but then "hacks" into other parts of the computer they do not have permission to access.[58] Under this interpretation, an "improper motive" or even a misuse of information, does not implicate the CFAA if the person had general permission to access the computer.[59] These circuits have concluded that the CFAA's purpose is to penalize those who breach cyber barriers without permission–not police those who misuse the data they are otherwise authorized to obtain.[60]

C. Pre Van Buren: United States v. Rodriguez

United States v. Rodriguez was the Eleventh Circuit's leading case involving §1030(a)(2) of the CFAA before *Van Buren*.[61] This case serves an important role in the discussion of the CFAA because it illustrates the approach that the Supreme Court eventually rejected.

Robert Rodriguez was an employee of the Social Security Administration (SSA) when he used the SSA's databases to research the birth dates and home addresses of seventeen people for personal use.[62] This conduct violated SSA policy, which prohibited employees from accessing information on its databases without a legitimate business reason.[63] As a result, Rodriguez was convicted of computer fraud in violation of the CFAA.[64] Rodriguez appealed his conviction to the Eleventh Circuit, claiming that he did not "exceed authorized access" because he was authorized to use the databases as a Teleservice Representative despite the fact that he used his authorization for personal reasons.[65] Rodriguez cited Ninth[66] and Fifth Circuit[67] precedent to persuade

---

[57] *Nosal*, 676 F.3d at 858. The narrow approach was articulated in *Nosal* when the Ninth Circuit held that employees of an executive search firm did not "exceed authorized access" when they removed information from their employer's confidential database and passed that information to a former employee of the firm in violation of company policy. *Id.*

[58] Katherine Mesenbring Field, *Agency, Code, or Contract: Determining Employees' Authorization Under the Computer Fraud and Abuse Act*, 107 MICH. L. REV. 819, 835–36 (2009).

[59] *Supreme Court Narrows Scope of Computer Fraud and Abuse Act in* Van Buren v. United States, BARNES & THORNBURG (July 16, 2021), https://btlaw.com/en/insights/alerts/2021/supreme-court-narrows-scope-of-computer-fraud-and-abuse-act-in-van-buren-v-united-states.

[60] *See Kraft*, 974 F.3d at 762–63 (finding that the CFAA does not bar employees from misusing company information they are authorized to access).

[61] United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010).

[62] *Id.* at 1260.

[63] *Id.* The SSA Administration warned its employees that they faced criminal penalties if they violated policies on the unauthorized use of its databases. Rodriguez, however, refused to sign the acknowledgement forms. *Id.*

[64] *Id.*

[65] *Id.*

[66] *See* LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1127 (9th Cir. 2009) (holding that an employee acts without authorization when he has no permission to access computers at all or when such permission is rescinded).

[67] United States v. John, 597 F.3d 263, 272 (5th Cir. 2010).

the court to adopt the narrow interpretation of the CFAA.[68] The Eleventh Circuit, however, rejected this argument and held that a person with authority to access a computer can be guilty of computer fraud if that person misuses their computer.[69] Relying on the Administration's computer-use policy and the plain-language of the CFAA,[70] the Eleventh Circuit affirmed Rodriguez's conviction holding that he exceeded his authorized access.[71]

The *Van Buren* case presents an interesting perspective in Eleventh Circuit history because it had the chance to overrule *Rodriguez* and declined to do so. On appeal to the Eleventh Circuit in *Van Buren,* the Court of Appeals noted that "the animating force behind [Van Buren's] argument [was] an appeal to overrule *Rodriguez*."[72] Rejecting its sister circuit's precedent, the court refused to use this opportunity as a chance to adopt the narrow interpretation of the CFAA.[73]

D. Other Interested Parties

The CFAA has not only left the courts wondering how to interpret the statute, but it has created a divide in other parties as well.[74] Prior to the *Van Buren* decision, numerous scholars and technology companies have noted the chilling affect created by the broad interpretation of the "exceeds authorized access" clause. Groups such as the Electronic Frontier Foundation (EFF)[75] and the American Civil Liberties Union were concerned that a broad interpretation would criminalize research conducted by journalists and cybersecurity experts.[76]

In support of Van Buren's petition for a writ of certiorari, the EFF drafted an amici curiae brief to argue for a narrow interpretation of the CFAA.[77] In its brief, the EFF explained how an expansive interpretation of the statute would impair a broad

---

[68] United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010)

[69] *Id.*

[70] *Id.* (arguing that "the plain language of the [CFAA] forecloses any argument that Rodriguez did not exceed his authorized access.").

[71] *Id.* "Rodriguez exceeded his authorized access and violated the Act when he obtained personal information for a non-business reason." *Id.*

[72] United States v. Van Buren, 940 F.3d 1192, 1207 (11th Cir. 2019).

[73] *Id.* at 1208. "[U]nder our prior-precedent rule, "a prior panel's holding is binding unless and until it is overruled or undetermined [s]ince Van Buren has identified no Supreme Court or en banc decision of this Circuit that abrogates *Rodriguez*, we must continue to follow it." *Id.*

[74] *See* Issie Lapowsky, Van Buren v. United States*: The SCOTUS Case Splitting the Privacy World in Two*, PROTOCOL (Nov. 30, 2020), https://www.protocol.com/van-buren-v-united-states-supreme-court ("Van Buren v. United States has divided frequent allies in the security and privacy space.").

[75] *Id.*; *see also Electronic Frontier Foundation*, MACARTHUR FOUND., (last visited Apr. 19 2022), https://www.macfound.org/grantee/electronic-frontier-foundation-37009/. "The EFF defends civil liberties in the digital world by championing privacy, free expression, and innovation." *Id.* The EFF is a non-profit civil liberties organization that works to protect innovation, free expression, and civil liberties in the digital world. *Id.*

[76] Lorraine Kenny, *Knight Institute Comments on Supreme Court Decision in* Van Buren v. United States, KNIGHT COLUMBIA (June 3, 2021), https://knightcolumbia.org/content/knight-institute-comments-on-supreme-court-decision-in-van-buren-v-united-states.

[77] *Id.*

range of First Amendment protected activity.[78] For example, the investigative techniques of journalists and academic researchers sometimes require violating specific company prohibitions on certain activities.[79] Online discrimination research and data journalism requires researchers to collect data through the use of research tools which automatically collect public data and provide false information to test accounts.[80] Many internet platforms, however, prohibit the use of these tools through their terms of service provisions.[81] Accordingly, any researcher or journalist who conducts research in violation of a website's terms of service would be subject to criminal and civil liability under the CFAA.[82] Thus, the EEC believed that the CFAA should not be interpreted to criminalize violations of computer use policies because it would ultimately chill activity protected by the First Amendment.

On the other hand, the Electronic Privacy Information Center (EPIC) and other prominent privacy scholars argued that the statute should be interpreted broadly.[83] In its amicus brief, EPIC argued that protecting privacy is "core to the CFAA" and that the law was written to defend against both outside hackers and authorized access from insiders.[84] EPIC cited a Senate report that was published when the CFAA was amended in 1996, which stated that the changes were designed to "increase protection for the privacy and confidentiality of consumer information."[85] EPIC, therefore, argued that the CFAA was designed to hold government officials, like Van Buren, accountable for misusing sensitive information.[86]

It is clear from the competing interpretations that the definition and language behind the "exceeds authorized access" clause is not as clear as what Congress intended it to be.[87] If so many courts and parties favored the broad approach, then why did the Supreme Court hold that individuals do not exceed authorized access when they obtain information for an improper purpose? The next Part will take a further look at the facts and procedure surrounding this decision. It will also address the competing arguments and interests at play and explain how the Supreme Court reached its conclusion in *Van Buren.*

---

[78] *See Whether the Computer Fraud and Abuse Act (CFAA) Should Be Interpreted to Create Liability for Violations of Computer Use Policies Including Website Terms of Service,* ACLU (July 13, 2020), https://www.aclu.org/cases/van-buren-v-united-states.

[79] Brief for Electronic Frontier Foundation et al. as Amici Curiae Supporting Petitioner, Van Buren v. United States, 141 S. Ct. 1648 (2021) (No. 19-783).

[80] Kenny, *supra* note 76.

[81] *Id.*

[82] *Id.*

[83] *See* Lapowsky, *supra* note 74.

[84] *Id.*

[85] *Id.*

[86] *Id.*

[87] *See* Paul J. Larkin, Jr., *U.S. v. Nosal: Rebooting the Computer Fraud and Abuse Act*, 8 SETON HALL CIR. REV. 257, 261 (2012) (explaining that the CFAA can be used in ways not intended by Congress).

III. THE CASE

A. Facts

It all began when Nathan Van Buren was a sergeant with the Cumming, Georgia Police Department.[88] In Van Buren's capacity as a sergeant, he came to know a man named Andrew Albo, who had a reputation in the Department for being "very volatile."[89] Despite his reputation, Van Buren developed a friendly relationship with Albo.[90]

One day, Van Buren approached Albo and asked him for a personal loan.[91] Unbeknownst to Van Buren, Albo secretly recorded the conversation and took it to the local county sheriff's office, where he complained that Van Buren attempted to "shake him down" for money.[92] Albo's complaint drew suspicion from the Federal Bureau of Investigation (FBI), and the FBI devised an operation to see how far Van Buren would actually go for the money.[93]

Over a series of meetings and communications monitored and recorded by the FBI, Albo put the plan into action when he asked Van Buren to look into a woman he met at a local strip club.[94] Albo claimed that he wanted to see if the woman was an undercover police officer and in return, he would provide Van Buren with cash.[95] The sting operation went according to plan when Van Buren agreed.

Using his valid police credentials to access the Georgia Crime Information Center ("GCIC") database, Van Buren searched the license plate information that Albo had provided.[96] Van Buren obtained the information from the database and contacted Albo to inform him that he had information to share.[97] The next day, the federal government arrived at Van Buren's doorstep[98] and charged him with a felony violation of the CFAA.[99]

---

[88] Van Buren v. United States, 141 S. Ct. 1648, 1653 (2021)

[89] *Id.*; *see also* United States v. Van Buren, 940 F.3d 1192, 1197 (11th Cir. 2019). The Deputy Chief of Police in the Cumming Police Department believed that Albo had a mental health condition and warned his officers to "be careful" with Albo. *Id.*

[90] *Id.* Van Buren first met Albo when he arrested him for providing alcohol a minor. *Id.* After handling various disputes between Albo and random women, Van Buren developed a relationship with Albo. *Id.* At the time, Van Buren was struggling with financial difficulties and believed that Albo could help improve his situation. *Id.*

[91] *Van Buren*, 940 F.3d at 1197. When Van Buren asked Albo for a loan, he falsely claimed he needed $15,368 to settle his son's medical bills. He explained to Albo that he could not obtain a bank because he had "shoddy" credit. *Id.*

[92] *Van Buren*, 141 S. Ct. at 1653.

[93] *Id.*

[94] *Id.*

[95] *Id.*

[96] *Id.*

[97] *Van Buren*, 141 S. Ct. at 1653.

[98] *Van Buren*, 940 F.3d at 1198. Van Buren admitted to the FBI that he had concocted a fake story about his son's need for surgery to justify asking Albo for money. Van Buren also confessed he had run a search for Albo and admitted that he knew doing it was "wrong." *Id.*

[99] *Id.* Van Buren was also charged with honest-services wire fraud in violation of 18 U.S.C. §§ 1343 and 1346. However, the United States Court of Appeals for the Eleventh Circuit vacated this conviction as it was contrary to the Court's decision in McDonnell v. United States, 579 U.S. 550 (2016). *Id.*

B. Procedural History and Issues

At trial, the Government claimed that Van Buren violated the "exceeds authorized clause" of the CFAA when he obtained information from the law enforcement database when he ran the license plate for Albo.[100] The Government presented evidence that Van Buren and other law enforcement officers were not allowed to use the law enforcement data base for personal use.[101] The Government additionally claimed that Van Buren violated the CFAA when he violated the department's policy preventing law enforcement officers from using the law enforcement databases for personal use.[102] The jury convicted Van Buren, and the District Court sentenced him to 18 months in prison.[103]

Van Buren subsequently appealed to the Eleventh Circuit, arguing that the "exceeds authorized access" clause only applies to those who obtain information to which their computer access does not extend–not to those who misuse access they otherwise have.[104] Relying on *United States v. Rodriguez,*[105] the Eleventh Circuit disagreed and held that Van Buren violated the CFAA by accessing the law enforcement database for an "inappropriate reason."[106]

The Supreme Court granted certiorari to resolve the circuit split in authority regarding the scope of liability under the CFAA's "exceeds authorized access" clause.[107]

C. The Parties' Arguments

On appeal to the United States Supreme Court, the parties agreed on three points: (1) that Van Buren "access[ed] a computer with authorization" when he used his patrol-car computer to log into the law enforcement databases; (2) that Van Buren obtained information in the computer when he acquired the license-plate record for Albo; and (3) that Van Buren had been given the right to acquire[108] the license-plate information.[109] However, the parties disagreed on whether Van Buren was "entitled so to obtain the information" as the statute requires.[110]

Van Buren argued that he was "entitled so to obtain" the license-plate information.[111] He claimed that the definition of the term "so," as used in the statute,

---

[100] *Van Buren*, 141 S. Ct. at 1653.

[101] *Id.*

[102] *Id.*

[103] *Id.*

[104] *Id.*

[105] *See Van Buren*, 940 F.3d at 1208 ("We acknowledge that other courts have rejected *Rodriguez's* interpretation of "exceeds authorized access" . . . [however] Van Buren has identified no Supreme Court or en banc decision of this Circuit that abrogates *Rodriguez,* [so] we must continue to follow it.").

[106] *Id.*

[107] *Van Buren*, 141 S. Ct. at 1654.

[108] *Id.* The parties agreed that Van Buren was "entitled to obtain" the license-plate information. *Id.* The definition of "entitle" means "to give a title, right or claim to something. Random House Dictionary of the English Language 649 (2d ed. 1987) . . . Black's Law Dictionary 477 (5th ed. 1979). ('to give a right or legal title to.')" The dispute, however, stems from whether Van Buren was "entitled so to obtain" the information.

[109] *Id.*

[110] *Id.*

[111] *Id.*

serves as a term of reference that recalls "the same manner as has been stated."[112] Thus, under Van Buren's interpretation, the question is whether Van Buren had the right, "in the same manner [as] has been stated," to obtain the license plate information.[113] Since the statute defines the manner of obtaining information "via a computer [one] is otherwise authorized to access,"[114] Van Buren contends that the disputed phrase–"is not entitled so to obtain"–only refers to information one is not allowed to obtain by using a computer that he is authorized to access.[115]

Under this interpretation, Van Buren did not violate the CFAA when he obtained information from the GCIC database because he had authorization to access the information, regardless of whether he pulled the license-plate record for a prohibited purpose. If, however, Van Buren pulled the information from a database in which he did not have access to, then his conduct would have violated the CFAA.[116]

On the other hand, the Government argued that the statute's use of the word "so" should be interpreted broadly.[117] The Government claimed that the phrase "is not entitled so to obtain" refers to information one was not allowed to obtain in the particular manner or circumstance in which he obtained it.[118] The manner or circumstances in which one has a right to obtain the information is defined by any "specifically and explicitly" communicated limits on one's right to access information.[119]

In other words, the Government claimed that a police officer could lawfully pull information from a database if he pulled that information for law enforcement purposes. If, however, he pulls the same information for a personal reason, then this would violate the CFAA.[120] Under this interpretation, employees are considered to "exceed authorized" access when they use their authorization for a purpose in which their authorization does not extend.

D. The Supreme Court's Holding

The Supreme Court held that an individual "exceeds authorized access" when he accesses a computer with authorization but then obtains information located in particular areas of the computer–such as files, folders, or databases–that are off-limits to him.[121]

---

[112] *Van Buren*, 141 S. Ct. at 1654.

[113] *Id.*

[114] *Id.*

[115] *Id.*

[116] *Id.* On this reading, if a person had access to information stored in a computer in Folder Y, they do not violate the CFAA by obtaining such information, regardless of whether they pulled the information for a prohibited purpose. But if the information is instead located in "Folder X," and the person does not have access to this folder, if the individual obtains the information located in this folder, they will have violated the CFAA. *Id.*

[117] *Van Buren*, 141 S. Ct. at 1654.

[118] *Id.*

[119] *Id.* at 1655.

[120] *Id.* Under the Government's reasoning, an employment might lawfully pull information from Folder Y in the morning for a permissible purpose-say, to prepare for a business meeting-but unlawfully pull the same information from Folder F in the afternoon for a prohibited purpose-say, to give the information to a competing employer. *Id.*

[121] *Id.* at 1649.

In a 6-to-3 decision,[122] the Supreme Court agreed with Van Buren's interpretation,[123] stating that the phrase "is not entitled so to obtain" is best read to refer to "information that a person is not entitled to obtain by using a computer that he is authorized to access."[124] The Supreme Court rejected the Government's broad interpretation of the phrase[125] and its contention that Van Buren's reading renders the word "so" as superfluous.[126] According to the Government, the term "so" adds nothing to the sentence if it refers solely to the earlier stated manner of obtaining the information through the use of a computer one has accessed with authorization.[127] The Government claimed that the language of the statute would not have changed even if the word "so" was deleted.[128] The Supreme Court disagreed and pointed out that without the word "so," the statute would allow individuals to use their right to obtain information in non-digital form as a defense to CFAA liability.[129] Additionally, the Supreme Court noted that Van Buren's account of the term "so" is reflected by other federal statutes[130] that use the word "so" in a similar manner.[131] As a result of this interpretation, the purpose for which the person obtained the information is irrelevant if the person was authorized to obtain the information.[132]

Therefore, the Supreme Court held that Van Buren did not exceed his authorized access as the CFAA defines the phrase.[133] Relying on the structure of the statute, the Court noted that the statute specifies two ways of obtaining information

---

[122] *Id.* Van Buren illustrates how two originalists–Justice Amy Coney Barrett, writing for the majority opinion, and Clearance Thomas, writing for the dissent-both focus on the original meaning of the statute and yet arrive at different conclusions. *Id.*

[123] *Van Buren*, 141 S. Ct. at 1649. "Van Buren's account of 'so' best aligns with the term's plain meaning as a term of reference, as further reflected by other federal statutes that use 'so the same way.'" *Id.*

[124] *Id.* at 1655. "'So' is not a free-floating term that provides a hook for any limitation stated anywhere. It refers to a stated, identifiable proposition from the 'preceding' text; indeed, 'so' typically '[r]epresent[s]' a 'word or phrase already employed,' thereby avoiding the need for repetition . . . Webster's Third New International Dictionary 2160 (1986)." "[S]o [is] often used as a substitute to express the idea of a preceding phrase." *Id.*

[125] *Id.* at 1649. The dissent accepts Van Buren's definition of the term "so," but would arrive at the Government's result by way of the word "entitled." According to the dissent, the term "entitled" demands a "circumstance dependent" analysis of whether access was proper. *Id.*

[126] *Id.* at 1656.

[127] *Id.*

[128] *Van Buren*, 141 S. Ct. at 1656.

[129] *Id.* (giving the example that a person who downloads restricted files, who is not entitled to obtain them by using his computer, could argue that he was "entitled to obtain" the information through another source (e.g., by requesting hard copies of the files)).

[130] *See* 7 U.S.C. § 171(8) (2022) (authorizing Secretary of Agriculture "[t]o sell guayule or rubber processed from guayule and to use funds so obtained in replanting and maintaining an area"); 18 U.S.C. § 648 (2022) (stating any person responsible for "safe-keeping of the public moneys who loans uses, or converts to his own use . . . any portion of the public moneys is guilty of embezzlement of the money so loaned, used, converted, deposited or exchanged"); 18 U.S.C. § 1708 (2022). "[W]hoever steals, takes, or abstracts, or by fraud, or deception obtains, or attempts so to obtain, parcels of mail is subject to punishment." *Id.*

[131] *Van Buren*, 141 S. Ct. at 1649.

[132] *See "So" What? SCOTUS Limits Scope of Computer Fraud and Abuse Act*, MOORE & VAN ALLEN (July 6, 2021), https://www.jdsupra.com/legalnews/so-what-scotus-limits-scope-of-computer-8047248/.

[133] *Van Buren*, 141 S. Ct. at 1649.

unlawfully.[134] First, when an individual "access[es] a computer without authorization," and second, "when an individual 'exceeds authorized access' by accessing a computer 'with authorization,' and then obtaining information he is 'not entitled so to obtain.'"[135] Thus, the Supreme Court articulated a gates-up-or-down inquiry–one either can or cannot access a computer system, and one either can or cannot access certain areas within the system.[136] As a result, Van Buren's conviction was reversed.

IV. ANALYSIS

The Supreme Court has resolved the long standing debate centered around the interpretation of the "exceeds authorized access" clause.[137] As a result of the *Van Buren* decision, millions of Americans are no longer in danger of committing a federal crime when they check Facebook at work, are dishonest on an online dating profile, or use their work Zoom account to chat with relatives.[138] Accordingly, this Part will analyze the Supreme Court's interpretation of the "exceeds authorized access" clause of the CFAA and argue that the Supreme Court was correct in its interpretation. In support of this argument, this Part will analyze the "gates-up-or-down approach" and address the "parade of horribles" that would stem from the Government's broad interpretation. Next, this Part will discuss issues that *Van Buren* did not address as well as explain the implications this decision has on employers and future litigation.

A. The Gates-Up-Or-Down Approach

Van Buren was the first case involving an interpretation of Section 1030(a)(2) of the CFAA to reach the Supreme Court. Its importance and reach cannot be overstated.[139] Before *Van Buren,* the overly broad language of the CFAA created an opportunity for unscrupulous prosecutors to arbitrarily prosecute individuals.[140] By

---

[134] *Id.* at 1650.

[135] *Id. See* 18 U.S.C. §§ (a)(2), (e)(6) (2022).

[136] *Id.*

[137] *See* Aashish Mittal, *Circuit Split of CFAA Resolved by the Supreme Court*, IPLEADERS (Sept. 15, 2021), https://blog.ipleaders.in/circuit-split-cfaa-resolved-supreme-court/.

[138] *See* Michael J. Ellis, *High Court Got It Right in Van Buren v. U.S.: Prosecute Hacking, Not Terms of Service Violations*, THE HERITAGE FOUND. (June 7, 2021), https://www.heritage.org/courts/commentary/high-court-got-it-right-van-buren-v-us-prosecute-hacking-not-terms-service.

[139] *See SCOTUS Decision Ushers in the "Gates Up or Down" Era for Employers Seeking to Protect Workplace Computers and ESI*, FISHER PHILLIPS (July 6, 2021), https://www.fisherphillips.com/news-insights/scotus-decision-ushers-era-for-employers.html.

[140] *See* Scott Ikeda, *Supreme Court Decision on Van Buren Restricts Excesses of CFAA, Is a Boon for Cybersecurity Research*, CPO MAG. (June 8, 2021), https://www.cpomagazine.com/cyber-security/supreme-court-decision-on-van-buren-case-restricts-excesses-of-cfaa-is-a-boon-for-cybersecurity-research/. ("[The CFA's] [o]verly broad language has created opportunity for unscrupulous prosecutors to levy excessive charges into plea deals and excessive sentences for over three decades.").

defining the phrase "exceeds authorized access," the Supreme Court has notably set the stage for future workplace litigation by limiting the scope of the CFAA.[141]

In writing for the majority opinion, Justice Amy Coney Barrett interpreted the phrase to apply to "individual[s] who access a computer with authorization but then obtain information [that is] located in a particular area of [the] computer that [is] off-limits to them."[142] The Supreme Court correctly came to this conclusion because the text and structure of the statute itself support this interpretation.

The Supreme Court was correct in its decision to reject the Government's approach because the Government's argument contained several structural problems.[143] Recall the two ways in which a violation could occur under the CFAA. The first type of violation occurs when an individual "accesses a computer without authorization."[144] This clause typically protects computers from outside hackers, usually those who access a computer without any permission at all.[145] The second type of violation occurs when an individual "exceeds authorized access" by accessing a computer with authorization and obtaining information they are not entitled to obtain.[146] This clause targets insider hackers, individuals who access a computer with permission, but then "'exceed' the parameters of authorized access by entering an area of the computer to which [that] authorization does not extend."[147] Following this framework, the Supreme Court correctly articulated the "gates-up-or-down" inquiry.[148] Under this approach, one either can or cannot access a computer system, and one either can or cannot access certain areas within that system.[149]

On appeal, the Government agreed that the phrase "without authorization" should be analyzed by a gates-up-or-down inquiry but believed that the "exceeds authorized access" phrase should be determined circumstance by circumstance.[150] This approach, however, applies an inconsistent analysis[151] of the two prohibitions within the statute.[152] Van Buren's interpretation is more persuasive because it "harmonize[s] both prongs of liability" under the CFAA by treating both parts consistently.[153]

---

[141] *See SCOTUS Decision Ushers in the "Gates Up or Down" Era for Employers Seeking to Protect Workplace Computers and ESI*, *supra* note 139.

[142] *Van Buren*, 141 S. Ct. at 1662.

[143] *See id.* at 1659. "The Government's position has another structural problem." *Id.*

[144] 18 U.S.C. § 1030(a)(2) (2022).

[145] *Van Buren*, 141 S. Ct. at 1658.

[146] 18 U.S.C. § 1030(a)(2) (2022).

[147] *Van Buren*, 141 S. Ct. at 1658.

[148] *Id.*

[149] *Id.* at 1658–59.

[150] *Id.* at 1659.

[151] *See* John A. Drake & Amy E. Jensen, *Supreme Court Weighs in on Computer Fraud and Abuse Act*, THE NAT'L L. REV. (June 23, 2021), https://www.natlawreview.com/article/supreme-court-weighs-computer-fraud-and-abuse-act. ("The Court noted that the approach applied an 'inconsistent' analysis to the two prohibitions within, while Van Buren's 'gates-up-or-down inquiry' treated them consistently.").

[152] *See Van Buren*, 141 S. Ct. at 1659. "[T]he Government's reading of the 'exceeds authorized access' clause creates 'inconsistenc[ies] with the design and structure' of subsection (a)(2)" (quoting Univ. of Tex. Sw. Med. Ctr. v. Nassar, 570 U.S. 338, 353 (2013)). *Id.*

[153] Thor Y. Urness & Mike Stephens, *Supreme Court Limits Scope of Computer Fraud and Abuse Act, Ending Deep Circuit Split,* BRADLEY (June 10, 2021), https://www.bradley.com/insights/publications/2021/06/supreme-court-limits-scope-of-computer-fraud-and-abuse-act-ending-deep-circuit-split.

Additionally, his interpretation aligns with the computer-context understanding of access as entry.[154]

The statute's structure further cuts against the Government's position.[155] Recall that a violation under Section 1030(a)(2) of the CFAA gives rise to civil liability as well as criminal liability.[156] Under Section 1030(e)(8) and (e)(11), the CFAA defines "damage" and "loss" to determine what a plaintiff could recover in a civil suit.[157] "[D]amage," is defined as "any impairment to the integrity or availability of data, a program, a system, or information."[158] Similarly, the term "loss" relates to costs caused by harm to computer data, programs, systems, or information services.[159] These statutory definitions thus focus on harms that are typically associated with traditional hacking techniques-not harms that result from the improper use of the information.[160] The statute, therefore, is ill-suited to deal with conduct that relates to the misuse of computer access.[161]

By the plain language of the statute, the CFAA was not meant to cover situations in which someone used their authorized access for an improper purpose. Nonetheless, the Government argued that the Court should look at precedent[162] and used the CFAA's statutory history to support its interpretation.[163] The original version of the "exceeds authorized access" clause of the CFAA covered "any person who "accessed a computer with authorization, [and] use[d] the opportunity [that] such access provides for purposes [in] which [the] authorization does not extend."[164] The Government argued that this version of the CFAA supports its claim that the CFAA should apply to circumstance-based restrictions.[165] This argument fails because Congress removed any reference to "purpose" when it amended the statute in 1986.[166]

---

[154] *Van Buren*, 141 S. Ct. at 1659. The Supreme Court noted that Van Buren's gates-up-or-down reading of the statute aligns with the CFAA's prohibition on password-trafficking. Enacted alongside the "exceeds authorized access" clause defining the provision, the password-trafficking provisions bars the sale of "any password or similar information through which a computer may be accessed without authorization" under § 1030(a)(6). This provision is consistent with *Van Buren* because it turns on whether a user's credentials allow him to proceed past a computer's access gate, rather than focusing on scope-based restrictions. *See id.* at 1659 n.9.

[155] *Id.* at 1649.

[156] 18 U.S.C. § 1030(g) (2022); *Id.* at 1659.

[157] *Van Buren*, 141 S. Ct. at 1659–60.

[158] 18 U.S.C. § 1030(e)(8) (2022).

[159] 18 U.S.C. § 1030(e)(11) (2022).

[160] *See Van Buren*, 141 S. Ct. at 1660. "The statutory definitions of 'damage' and 'loss' thus focus on technological harms—such as corruption of files—of the type of unauthorized users cause to computer systems and data." *Id.* The majority opinion stated that the CFAA's intent is to create a system of punishment for hacking, not to govern situations where one party misuses information. *Id.*

[161] *Id.* "The term's definitions are ill fitted, however, to remediating 'misuse' of sensitive information that employees may permissibly access using their computers." *Id.*

[162] *Id.* The Government argued that the Supreme Court's decision in *Musacchio* supported its interpretation of the CFAA. The Supreme Court, however, claimed that it was not required to follow any dicta in the case. *See id.* at 1661. "*Musacchio* did not address-much less resolve in the Government's favor-the 'point now at issue,' and we thus 'are not bound to follow' any dicta in the case." *Id.*

[163] *Id.*

[164] 18 U.S.C. § 1030(a)(2) (2022).

[165] *Van Buren*, 141 S. Ct. at 1661.

[166] *Id.* at 1660 (citing Ross v. Blake, 578 U.S. 632, 641–42 (2016)). "When Congress amends legislation, courts must presume it intends the change to have real and substantial effect." *Id.*

Additionally, the CFAA's historical and statutory context establishes that Congress sought to "prevent intentional intrusion onto someone else's computer-specifically computer hacking."[167] This is in stark contrast with the Government's claim that the CFAA was intended to cover purpose-based limitations. The legislative history also indicates that the law was "designed to target hackers who accessed computers to steal information or to disrupt or destroy computer functionality."[168] As a practical matter, the CFAA's legislative history cuts against reading the statute to cover purpose-based limitations.[169]

Along with the structural problems articulated above, there are policy implications that support the Supreme Court's interpretation of the CFAA.[170] While one might think that it is against public policy to acquit a corrupt police officer who took a bribe and used his law enforcement database authorization against department policy,[171] there are other policy implications that trump this concern.[172] If the Court upheld Van Buren's CFAA charge, it could have cleared the path for the Government to impose criminal liability upon individuals who violate contractual agreements, employer policies, and/or terms of service agreements.[173]

The next Part will discuss the public policy issues at play in *Van Buren*. It will also address the "parade of horribles" that would have been reality if the Supreme Court had adopted the broad interpretation of the CFAA.

B. The Parade of Horribles

There is a well-known legal maxim that states "hard cases make bad law."[174] This phrase stands for the proposition that an extreme case is a poor basis for a general law that would cover a wider range of less extreme cases.[175] The CFAA is a solution to a specific problem, not a prohibition on all forms of computerized wrongdoing.[176]

---

[167] HiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985, 1000 (9th Cir. 2019).

[168] LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1130–31 (9th Cir. 2009) (citing H.R. REP. NO. 98–894).

[169] *Van Buren*, 141 S. Ct. at 1649.

[170] *See* Urness, *supra* note 153 ("Lastly, the Court pointed to policy reasons supporting Van Buren's narrow reading of the CFAA.").

[171] Jonathan Knowles, *The Scope of the Computer Fraud and Abuse Act After Van Buren*, BURNHAM & GOROKHOV, https://www.burnhamgorokhov.com/the-scope-of-the-computer-fraud-and-abuse-act-after-van-buren/ (last visited Apr. 19, 2022).

[172] *See id.* In criminal law, there is a saying that "it is better that ten guilty persons escape liability than that one innocent suffer;" *see also Blackstone's Ratio: Is it More Punishable to Protect Innocence or Punish Guilt?*, CATO INST., https://www.cato.org/policing-in-america/chapter-4/blackstones-ratio (last visited Apr. 19, 2022). A similar proposition should apply to *Van Buren*. As a matter of policy, it is better to narrowly interpret the CFAA so that individuals who misuse computer authorization are not found guilty of conduct that is not otherwise criminal. *Id.*

[173] Ikeda, *supra* note 140. "While the sergeant clearly did something wrong, if the court had upheld the CFAA charge it might have cleared a path for end user license agreements (EULA) and terms of service (TOS) to become enforceable by criminal law if violated." *Id.*

[174] *See* N. Sec. Co. v. United States, 193 U.S. 197, 400 (articulating the phrase "hard cases make bad law.").

[175] F.A. HAYEK, STUDIES ON THE ABUSE AND DECLINE OF REASON: TEXT AND DOCUMENTS 63 (2010).

[176] Knowles, *supra* note 171.

Accordingly, the broad interpretation of the CFAA would have criminalized widespread behavior and the Supreme Court was correct in its decision to reject it.[177]

Van Buren acknowledged that the Government's broad interpretation would lead to a scenario in which any computer misuse would give rise to CFAA liability.[178] In his oral argument to the Supreme Court, Van Buren's attorney articulated a "parade of horribles" that could result from such an interpretation.[179] Under the "parade of horribles," an employee who uses their zoom account to connect with relatives, a law student who uses their Westlaw or Lexis access for work, and a person who lies about their age on a dating website[180] would all be subject to CFAA liability.[181]

In its analysis, the Supreme Court noted that employers commonly prevent employees from using their computers for non-business purposes and that any individual who sends a personal email or reads the news at work would be in violation of the CFAA.[182] Additionally, the Supreme Court pointed out that many websites and databases authorize a user's access only if he or she agrees to follow the specified terms of service.[183] If a person were to violate one of these terms of services,[184] then that individual would also be subject to CFAA liability.[185] Thus, as a matter of policy, the Court held that the Government's interpretation "would attach criminal penalties to a breathtaking amount of commonplace computer activity."[186] In sum, the Court concluded that "millions of otherwise law-abiding citizens would be criminals if the CFAA [was] read to criminalize every violation of a computer-use policy."[187]

The CFAA would not only criminalize commonplace activity, but it would also give employers and private companies the power to arbitrarily determine what conduct is criminal.[188] Under a broad interpretation of the statute, employers using computer-use policies could transform categories of otherwise innocuous behavior into federal

---

[177] *See* Joshua A. Mooney, *False Accounts On Social Media Does Not Violate The Computer Fraud And Abuse Act*, WHITE AND WILLIAMS (Oct. 11, 2013). "[A] broad interpretation of the [CFAA] would criminalize widespread behavior." *Id.*

[178] Oral Argument at 5:25, Van Buren v. United States, 141 S. Ct. 1648 (2021) (No. 19-783), https://www.supremecourt.gov/oral_arguments/audio/2020/19-783.

[179] *Id.* at 0:58.

[180] *Id.*

[181] *Id.* at 1:19. "If the government is right, then a computer user who disregards any of these stated use restrictions commits a federal crime." *Id.*

[182] *Van Buren*, 141 S. Ct. at 1661.

[183] *Id.*

[184] *Id.* Under the Government's reading of the CFAA, the Supreme Court noted that an individual who uses a pseudonym on Facebook would be subject to CFAA liability.

[185] *Id.* "If the 'exceeds authorized access' clause encompasses violations of circumstance-based access restrictions on employers' computers, it is difficult to see why it would not also encompass violations of such restrictions on website providers' computers." *Id.*

[186] *Id.*

[187] *Van Buren*, 141 S. Ct. at 1661. In response to this point, the Government argued that the terms "authorization," "use," and "may well" would limit its prosecutorial power. However, it failed to cite any precedent in which a court has read the statute to contain such limitations. Instead, Van Buren cited to cases in which prosecutions were brought based on "de minimis harm." *Id.*

[188] *See Van Buren v. United States*, ELEC. FRONTIER FOUND., https://www.eff.org/cases/van-buren-v-united-states#:~:text=Van%20Buren%20v.-,United%20States,overbroad%20interpretation%20of%20the%20law (last visited Apr. 19, 2022). "If violating terms of service is a crime, private companies get to decide who goes to prison and for what, putting us all at risk for everyday online behavior." *Id.*

crimes simply because a computer is involved.[189] The Supreme Court explored the consequences of imputing criminal liability based on a violation of a computer use policy.[190] Accordingly, the Court noted that the Government's approach would inject "arbitrariness into the assessment of criminal liability."[191] The Court surprisingly declined to invoke the rule of lenity[192] in order to resolve this issue.[193] The rule of lenity provides that if there is an ambiguity in a criminal statute, courts should resolve all doubts in favor of the defendant.[194] This rule protects the rights of potential defendants by warning them about what conduct is considered criminal under a statute.[195] The majority opinion declined to invoke the rule of lenity because the text, context, and structure supported Van Buren's reading of the CFAA.[196] This is quite shocking considering the federal circuit courts, and even the justices themselves,[197] had a difficult time interpreting the "exceeds authorized access clause." If the text, context and structure clearly support the narrow interpretation, then why did the circuit courts disagree for so long?

Even though the Supreme Court did not come to its decision by implementing the rule of lenity, it nonetheless came to the correct conclusion. By relying on the text, structure, and policy implications, the Court recognized the tremendous danger of an overly broad CFAA.[198] Now, if an individual checks his Facebook at work, he will no longer be subject to criminal prosecution. He may still be subject to other disciplinary actions but he will no longer have the threat of criminal prosecution hanging over his head.

---

[189] United States v. Nosal, 676 F.3d 854, 860 (9th Cir. 2012). "[The CFAA's] ill-defined terms may capture arguably innocuous conduct, such as password sharing among friends and family, inadvertently mak[ing] criminals of large groups of people who would have little reason to suspect they are committing a federal crime." *Id.*

[190] *See Van Buren*, 141 S. Ct. at 1661. There were many parties that had an interest in the *Van Buren* litigation. *Id.* Many organizations filed *Amici Curiae* briefs to explain the disastrous effect the broad interpretation of the "exceeds authorized access" clause would have on these parties. Accordingly, when rejecting the broad interpretation, the Supreme Court cited these briefs to support its decision. *Id.*

[191] *Id.* at 1662.

[192] *Id.* at 1661. The rule of lenity is one of the oldest principles governing statutory interpretation. It is "founded on . . . the plain principle that the power of punishment is vested in the legislative, not in the judicial department.; *see also* United States v. Wiltberger, 18 U.S. (5 Wheat.) 76, 95 (1820).

[193] *See Van Buren*, 141 S. Ct. at 1661 ("Van Buren frames the far-reaching consequences of the Government's reading as triggering the rule of lenity or constitutional avoidance. That is not how we see it: Because the text, context, and structure support Van Buren's reading, neither of these cannons is in play.").

[194] *See* United States v. Bass, 404 U.S. 336, 348 (1971); Aaron Mackey & Kurt Opsahl, *Van Buren is a Victory Against Overbroad Interpretation of the CFAA, and Protects Security Researchers*, ELEC. FRONTIER FOUND. (June 3, 2021), https://www.eff.org/deeplinks/2021/06/van-buren-victory-against-overbroad-interpretations-cfaa-protects-security (defining the rule of lenity).

[195] United States v. Lanier, 520 U.S. 259, 266 (1997).

[196] *Van Buren*, 141 S. Ct. at 1661.

[197] *See id.* at 1656. The *Van Buren* dissent criticizes the majority's interpretation of the "exceeds authorized access" clause as being inconsistent with "basic principles of property law." In turn, the majority notes that it was the failure of pre-existing law to capture computer crime that helped Congress enact the CFAA in the first place.

[198] Mackey, *supra* note 194.

C. Van Buren's Implications on Future Litigation

The *Van Buren* decision presents significant ramifications for employers concerned with protecting sensitive information and it has far-reaching effects on civil litigation[199] as well.[200] Pre *Van Buren*, many companies, who provided their employees with access to sensitive and proprietary data, used the CFAA as a litigation tool against those who misappropriated, misused, or compromised the data on its networks.[201] The Court's decision in *Van Buren* now sharply limits the ability of companies to use the CFAA against company insiders.[202]

This decision not only protects computer users from overzealous prosecutors and vindictive employers, but also creates a magnitude of problems for employers.[203] The *Van Buren* decision inadvertently provides protection for whistleblowers and other employees with claims against their employers.[204] Before *Van Buren,* the threat of litigation and prosecution under the CFAA was used to deter whistleblowers and other potential defendants from collecting documents and other information to prove that their employer had either engaged in fraud or violated their rights.[205] Employers would often file counterclaims against whistleblowing plaintiffs, alleging that those plaintiffs "exceeded their authorized access" when taking documents to prove his or her claim.[206] By filing or threatening to file a CFAA counterclaim, employers had the ability to chill

---

[199] *See SCOTUS Limits Scope of Computer Fraud and Abuse Act, Which Could Impact Terms of Use Agreements*, DUANE MORRIS (June 21, 2021), https://www.duanemorris.com/alerts/scotus_limits_scope_computer_fraud_abuse_act_which_could_impact_terms_use_agreements_0621.html ("Justice Barrett's heavy reliance on the expansive reading's real world effects . . . provides clues for future rulings interpreting the CFAA.").

[200] *See* Aime Dempsey, *What's "So" Important: Computer Fraud and Abuse Act Gets a Close Look From the U.S. Supreme Court*, EPSTEIN BECKER GREEN (Jan. 25, 2021), https://www.ebglaw.com/wp-content/uploads/2021/07/Intellectual-Property-Technology-Law-Journal-Feb-2021-Dempsey.pdf; Kevin M. Cloutier & David M. Poell, *U.S. Supreme Court Case Preview*-Van Buren v. United States*: Does Use of a Computer for an "Improper Purpose" Violate the Computer Fraud and Abuse Act?*, THE NAT'L L. REV. (Apr. 30, 2020), https://www.natlawreview.com/article/us-supreme-court-case-preview-van-buren-v-united-states-does-use-computer-improper (explaining CFAA implications on civil litigation).

[201] Dempsey, *supra* note 200. In recent years, employers have relied on the CFAA's civil private right of action to target disloyal employees.

[202] Shay Dvoretzky, William Ridgway & Alexander J. Kasparie, *Supreme Court Outlines Bounds of the Computer Fraud and Abuse Act*, SKADDEN, ARPS, SLATE, MEAGHER & FLOM (June 7, 2021), https://www.skadden.com/insights/publications/2021/06/supreme-court-outlines-bounds.

[203] Nicolas Enrique O'Connor, *Whistleblowers Accessing Company Documents Likely Will Not Be Prosecuted Under The Computer Fraud And Abuse Act*, THE NAT'L L. REV. (Aug. 16, 2021), https://www.natlawreview.com/article/whistleblowers-accessing-company-documents-likely-will-not-be-prosecuted-under.

[204] *See* Todd Yoder, *Supreme Court Computer Access Decision Has Positive Implications For Whistleblowers*, THE NAT'L L. REV. (June 4, 2021), https://www.natlawreview.com/article/supreme-court-computer-access-decision-has-positive-implications-whistleblowers ("While the [Van Buren] case did not directly involve a whistleblower issue, the decision nevertheless held profound implications for whistleblowers.").

[205] *See* O'Connor, *supra* note 203. "Without the limitations imposed by *Van Buren*, a whistle blower who mistakenly takes documents unrelated to her claim, despite having authorized access to those documents, could face liability since her employer could claim the documents were taken for an 'improper purpose.'" *Id.*

[206] *Id.*

whistleblowing activity.[207] The *Van Buren* decision, however, limits an employer's ability to use the CFAA as a defense mechanism for curbing plaintiff's whistleblowing claims.[208]

Despite the fact that a CFAA claim or counterclaim will be more difficult for an employer to prove, employers still have other litigation avenues that they can pursue.[209] For example, trade secret laws provide employers a robust defense against employees who seek to use their former employers' information for improper purposes.[210] Similarly, the government can prosecute individuals who abuse their authorized access for personal gain.[211] The government can do this by charging individuals with wire fraud and honest services fraud, as it did in *Van Buren.*[212] One must note that even though *Van Buren* provides protection for employees who are sued under the CFAA, it does not stop the employer from pursuing other legal causes of actions. Additionally, employers can terminate an employee for improper use, especially if it violates company policy.[213] Nonetheless, the contours of the Court's ruling will undoubtedly affect employers who wish to bring CFAA claims against their employees.[214]

The *Van Buren* decision will similarly affect litigation for other parties as well.[215] In recent years, technology companies have used the CFAA and other legal

---

[207] *Id.*

[208] *Id.* "By limiting the CFAA to situations where an employee did not have any authorized access to the documents, the risk to a whistleblower of finding himself in an unanticipated litigation related to his efforts to gather evidence is substantially reduced." *Id.*

[209] O'Connor, *supra* note 203.

[210] *See* Yoder, *supra* note 204. "While trade secret laws still provide employers a robust defense against employees who seek to misappropriate their former employers' proprietary information or personal pecuniary gain, trade secrets apply in a much narrower set of circumstances than the 'exceeds authorized access' portion of the CFAA." *Id.*

[211] *Id.* "The government is not stymied in its ability to prosecute illegal, non-whistleblowing conduct." *Id.*

[212] *Id.*

[213] *Id.* Even if the employee's termination is proven to be unlawful, the after acquired evidence doctrine may limit an employee's recovery in a wrongful termination claim. *Id.* Under this doctrine, an employee may not be able to recover if the employer can prove that an employee's misconduct would have eventually led to termination. *Id.*

[214] Geoff Schweller, *Supreme Court Decision in Computer Access Case a Win for Whistleblowers*, WHISTLEBLOWER NETWORK NEWS (June 4, 2021), https://whistleblowersblog.org/false-claims-qui-tam-news/supreme-court-decision-in-computer-access-case-a-win-for-whistleblowers/ ("[W]ith the decision by the Court in *Van Buren*, it appears likely that . . . retaliatory tactics by . . . defendants will be foreclosed"); *see also* O'Connor, *supra* note 203:

> While employees with claims against their employers still face obstacles to pursuing their claims free of the risk of their employers' counterclaims, *Van Buren* eliminates a key barrier to ensuring justice for those whose rights have been violated and to battling fraud perpetrated upon investors, the government, and the public at large.

[215] *See* Jeffrey Neuburger, *Supreme Court Vacates LinkedIn-HiQ Scraping Decision, Remands to Ninth Circuit For Another Look*, THE NAT'L L. REV. (June 16, 2021), https://www.natlawreview.com/article/supreme-court-vacates-linkedin-hiq-scraping-decision-remands-to-ninth-circuit. On June 14, 2021, the Supreme Court granted LinkedIn Corp.'s petition for certiorari in a web scraping case involving the CFAA. It subsequently vacated the Ninth Circuit's

remedies to enforce terms of service violations.[216] The Supreme Court's decision limits CFAA applicability in cases where the defendant violated a website's term of service.[217] By holding that "an individual 'exceeds authorized access' when he accesses a computer with authorization but then obtains information located in particular areas of the computer that is off limits to him," the Supreme Court implicitly held that violations of circumstance-based access restrictions are not CFAA violations.[218] Under this reading, the Court established a "digital gate"[219] requirement which requires the defendant to have gone through some sort of barrier in order to trigger CFAA liability.[220] However, the Court did not firmly establish that the "digital case" must only apply to technical or code-based measures.[221]

In footnote eight of the *Van Buren* decision, the Court declined to address whether the gates-up-or-down approach turns only on technical or code-based limitations on access, or if it also looks to limits contained in contracts or policies.[222] By way of this footnote, the Court left open an important question:[223] Does the CFAA's technological and code-based limitations on access extend to limitations on contracts and policies? "The general tone of the Court's opinion seems to favor a bright line approach to technological limitations, rather than the more ambiguous question of when a contract or policy authorizes access."[224] Nonetheless, the Court "does not definitively resolve the question of whether unauthorized access must be barred by a hardware or software gateway or if activity can become 'unauthorized' by a contractual ban."[225] "Largely for that reason, the practical effects on the CFAA's civil enforcement provisions remain to be seen."[226]

Ultimately, the implications of the *Van Buren* decision are far-reaching.[227] Employers will have to rely on other types of claims to address employees who misuse

---

opinion and remanded the case back to the Ninth Circuit for further consideration in light of the Supreme Court's decision in *Van Buren*.

[216] Lapowsky, *supra* note 74. Recently, Facebook tried to shut down a research project at New York University. Facebook argued that the researchers' strategy violated its terms of services and claimed that it put Facebook at risk of violating its consent decree with the Federal Trade Commission. *Id.*

[217] *See* Mackey, *supra* note 194. "[P]rivate parties' terms of service limitations on how you can use information, or for what purposes you can access it, are not criminally enforced by the CFAA." *Id.*

[218] *Van Buren*, 141 S. Ct. at 1649.

[219] Ikeda, *supra* note 140.

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

[221] *Id.*

[222] *Van Buren*, 141 S. Ct. at 1659 n.8.

[223] *See* Ikeda, *supra* note 140. "While opponents of the CFAA consider this an important victory, it does not address all of the issues with the law." *Id.*

[224] Knowles, *supra* note 171.

[225] *See SCOTUS Limits Scope of Computer Fraud and Abuse Act, Which Could Impact Terms of Use Agreements*, *supra* note 199.

[226] *Id.*; *see also* Mackey, *supra* note 194. "[L]eaving the question open means that we will have to litigate whether and under what circumstances a contract or written policy can amount to an access restriction in the years to come." *Id.*

[227] *See* Jon Knight, *The Supreme Court Narrows The Scope of The Computer Fraud and Abuse Act*, ALSTON & BIRD (June 3, 2021), https://www.alstonprivacy.com/the-supreme-court-narrows-the-scope-of-the-computer-fraud-and-abuse-act/ ("*Van Buren* serves as a useful reminder that employers must be vigilant about controlling access to its internal computer systems.").

electronically stored information.[228] In light of this decision, companies may also need to revisit the language of their internal corporate policies and employee handbooks to find alternative solutions for deterring or penalizing unwanted conduct.[229] Employers should have clear policies and procedures that prohibit improper access to confidential information, and they should use confidentiality agreements for employees who are authorized to access sensitive data.[230] To increase the likelihood that it will have recourse under the CFAA, employers should adopt company policies that narrowly limit the users who have access to sensitive information and employ electronic barriers to prohibit employees from accessing particular data or areas of the computer network.[231] Additionally, companies that are heavily dependent on terms of use and internal corporate policies to protect sensitive data should stay up-to-date on continued developments in the law.[232] The *Van Buren* decision has significant implications on how organizations should protect confidential and sensitive information from insider threats and other individuals legitimately on their computer networks.[233] It will have a large impact on civil litigation and courts will likely continue to examine the *Van Buren* decision for years to come.[234]

V. CONCLUSION

The Supreme Court's decision in *Van Buren* ended the long standing circuit split between the federal courts and has provided much-needed clarity on the issues surrounding the Computer Fraud and Abuse Act.[235] Employers, consumers,

---

[228] *See Supreme Court in Van Buren Narrows Scope of the Computer Fraud and Abuse Act*, DORSEY & WHITNEY (June 16, 2021), https://www.dorsey.com/newsresources/publications/client-alerts/2021/06/supreme-court-in-van-buren ("While the CFAA may no longer provide a legal remedy for many types of improper computer access, employers still have a number of tools available to protect sensitive business information.").

[229] Knight, *supra* note 227.

[230] *Supreme Court in Van Buren Narrows Scope of the Computer Fraud and Abuse Act, supra* note 228.

[231] *U.S. Supreme Court Narrows the Scope of Federal Anti-Hacking Law in* Van Buren v. United States, SULLIVAN & CROMWELL (June 4, 2021), https://www.sullcrom.com/files/upload/sc-publication-supreme-court-narrows-scope-federal-anti-hacking-law-van-buren-united-states.pdf.

[232] Knight, *supra* note 227.

[233] Sumon Dantiki, Scott Ferber, Zachary Harmon & Bethany Rupert, *Supreme Court Decision on Computer Fraud and Abuse Act: Implications for Cybersecurity and Insider Threat Programs*, KING & SPALDING (June 25, 2021), https://www.jdsupra.com/legalnews/supreme-court-decision-on-computer-8704865/.

[234] Hannah T. Joseph, *Supreme Court Narrows Computer Fraud and Abuse Act*, N. ENG. BIZ L. UPDATE (July 8, 2021), https://newenglandbizlawupdate.com/2021/07/08/supreme-court-narrows-computer-fraud-and-abuse-act/#:~:text=In%20a%206%2D3%20decision,or%20databases%20%E2%80%94%20that%20are%20off

[235] *Supreme Court to Resolve Longstanding Circuit Split Over Scope of Federal Anti-Hacking Statute*, GIBSON DUNN (Apr. 20, 2021), https://www.gibsondunn.com/supreme-court-to-resolve-longstanding-circuit-split-over-scope-of-federal-anti-hacking-statute/; *see also* Sabrina Marcos Smith & Dennis Vacco, *'Leave the Date Up or Leave it Down': The Supreme Court's Recent Decision Marks Changes in the Landscape of Cybersecurity and Privacy in Corporate America*, LIPPES MATHIAS (July 12, 2021), https://www.jdsupra.com/legalnews/leave-the-gate-up-or-leave-it-down-the-5566337/ ("The Supreme Court's recent decision in *Van Buren* . . . puts an end to any potential ambiguity regarding authorization and clearly defines the parameters of authority outlined in the CFAA.").

prosecutors, and law enforcement officials now have a better understanding of what type of computer conduct is subject to civil and criminal liability under the CFAA.[236]

The Supreme Court correctly held that an individual does not violate the CFAA when he or she obtains information from a computer and uses it for an improper purpose so long as he or she was authorized to access the computer and obtain the information in the first place. The statute now only imposes liability when a person hacks into, or accesses, an electronic database that the person does not have permission to access.[237] The Court rightfully came to this conclusion because the text, structure, and legislative history clearly indicate that the CFAA was meant to combat computer hacking, not police those who misuse information they are otherwise authorized to obtain. Penalizing individuals who misuse information on a computer would criminalize commonplace activity and give employers the power to determine what conduct is criminal.[238] Accordingly, the Supreme Court correctly reversed Van Buren's conviction under the CFAA.

The *Van Buren* decision will inevitably affect how employers pursue legal remedies against employees who have authorized access to computer networks.[239] The CFAA will no longer be available in situations in which an employee obtains information on a computer for an unauthorized purpose.[240] As a result, employers must now look to other state and federal statutes to resolve their claims.[241] The *Van Buren* decision will also have broad implications on trade secret litigation.[242] An employer may no longer establish a CFAA violation based solely on an employee downloading, destroying, or misappropriating confidential employer information in violation of a company's computer-use policy.[243] In light of *Van Buren*, employers concerned with

---

[236] *Supreme Court to Resolve Longstanding Circuit Split Over Scope of Federal Anti-Hacking Statute, supra* note 235.

[237] *Supreme Court Narrows Scope of Computer Fraud and Abuse Act in* Van Buren v. United States, *supra* note 59.

[238] *Van Buren*, *No Not the Eighth*, CAA FLOG (June 8, 2021), http://www.caaflog.org/home/van-buren-no-not-the-eighth ("When technological advancement is ever-expanding, the Supreme Court rightfully acknowledged the dangers of criminalizing every trivial violation of a 'computer-use policy.'").

[239] Hotaling, *supra* note 23.

[240] *See* Connie Elder Carrigan, *SCOTUS Resolves Circuit Split Regarding Scope of The Computer Fraud and Abuse Act*, SMITH DEBNAM (July 13, 2021), https://www.smithdebnamlaw.com/2021/07/scotus-resolves-circuit-split-regarding-scope-of-the-computer-fraud-and-abuse-act/. "Following *Van Buren*, it is no longer relevant for purposes of CFAA liability that an employee obtains computer information for an improper purpose." *Id.* The CFAA may still be available to companies in limited situations. Moving forward, to prevail under the CFAA, an employer must demonstrate that the employee exceed his authorized access by obtaining information and accessing a computer, file, folder, or database that was off-limits to the employee. *Id.*

[241] *See* Kathleen Grossman & Jeffrey McPhaul, *Supreme Court Limits Claims Under Computer Fraud and Abuse Act*, LOCKE LORD (July 27, 2021), https://www.jdsupra.com/legalnews/supreme-court-limits-claims-under-9201926/ ("Although the Supreme Court limited companies' use of the CFAA against employees, there are many laws which employers can effectively use in response to misappropriation of confidential information and trade secrets, including the federal Defend Trade Secrets Act and state trade secret laws, as well as the common law duty of loyalty.").

[242] Jean E. Dassie, *U.S. Supreme Court Limits Scope of Employee-Employer Liability Under the CFAA*, N.J L. J. (Sept. 30, 2021), https://www.law.com/njlawjournal/2021/09/30/supreme-court-limits-scope-of-employee-employer-liability-under-the-cfaa/?slreturn=20220319210452.

[243] *Id.* A district court in the Third Circuit has already relied on the *Van Buren* decision to dismiss a CFAA claim based on misuse of confidential information. *See* KBS Pharm. v. Patel, No. 21-1339,

employees misusing information stored on company computers should reassess their security policies.[244] Additionally, companies should limit each employee's computer access to only the files, folders, and databases that are necessary to carry out the employee's individual job responsibilities.[245]

While *Van Buren* provides a much-needed check on the CFAA, it left many questions unanswered.[246] Even though the Supreme Court interpreted the "exceeds authorized access" clause, it did not explicitly address what types of barriers an employee must breach to exceed authorized access under the CFAA.[247] The Supreme Court declined to address whether a technological barrier must have been breached or whether a violation of a written policy is sufficient to trigger CFAA liability.[248] The *Van Buren* decision thus leaves open the question of whether violations of contractual restrictions may give rise to liability under the "exceeds authorized access" clause of the CFAA.[249] Hopefully, the next generation of litigation will provide answers to the issues that the Court declined to address.[250]

Nevertheless, the *Van Buren* decision forecloses any implication that criminal or civil liability may rise if an individual accesses information for an improper purpose.[251] While the decision does not address all issues and scenarios that may arise under the CFAA, it certainly is a step in the right direction.[252] Now any employee who accesses Facebook on their work computer can breathe a little easier knowing that

---

2021 U.S. Dist. LEXIS 107779, at *6 (E.D. Pa. June 9, 2021) (dismissing a CFAA claim because "[t]he CFAA simply does not encompass the employee's misuse of the information if the employee had authorized access to the information in the computer in the first place.").

[244] Lauren S. Frisch, *Supreme Court Rules on Computer Fraud and Abuse Act: What Should Employers Do Now?*, BERMAN FINK VAN HORN (July 30, 2021), https://www.bfvlaw.com/supreme-court-rules-on-computer-fraud-and-abuse-act-what-should-employers-do-now/.

[245] *Id.*

[246] John Villasenor, *Reining in Overly Broad Interpretations of the Computer Fraud and Abuse Act*, BROOKINGS (June 7, 2021), https://www.brookings.edu/blog/techtank/2021/06/07/reining-in-overly-broad-interpretations-of-the-computer-fraud-and-abuse-act/. The *Van Buren* decision clarifies the "exceeds authorized access" clause, however, it does not clarify what it means to have "authorized access." *Id.*

[247] *See* Van Buren v. United States, 141 S. Ct. 1648, 1659 n.8 (2021). "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." *Id.*

[248] Grossman, *supra* note 241.

[249] Van Buren v. United States*: Supreme Court Holds Access Information on a Computer for Unauthorized Purposes Not Federal Crime*, CONGRESSIONAL RSCH. SERV. (July 1, 2021), https://crsreports.congress.gov/product/pdf/LSB/LSB10616/2.

[250] David Barnard, Scott Eidson, Kevin Conneely, Jason Conaway, Steve Cosentino & Nicci Warr, *Justices Clarify Scope of Anti-Hacking Law*, STINSON (June 10, 2021), https://www.stinson.com/newsroom-publications-Justices-Clarify-Scope-of-Anti-Hacking-Law. ("Lower courts will have to decide whether the restrictions on access under the CFAA are required to be technological-e.g., a password does not permit access to certain files-or whether non-technological limits can have the same effect.").

[251] *See* Freel, *supra* note 44. "In addition to providing clarity to the scope of the law, the Supreme Court has significantly narrowed the reach of the CFAA to foreclose criminal and civil liability for a 'breathtaking amount of commonplace computer activity,' such as violations of a websites terms of service or using a work computer to access personal email." *Id.*

[252] Will Duffield, *Van Buren Decision Is a Step in the Right Direction*, CATO INST. (June 24, 2021), https://www.cato.org/blog/van-buren-decision-step-right-direction. ("Dispensing with the government's purpose-driven reading in favor of a gate-based approach is a step in the right direction. Now, however, someone must decide which gates count.").

they are not committing computer fraud every time they use their work computer against company policy.