Loyola University Chicago Law Journal

Volume 54
Issue 5 *Online*

Article 4

2023

"So" What? Why the Supreme Court's Narrow Interpretation of the Computer Fraud and Abuse Act in Van Buren v. United States Has Drastic Effects

Landon Wilneff
Loyola University Chicago Law School

Recommended Citation

Landon Wilneff, *"So" What? Why the Supreme Court's Narrow Interpretation of the Computer Fraud and Abuse Act in Van Buren v. United States Has Drastic Effects*, 54 Loy. U. Chi. L. J. 1 (2023).
Available at: https://lawecommons.luc.edu/luclj/vol54/iss5/4

"So" What? Why the Supreme Court's Narrow Interpretation of the Computer Fraud and Abuse Act in *Van Buren v. United States* Has Drastic Effects

Landon Wilneff[*]

In Van Buren v. United States*, the United States Supreme Court held that one does not "exceed authorized access" under the Computer Fraud and Abuse Act (CFAA) when one accesses information they were otherwise entitled to access. Part I will outline the legislative history of the CFAA, and will explain the circuit split between the Second, Fourth, Sixth, and Ninth Circuits and the First, Third, Fifth, and Seventh Circuits. Part II will detail the facts and procedural history of* Van Buren*, and will walk through the reasoning of the majority and dissent. Part III will analyze the majority's narrow reading of the statute that employed a highly strict, granular textual analysis, including the CFAA's use of the word "so." Part III will also analyze the dissent's conclusion that the circumstances of a potential CFAA offense should factor into the assessment of liability. In contrast to the majority's highly technical reading, the dissent offered a plain meaning reading of the statute in congruence with its legislative purpose, the fundamentals of property law, and the importance of punishing bad-faith actors like Van Buren. Part IV will explore the impact of the decision. The dissent's interpretation adequately limits liability under the CFAA through the statute's mens rea requirement, while also protecting sensitive data from businesses, law enforcement, and the government.*

[*] J.D. Candidate, Loyola University Chicago School of Law, Class of 2024. I would like to thank the editorial staff of the *Loyola University Chicago Law Journal* for its support, insight, and guidance.

INTRODUCTION

Congress enacted the Comprehensive Crime Control Act ("CCCA") to "to fight emerging computer crimes" in the burgeoning internet age.[1] The

[1] H. Marshall Jarrett et al., OFF. LEGAL EDUC. EXEC. OFF. FOR U.S. ATT'YS, PROSECUTING COMPUTER CRIMES 1 (2007), https://www.steptoecyberblog.com/files/2012/11/ccmanual1.pdf [https://perma.cc/L823-8R3A]; *see also* Joseph B. Thompkins, Jr. & Linda A. Mar, *The 1984 Federal Computer Crime Statute: A Partial Answer to a Pervasive Problem*, 6 COMPUTER/L.J. 459, 460–61 (1986) (detailing how the Comprehensive Crime Control Act of 1984 led to the Counterfeit

CCCA established 18 U.S.C. § 1030, the first federal statute for "computer-related offenses."[2] In 1986, Congress enacted the Computer Fraud and Abuse Act ("CFAA") that evolved directly from the CCCA and 18 U.S.C § 1030.[3] The CFAA's original purpose was to protect the federal government's interest in cybercrime while also acknowledging states' rights in this area.[4] In short, the CFAA is the most significant piece of federal legislation for computer crime and cybersecurity.[5]

The CFAA lists seven federal offenses related to cybercrime.[6] In *Van Buren v. United States*, the Supreme Court interpreted section 1030(a)(2) of the CFAA, the section that prohibits one from "intentionally access[ing] a computer without authorization or exceed[ing] authorized access" to obtain information.[7] In section (e)(6) of the CFAA, Congress defined the "exceeds authorized access" prong from section (a)(2).[8] The definition of "exceeds authorized access" reads as follows: "access[ing] a computer with authorization and [using] such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."[9] Section (a)(2) and its definitional provision section (e)(6) are

Access Device and Computer Fraud and Abuse Act of 1984, which ultimately led to the Computer Fraud and Abuse Act); *see generally* Comprehensive Crime Control Act of 1984, Pub. L. No. 98-473, § 2102, 98 Stat. 2190 (1984) (codified at 18 U.S.C. § 1030).

[2] Jarrett et al., *supra* note 1; *see generally* 18 U.S.C. § 1030 (2022).

[3] 18 U.S.C. § 1030; *see* Jarrett et al., *supra* note 1, at 1–2 (describing the legislative history of the CFAA).

[4] *See* Jarrett et al., *supra* note 1, at 1 ("In the CFAA, Congress attempted to strike an 'appropriate balance between the Federal Government's interest in computer crime and the interests and abilities of the States to proscribe and punish such offenses.'"); *see also* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1597 (2003) ("In the last quarter century, the federal government, all fifty states, and over forty foreign countries have enacted computer crime laws that prohibit 'unauthorized access' to computers.") (footnotes omitted).

[5] *See* Jason B. Freeman, *The Computer Fraud and Abuse Act (CFAA)*, FREEMAN L., https://freemanlaw.com/computer-fraud-abuse-act-cfaa/ [https://perma.cc/2DH3-ATCW] (last visited Apr. 14, 2023) ("The CFAA is perhaps the most important—certainly the most comprehensive—federal statute governing computer crimes and violations. It is the primary federal statute protecting computers and digital information from unauthorized intrusions."); *see also* Lee Goldman, *Interpreting the Computer Fraud and Abuse Act*, 13 PITT. J. TECH. L. & POL'Y 1, 1 (2012) (explaining the background of the CFAA and its importance).

[6] *See* 18 U.S.C. § 1030(a)(1)–(7) (each section describing a different federal cybercrime offense); *see also* Freeman, *supra* note 5 (summarizing the various crimes of the CFAA).

[7] 18 U.S.C. § 1030(a)(2); *see* Van Buren v. United States, 141 S. Ct. 1648, 1652 (2021) (introducing the legal issue on appeal in the case).

[8] 18 U.S.C. § 1030(a)(2); *see Van Buren*, 141 S. Ct. at 1652 (introducing the statutory language of the CFAA).

[9] 18 U.S.C. § 1030(a)(2).

at issue in *Van Buren v. United States*.[10] Practical implications of what it means to access a computer without authorization or to exceed the scope of authorized access affect every computer-user in America. Employers and employees who are responsible for accessing and distributing sensitive data are especially affected by the CFAA.[11]

The prevalence of computers in modern society is obvious. With the digital revolution and the rise of the internet age, computer use is critical to the success of students and professionals.[12] The work-from-home boom caused by the COVID-19 pandemic further cemented the critical role of computers and the internet in American society.[13] The pandemic advanced "remote work and virtual interactions, e-commerce and digital transactions, and deployment of automation and AI," significantly disrupting the labor market.[14] As a result of this disruption, business leaders are rapidly reducing office space.[15] Furthermore, many employees want to continue to work remotely now that the model has proven successful in a variety of industries.[16]

With employees working remotely, employers have less direct

[10] 18 U.S.C. § 1030(a)(2); *seeVan Buren*, 141 S. Ct. at 1653–54 (contextualizing the statutory language for the purposes of the case).

[11] *See* Brief of the Managed Funds Ass'n as Amicus Curiae in Support of Respondent at 6, Van Buren v. United States, 141 S. Ct. 1648 (2021) (No. 19-783) [herinafter Brief of the Managed Funds Ass'n] (explaining how investment firms are protected by the CFAA); *see also* Brief of the Federal Law Enforcement Officers Ass'n as *Amicus Curiae* in Support of Respondent at 4, Van Buren v. United States, 141 S. Ct. 1648 (2021) (No. 19-873) [hereinafter Brief of the Federal Law Enforcement Officers] (explaining how law enforcement and other governmental agencies are protected by the CFAA).

[12] *See* Romina Bandura & Elena I. Méndez Leal, DIGIT. LITERACY IMPERATIVE (July 2022), https://www.csis.org/analysis/digital-literacy-imperative [https://perma.cc/P73H-T2F4] ("Digital literacy has become indispensable for every global citizen, whether to communicate, find employment, receive comprehensive education, or socialize.").

[13] *See* SUSAN LUND ET AL., MCKINSEY GLOB. INST., THE FUTURE OF WORK AFTER COVID-19 5 (2021), https://www.mckinsey.com/featured-insights/future-of-work/the-future-of-work-after-covid-19#/ [https://perma.cc/FZ69-U2GG] (last visited Apr. 14, 2023) (outlining the impact of the COVID-19 pandemic on working remotely); *see also* Severin Sorensen, *Monitoring the Remote Employee: Oversight or an Overstep*?, ARETE COACH (Jan. 7, 2022), https://www.aretecoach.io/post/monitoring-the-remote-employee-oversight-or-an-overstep [https://perma.cc/B8Y4-ZWW2] (explaining the rise of remote work).

[14] Lund et al., *supra* note 13, at 1; *see generally* Sorensen, *supra* note 13.

[15] *Id.* at 7 ("A survey of 278 executives by McKinsey in August 2020 found an average planned reduction in office space of 30 percent."); *see also* Sorensen, *supra* note 13 (explaining that managers and employers are prepared to monitor their employees remotely).

[16] Lund et al., *supra* note 13, at 37 ("Roughly 20 to 25 percent of the workforce in advanced economies could be as effective working remotely three to five days a week as working from an office. If remote work took hold at that level, four to five times as many people would work from home at least part of the time compared to before the pandemic."); *see* Cedric Nabe, *Impact of COVID-19 on Cybersecurity*, DELOITTE, https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html [https://perma.cc/XB83-Y4DY] (last visited Apr. 14, 2023) (explaining the link between remote work and cybersecurity).

oversight.[17] Therefore, section (a)(2) of the CFAA, and how courts define accessing digital information without authorization, are especially significant today.[18] Similarly, the increase in remote work that requires either a personal or company-issued computer brings the dangers of hacking and the importance of cybersecurity to the forefront of national attention.[19]

Comprehensive governmental efforts by the Department of Homeland Security's Cybersecurity and Infrastructure Agency to promote cybersecurity demonstrate that private businesses need to take cybersecurity measures seriously.[20] The illicit access of computers is no longer just a problem for information technology teams, but one that CEOs of both large and small companies must work to solve.[21] Executives should speak the language of information technology to best protect sensitive data and ensure their organization is properly protecting itself against cyber threats.[22]

Small businesses are at risk from cyberattacks too, and many hackers target smaller businesses because of a perception that small businesses

[17] *See* Sorensen, *supra* note 13 (explaining that employers have concerns about employees working remotely); *see also* Nabe, *supra* note 16 (linking remote work and cybersecurity).

[18] *See* Kerr, *supra* note 4, at 1602–05 (explaining the economic and noneconomic effects of computer misuse); *see also* Goldman, *supra* note 5, at 1 (detailing that computer misuse has significant implications).

[19] *See* Nabe, *supra* note 16 ("The increase in remote working calls for a greater focus on cybersecurity, because of the greater exposure to cyber risk."); *see also* Alejandro Mayorkas, *Secretary Mayorkas Outlines His Vision for Cybersecurity Resilience*, U.S. DEP'T OF HOMELAND SEC. (Mar. 31, 2021), https://www.dhs.gov/news/2021/03/31/secretary-mayorkas-outlines-his-vision-cybersecurity-resilience [https://perma.cc/8Z9M-MRGV] (detailing the importance of cybersecurity protection in America today, including over $4 billion in cybercrime losses in 2020).

[20] *See* Mayorkas, *supra* note 19 ("For too long, cybersecurity has been seen as a technical challenge couched in bureaucratic terms. But cybersecurity is not about protecting an abstract 'cyberspace.' Cybersecurity is about protecting the American people and the services and infrastructure on which we rely."); *see also* INTERNET CRIME REPORT 2021, FED. BUREAU OF INVESTIGATION, https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf [https://perma.cc/Y6NF-DGPV] (last visited Apr. 14, 2023) (demonstrating that cybersecurity measures are extremely important for businesses).

[21] *See* Ty Ward, *The Importance of Cybersecurity for Business Executives*, FORBES (Feb. 22, 2022, 9:45 AM), https://www.forbes.com/sites/forbestechcouncil/2022/02/02/the-importance-of-cybersecurity-for-business-executives/?sh=4f70afa01b52 [https://perma.cc/2YAN-LWE4] ("Business executives and information security leaders must become familiar with one another, speak often and speak a common language. Determine and define your organization's appetite for risk and its resilience to cyberattacks, then encounter threats head-on."); *see also* Mayorkas, *supra* note 19 (outlining the country's plan to solve cybersecurity issues).

[22] *See* Ward, *supra* note 21 ("Therefore, it is the responsibility of executives, board members and information security departments to set the table with measurable objectives and recurring risk thresholds."); *see also* INTERNET CRIME REPORT 2021, *supra* note 20, at 1, 7–9 (illustrating that cybersecurity measures are extremely important for businesses and management).

are particularly vulnerable.[23] Furthermore, small businesses often store sensitive customer data that hackers target.[24] Small businesses may lack the finances and motivation to protect against cyberattacks to the fullest extent.[25] For businesses of all sizes, section (a)(2) of the CFAA is critical for protection from cyberattacks.[26]

Section (a)(2) of the CFAA defines the crime of hacking as "intentionally access[ing] a computer without authorization."[27] The more controversial question at issue in *Van Buren* is how courts define what "exceeds authorized access."[28] This may refer to an employee who is authorized to access only certain parts of a database, who then exceeds their authorized access by entering an off-limits section of the database.[29] A narrow definition of what "exceeds authorized access," or weaker protection under the CFAA, can make businesses more vulnerable to cyber threats.[30] A broad definition poses the risk of overcriminalization.[31] *De minimus* activities need not, and should not,

[23] Yulia Volyntseva, *Why Is Cybersecurity Important for Small Businesses?*, BUSINESSTECHWEEKLY (Mar. 13, 2022), https://www.businesstechweekly.com/cybersecurity/application-security/why-is-cybersecurity-important/ [https://perma.cc/Y627-PVV4] ("As more prominent companies are sometimes harder to penetrate, attackers target small businesses that partner with them to get the more effective systems.").

[24] *See* Volyntseva, *supra* note 23 ("Cybercriminals know that small businesses generally store and handle customer data that is easy to offload for profit."); *see generally* Brief of the Managed Funds Ass'n, *supra* note 11, at 4–5 (explaining that both hackers and insider threats can disrupt the cybersecurity efforts of a business).

[25] *See* Volyntseva, *supra* note 23 ("As start-ups often work on tight budgets, they cannot prioritize cybersecurity. They avoid spending on resources, training, and consultants for information security and ignore the latest updates and patches, leaving their systems vulnerable to attacks."); *see also* Morah, *supra* note 23 (explaining that computer software is an asset that needs protection).

[26] *See* Volyntseva, *supra* note 23 (explaining how startups are especially vulnerable to cyberattacks); *see also* Ward, *supra* note 21 (detailing the importance of cybersecurity for management).

[27] 18 U.S.C. § 1030(a)(2); *see also* Goldman, *supra* note 5, at 4 (explaining the terms in the statute).

[28] *See* Van Buren v. United States, 141 S. Ct. 1648, 1652 ("This provision [section (a)(2) of the CFAA] covers those who obtain information from particular areas in the computer—such as files, folders, or databases—to which their computer access does not extend."); *see also* 18 U.S.C. § 1030(e)(6) (defining "exceeds authorized access").

[29] *See* Goldman, *supra* note 5, at 10 (explaining the plain meaning approach to CFAA interpretation). *Contra Van Buren*, 141 S. Ct. at 1652 (Van Buren did not enter off-limits sections of the database; he exceeded his authorized access in a database that he was otherwise authorized to access);

[30] *See* Nabe, *supra* note 16 ("Malicious employees working from home with less supervision and fewer technical controls may be tempted to carry out a fraud or other criminal activity."); *see generally* INTERNET CRIME REPORT 2021, *supra* note 20.

[31] *See Department of Justice Announces New Policy for Charging Cases under the Computer Fraud and Abuse Act*, DEP'T OF JUST. (May 19, 2022) [hereinafter *DOJ Announcement*],

be punished under the CFAA.[32]

Businesses and their data must be protected, and non-hackers should be prevented from improperly accessing and distributing sensitive information.[33] In *Van Buren*, the Supreme Court could have interpreted section (a)(2) of the CFAA to prevent the criminalization of *de minimus* activities while simultaneously protecting businesses.[34] Instead, the Court offered an extremely narrow interpretation of what "exceeds authorized access" without considering the bad-faith of the perpetrator or the circumstances of the incident.[35]

It is important to note that circuit courts are split regarding what "exceeds authorized access."[36] In Part I, this Note will explain the circuit split and provide the legislative background, including a number of amendments to the CFAA, that led to the Supreme Court's holding in *Van Buren*. Part II will explore the Court's textual reasoning in the case and consider the negative impact of the decision on governmental agencies and businesses alike. The dissent's rationale will then be thoroughly analyzed in Part III, illustrating how the statute's mens rea requirement supports a broader interpretation of the CFAA, allowing the statute to capture bad-faith actors such as Van Buren.

https://www.justice.gov/opa/pr/department-justice-announces-new-policy-charging-cases-under-computer-fraud-and-abuse-act [https://perma.cc/7GQ2-HDB9] ("Embellishing an online dating profile contrary to the terms of service of the dating website; creating fictional accounts on hiring, housing, or rental websites . . . are not themselves sufficient to warrant federal criminal charges [under the CFAA]."); *see also Van Buren*, 141 S. Ct. at 1661 ("And indeed, numerous *amici* explain why the Government's reading of subsection (a)(2) would do just that—criminalize everything from embellishing an online-dating profile to using a pseudonym on Facebook.").

[32] *Cf. DOJ Announcement*, *supra* note 31 (explaining that inconsequential acts such as embellishing an online dating profile or checking the score of a sports game on a company-issued computer should not be prosecuted under the CFAA).

[33] *See DOJ Announcement*, *supra* note 31 (explaining that we must protect sensitive financial data); *see also* Nabe, *supra* note 16 (explaining the need for businesses to have proper cybersecurity measures to protect their data from hackers).

[34] *Cf. Van Buren*, 141 S. Ct. at 1662 (holding that Van Buren's bad-faith conduct was not punishable under the CFAA); *see also* Brief of the Managed Funds Ass'n, *supra* note 11, at 3 (explaining the importance of the CFAA's role in protecting businesses).

[35] *See Van Buren*, 141 S. Ct. at 1661 ("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."); *see also* Maddison Addicks, Van Buren v. United States*: The Supreme Court's Ruling on the Fate of Web Scraping*, 24 TUL. J. TECH. & INTELL. PROP. 161, 171 (2022) (explaining the difference between the majority's approach and the dissent's focus on circumstances).

[36] *See Van Buren*, 141 S. Ct. at 1654 ("We granted certiorari to resolve the split in authority regarding the scope of liability under the CFAA's 'exceeds authorized access' clause."); *see also* Melanie Assad, Van Buren v. United States*: An Employer Defeat or Hackers' Victory—or Something in Between?*, 21 UIC REV. INTELL. PROP. L. 166, 170–71 (2022) (outlining the circuit split).

In an effort to resolve the circuit split between narrow and broad definitions of section (a)(2) of the CFAA, Part IV will argue that the majority should have adopted the broad approach based on the statute as written and to incentivize proper cyber behavior without limiting law enforcement. Further, amending the CFAA to further specify its mens rea requirement is a reasonable approach, but unnecessary because the CFAA already includes an intentional mental state in section (a)(2).

I. BACKGROUND

A. Legislative History of the CFAA

In 1984, Congress enacted the CCCA, the predecessor to the CFAA and 18 U.S.C. § 1030.[37] Congress decided that a federal cybercrime statute was required to respond to cybersecurity challenges brought on by the development and expansion of the internet age.[38] The CCCA was more limited than CFAA, setting forth three new federal crimes that applied only to scenarios protecting governmental interests.[39] Nevertheless, the three new federal crimes created by the CCCA served as the foundation for the CFAA.[40] The CCCA's prohibition of "us[ing] the opportunity such access provides for purposes to which such access does not extend" is the origin of the CFAA's "exceeds authorized access" prong at issue in *Van Buren*.[41]

[37] Comprehensive Crime Control Act, *supra* note 1; 18 U.S.C. § 1030; *see also Van Buren*, 141 S. Ct. at 1652 ("Congress, following the lead of several states, responded by enacting the first federal computer-crime stature as part of the Comprehensive Crime Control Act of 1984.").

[38] Comprehensive Crime Control Act, *supra* note 1; *see Van Buren*, 141 S. Ct. at 1652 ("Technological advances at the dawn of the 1980s brought computers to schools, offices, and homes across the Nation. But as the public and private sectors harnessed the power of computing for improvement and innovation, so-called hackers hatched ways to coopt computers for illegal ends.").

[39] *See* Comprehensive Crime Control Act, *supra* note 1 (setting out three federal violations); *see also CFAA Background*, NAT'L ASS'N CRIM. DEF. LAWS. (July 14, 2022), https://www.nacdl.org/Content/CFAABackground [https://perma.cc/PB2C-KZ3X] ("When enacted, this new statute only set forth three new federal crimes . . . . The crimes also added requirements that collectively limited the statute to three specific scenarios tailored to particular government interests—computer misuse to obtain national security secrets, computer misuse to obtain personal financial records, and hacking into government computers.").

[40] *See* 18 U.S.C. § 1030(a)(1)–(2) (using the three original offenses as a foundation for the CFAA); *see also* Comprehensive Crime Control Act, *supra* note 1 (listing the three original offenses); *CFAA Background*, *supra* note 39 (alteration in original) ("These crimes covered certain conduct by a person who 'knowingly accesses a computer without authorization, or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend[.]'"); Addicks, *supra* note 35, at 163 (detailing the history of amendments to the CFAA).

[41] *See* 18 U.S.C. § 1030; Comprehensive Crime Control Act, *supra* note 1; *see also CFAA Background*, *supra* note 39 (documenting how the CCCA became the CFAA); Assad, *supra* note 36, at 168–70 (explaining the amendments to the CFAA).

The CFAA built upon the CCCA by adding three new offenses.[42] Like the CCCA, the original CFAA was focused on protecting governmental institutions, but expanded the scope to financial institutions as well.[43] Since 1986, computer usage and computer crimes continued to grow, such that the CFAA required further amending.[44] Congress amended the CFAA eight times between 1988 and 2008.[45] These amendments have since broadened the CFAA "far beyond its original intent."[46]

The first significant batch of amendments to the CFAA occurred in 1994.[47] Congress expanded the CFAA to not merely provide criminal penalties, but also added the option of civil penalties to further disincentivize less-serious offenses.[48] Congress included additional prohibited acts, such as data theft to defraud, intentional destruction of data, distribution of malware, and password trafficking.[49] These prohibited acts, among other amendments to the CFAA in 1994, shifted the focus of the statute "from a technical concept of computer access and authorization, to the defendant's malicious intent and resulting harm."[50] In *Van Buren*, the majority and dissent debated how the circumstances of

[42] *See* 18 U.S.C. § 1030; Comprehensive Crime Control Act, *supra* note 1; *see also CFAA Background*, *supra* note 39 ("The CFAA also added three new prohibitions."); Addicks, *supra* note 35, at 163 (explaining the amendments to the CFAA).

[43] *See* 18 U.S.C. § 1030; *see also* Comprehensive Crime Control Act, *supra* note 1; *see also CFAA Background*, *supra* note 39 ("The original CFAA was directed at protecting classified information, financial records, and credit information on governmental and financial institution computers."); Assad, *supra* note 36, at 168–69, 168 n.17 (explaining the amendments to the CFAA).

[44] *See* Jarrett et al., *supra* note 1, at 2 ("As computer crimes continued to grow in sophistication and as prosecutors gained experience with the CFAA, the CFAA required further amending, which Congress did in 1988, 1989, 1990, 1994, 1996, 2001, 2002, and 2008.").

[45] *See id.* at 2–3 (listing all the amendments to the CFAA); *see also* Addicks, *supra* note 35, at 163 (detailing the history of amendments to the CFAA).

[46] *Computer Fraud and Abuse Act*, NAT'L ASS'N CRIM. DEF. LAWS., https://www.nacdl.org/Landing/ComputerFraudandAbuseAct [https://perma.cc/9A55-645T] (last visited Apr. 14, 2023).

[47] *See CFAA Background*, *supra* note 39 (explaining the amendments); *see also* Goldman, *supra* note 5, at 2–3 (discussing the changes to the scope of the CFAA).

[48] *See CFAA Background*, *supra* note 39 ("Until it was amended in 1994, the CFAA only provided criminal penalties for engaging in prohibited conduct. At that point, Congress added a civil cause of action for CFAA violations that afforded private parties the ability to obtain compensatory damages, injunctive relief, and/or other equitable relief."); *see also* Goldman, *supra* note 5, at 3 (explaining when the CFAA provided for civil liability).

[49] *See* 18 U.S.C. § 1030; *CFAA Background*, *supra* note 39 ("The CFAA also added three new prohibitions—section 1030(a)(4) prohibiting unauthorized access with intent to defraud; section 1030(a)(5) prohibiting accessing a computer without authorization and altering, damaging, or destroying information; and section 1030(a)(6) prohibiting trafficking in computer passwords."); *see also* Goldman, *supra* note 5, at 3 (discussing the additional CFAA provisions).

[50] *CFAA Background*, *supra* note 39; *see* Goldman, *supra* note 5, at 3–4 (explaining the 1994 amendments).

a defendant's potential violation of the CFAA factor into liability under the CFAA.[51]

The Economic Espionage Act of 1996 further broadened the scope of the CFAA to protect private companies in addition to the government and financial institutions.[52] Congress enacted the 1996 amendments to protect companies' digital information from both employee and outsider threats.[53] In turn, the 1996 amendments widened the scope of the CFAA, this time with the specific intent to protect and cover private businesses under the "exceeds authorized access" prong.[54]

Most significantly, the 2008 amendments gave rise to the present day CFAA seen in *Van Buren*.[55] Under section 1030(a)(2)(C) of the CFAA, an individual cannot intentionally access a protected computer without authorization or exceed authorized access to retrieve information.[56] Furthermore, the current version of the CFAA "defines 'exceeds authorized access' in Section 1030(e)(6) as accessing 'a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter.'"[57] These two provisions are central to the decision in *Van Buren*.

The CFAA's phrase "intentionally accesses a computer without authorization or exceeds authorized access" and the definitions of its various elements have long been a source of debate and controversy.[58]

[51] *See* Van Buren v. United States, 141 S. Ct. 1648, 1663–64 (2021) (Thomas, J., dissenting) (claiming that circumstances matter in determining whether a defendant "exceeds authorized access" under the CFAA).

[52] *See* 18 U.S.C § 1831; *see also* Justin Precht, *The Computer Fraud and Abuse Act or the Modern Criminal at Work: The Dangers of Facebook from Your Cubicle*, 82 U. CIN. L. REV. 359, 360–61 (2013) ("The CFAA remained limited until Congress passed the Economic Espionage Act of 1996 (EEA)"); *id.* at 361 (explaining that the 1996 amendments to the CFAA increased the scope of coverage beyond the government to private enterprise).

[53] *See* Precht, *supra* note 52, at 361 ("Thus, by 1996 the CFAA protected a company's proprietary information and could be used in actions by private employers against their employees."); *see also* Goldman, *supra* note 5, at 16 & n.95 (noting the legislative history covers "hackers").

[54] *See* 18 U.S.C § 1030; *see also* Precht, *supra* note 52, at 361 ("In short, the 1986 amendment was responsible for broadening the language of the statute to cover instances where a person 'exceeds authorized access,' and the 1996 amendment substantially broadened the scope beyond mere misuse of government owned computers."); Goldman, *supra* note 5, at 17 ("[T]he Economic Espionage Act of 1996 evidences Congress' desire to maintain the traditional requirements of trade secret protection.").

[55] 18 U.S.C § 1030; *see also* Peter J.G. Toren, *Computer Fraud and Abuse Act*, 34 GPSOLO 70 (2017).

[56] 18 U.S.C § 1030(a)(2); *see* Precht, *supra* note 52, at 361 ("The current CFAA, as amended in 2008, makes it a crime under Section 1030(a)(2)(C) when an individual 'intentionally accesses a computer without authorization or exceeds authorized access' to obtain 'information from any protected computer.'").

[57] 18 U.S.C § 1030(e)(6).

[58] 18 U.S.C § 1030(a)(2); *see also* Kerr, *supra* note 4, at 1616, 1619–24 (discussing the ambiguities of "access" and "authorization" in the CFAA).

"Access" could mean typing in a password and username, navigating to a public website without providing credentials, or simply commanding a computer to perform a task.[59] Courts have interpreted "access" in each of these ways, illustrating a lack of clarity.[60] Courts have interpreted the concept of "authorization" with even more variance than "access."[61] The main reason for this variance is that the source of authorization could arise from the context of a specific situation, social norms, or contractual language, and the CFAA provides no clarification.[62] In short, courts have not uniformly interpreted the terms "access" and "authorization" under the CFAA.[63]

B. The Second, Fourth, Sixth, and Ninth Circuits Interpreted the CFAA Narrowly

With this background in mind, it is unsurprising that prior to *Van Buren*, circuit courts split on how "exceeds authorized access" should be interpreted.[64] The Second, Fourth, Sixth, and Ninth Circuits adopted a

[59] *See* Kerr, *supra* note 4, at 1619–21 (providing examples to show how "access" has been and can be interpreted); *see also* Goldman, *supra* note 5, at 9 n.53 (describing the "plain meaning" approach in interpreting the Act).

[60] *See, e.g.*, United States v. Valle, 807 F.3d 508, 528 (2d Cir. 2015); United States v. Nosal, 676 F.3d 854, 864 (9th Cir. 2012); EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 583–84 (1st Cir. 2001), *abrogated by* Van Buren v. United States, 141 S. Ct. 1648 (2021); United States v. John, 597 F.3d 263, 272 (5th Cir. 2010); *see also* Kerr, *supra* note 4, at 1621 ("Most computer crime statutes (including the federal statute) do not define access, and most statutes that do include a definition shed little light on these questions. In the handful of cases that have interpreted the meaning of access, however, courts have at one point or another suggested every one of these possible interpretations of access.").

[61] *See, e.g.*, *Valle*, 807 F.3d at 528; *Nosal*, 676 F.3d at 864; *Explorica*, 274 F.3d at 583–84; *John*, 597 F.3d at 272; *see also* Goldman, *supra* note 5, at 24 (discussing the challenges with "authorization."); *see also* Kerr, *supra* note 4, at 1628 ("Courts have faced even greater difficulties trying to interpret the meaning of authorization.");

[62] *See* Kerr, *supra* note 4, at 1623–24 ("More broadly, who and what determines whether access is authorized, and under what circumstances? Can a computer owner set the scope of authorization by contractual language? Or do these standards derive from the social norms of Internet users? The statutes are silent on these questions: The phrase 'without authorization' generally is left undefined.").

[63] *See, e.g.*, *Valle*, 807 F.3d at 528; *Nosal*, 676 F.3d at 864; *Explorica*, 274 F.3d at 583–84; *John*, 597 F.3d at 272; LVRC Holdings, LLC v. Brekka, 581 F.3d 1127, 1137 (9th Cir. 2009); *see also* Kerr, *supra* note 4, at 1619–23 (explaining the differing interpretations of "access" and "authorization"); Van Buren v. United States, 141 S. Ct. 1648, 1654 (2021) (granting certiorari to resolve the circuit split); *see also* Goldman, *supra* note 5, at 5 ("Courts have not agreed on the proper interpretation of 'without authorization' and 'exceeds authorized access.' Rather, they have adopted three different approaches to interpreting these terms.").

[64] *See Van Buren*, 141 S. Ct. at 1661 (illustrating the challenges with the statute); *see also* Assad, *supra* note 36, at 170–71 (noting the circuit courts disagreement about liability under the "exceed authorized access" clause).

narrow view of the "exceeds authorized access" clause.[65] These circuits adopted a defendant-friendly interpretation that limited prosecution under the CFAA.[66]

Beginning with Second Circuit precedent, *United States v. Valle* illustrates a narrow view of "exceeds authorized access," setting the stage for policy arguments adopted by the majority in *Van Buren*.[67] In *Valle*, defendant police officer Gilberto Valle accessed the federal National Crime Information Center database to retrieve sensitive information regarding Maureen Hartigan, a woman who he conspired to kidnap.[68] Valle allegedly improperly accessed a governmental computer to obtain information, a CFAA violation under section 1030(a)(2)(B). The Second Circuit reversed Valle's conviction under the CFAA on appeal, holding that the rule of lenity prevented a conviction.[69]

Even though Valle violated department policy, the court held that Valle did not "exceed authorized access" by using his police credentials to search Maureen Hartigan.[70] Valle obtained the information for an improper purpose, but the court held that he was otherwise authorized to access the information.[71] To argue that Valle did in fact "exceed authorized access," the prosecution pointed to the original language of the CFAA from 1984, which criminalized the act of using a computer for reasons exceeding the scope of the accessor's authorization.[72] The Government argued that this legislative history supported that Valle's improper purpose was relevant to his liability under the CFAA.[73] While

[65] *See, e.g.*, *Valle*, 807 F.3d at 523; WEC Carolina Energy Sols. LLC v. Miller, 687 F.3d 199, 206 (4th Cir. 2012); Royal Truck & Trailer Sales and Servs., Inc. v. Kraft, 974 F.3d 756, 760–61 (6th Cir. 2020); *Nosal*, 676 F.3d at 858; *Brekka*, 581 F.3d at 1133–35; *see also* Addicks, *supra* note 35, at 166 (discussing the Second, Fourth, Sixth, and Ninth Circuit's narrow interpretation); *see generally Van Buren*, 141 S. Ct. at 1648.

[66] *See, e.g.*, *Valle*, 807 F.3d at 523; *Miller*, 687 F.3d at 206; *Royal Truck*, 974 F.3d at 760–61; *Nosal*, 676 F.3d 864; *Brekka*, 581 F.3d 1133–35; *see also* Addicks, *supra* note 35, at 166 (equating a narrow view to a defendant-friendly interpretation; Assad, *supra* note 36, at 170–73 (outlining the circuit split and the limited prosecution under a narrow interpretation).

[67] *See Valle*, 807 F.3d at 528; *see also* 141 S. Ct. at 1661 ("To top it all off, the Government's interpretation of the statute would attach criminal penalties to a breathtaking amount of commonplace computer activity.").

[68] *Valle*, 807 F.3d at 512–13.

[69] *Id.* at 528.

[70] *Id.* at 523–28 (adopting the rule of lenity given that the statute could criminalize a broad range of ordinary behavior).

[71] *Id.* at 523–24.

[72] *See id.* at 525 ("As originally enacted, section 1030(a) made it a crime to "knowingly access[ ] a computer without authorization, *or having accessed a computer with authorization, use[ ] the opportunity such access provides for purposes to which such authorization does not extend.*") (alterations in original) (citing Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98–473, § 2102(a), 98 Stat. 1837 (codified as amended at 18 U.S.C. § 1030)).

[73] *See id.* at 525 ("The Government argues that no substantive change was intended because the substitution was made 'to simplify the language.'") (citing S. Rep. No. 99-432, at 2486 (1986)).

the court gave credence to the prosecution's view, it overturned Valle's conviction because the true meaning of "exceeds authorized access" is unclear.[74] In turn, the court applied the rule of lenity to the statute, a key argument made by Valle.[75] The court construed the phrase "exceeds authorized access" narrowly to prevent Valle's conviction and the overcriminalization of similar actors under the CFAA.[76]

In the Fourth Circuit, the court in *WEC Carolina Energy Solutions LLC v. Miller* also evaluated congressional intent to free a defendant from prosecution under the CFAA.[77] In *Miller*, former WEC employee Mike Miller allegedly downloaded and used WEC's proprietary information for a presentation on behalf of a competitor.[78] The district court granted Miller's motion to dismiss WEC's CFAA claim because WEC authorized Miller to access the computer.[79] The appellate court considered two main arguments that support a broad and a narrow interpretation of section 1030(a)(2) of the CFAA, respectively. The first, the prosecution's view, "holds that when an employee accesses a computer or information on a computer to further interests that are adverse to his employer, he violates his duty of loyalty, thereby terminating his agency relationship and losing any authority he has to access the computer or any information on it."[80] The second, the defendant's view, "interprets 'without authorization' and 'exceeds authorized access' literally and narrowly, limiting the terms' application to situations where an individual accesses a computer or information on a computer without permission."[81] The court sided with

[74] *See id.* at 526 ("Where, as here, ordinary tools of legislative construction fail to establish that the Government's position is unambiguously correct, we are required by the rule of lenity to adopt the interpretation that favors the defendant.").

[75] *See id.* ("At the end of the day, we find support in the legislative history for both Valle's and the Government's construction of the statute. But because our review involves a criminal statute, some support is not enough. Where, as here, ordinary tools of legislative construction fail to establish that the Government's position is unambiguously correct, we are required by the rule of lenity to adopt the interpretation that favors the defendant.").

[76] *See id.* at 528 ("Whatever the apparent merits of imposing criminal liability may seem to be *in this case,* we must construe the statute knowing that our interpretation of 'exceeds authorized access' will govern many other situations.") (quoting 18 U.S.C. §1030(e)(6)).

[77] WEC Carolina Energy Sols., LLC v. Miller, 687 F.3d 199, 207 (4th Cir. 2012).

[78] *Id.* at 201–02.

[79] *See* WEC Carolina Energy Sols., LLC v. Miller, No. 0:10-cv-2775-CMC, 2011 WL 379458, at *4 (D. S.C. Feb. 3, 2011) ("At the point Miller and Kelley were allegedly accessing the confidential information, they were performing an action authorized by WEC. In short, accessing the confidential information did not involve accessing a computer 'without authorization' under the CFAA. Therefore, Defendants were not acting 'without authorization' when they accessed the confidential information."); *see also Miller*, 687 F.3d 199 at 201, 207 ("The district court dismissed WEC's CFAA claim, holding that the CFAA provides no relief for Appellees' alleged conduct.").

[80] *Miller*, 687 F.3d at 203.

[81] *Id.*

the latter.[82]

The *Miller* court based its narrow interpretation of "exceeds authorized access" on congressional intent.[83] Ultimately, the Fourth Circuit maintained that siding with the prosecution's agency theory would criminalize commonplace activity, such as checking Facebook at work.[84] Moreover, the court concluded that the intent of the CFAA was to target hackers and not employees who violate company policy.[85] Even though Miller greatly harmed his employer if the alleged facts were true, he did not face criminal charges under the CFAA.[86]

Moving to the Sixth Circuit, in *Royal Truck & Trailer Sales & Service, Inc. v. Kraft*, the court held that when a defendant's conduct violates company policy or another federal law, if the defendant is authorized to access the information at issue, a claim under section 1030(a)(2) fails.[87] Defendants Mike Kraft and Kelly Matthews, former employees of Royal Truck, sent confidential and proprietary sales information to their personal email accounts for the purpose of benefiting a competitor.[88] Royal Truck sued Kraft and Matthews for violating the CFAA.[89] To prove Royal Truck's claim, the Sixth Circuit set out a four-part test, focusing on element two: the "exceeds authorized access" element.[90] Like in *Valle*, the *Royal* court opined that because the defendants sent proprietary information to their personal accounts while they were still employed by Royal Truck, they did not "exceed authorized access."[91] A violation of company policy does not automatically extend

[82] *Id.*

[83] *See id.* at 206 ("In so doing, we adopt a narrow reading of the terms 'without authorization' and 'exceeds authorized access' and hold that they apply only when an individual accesses a computer without permission or obtains or alters information on a computer beyond that which he is authorized to access."); *see also infra* note 85.

[84] *See Miller*, 687 F.3d at 206 ("[A] rule would mean that any employee who checked the latest Facebook posting or sporting event scores in contravention of his employer's use policy . . . would be left without any authorization to access his employer's computer systems.").

[85] *See id.* at 207 ("But we are unwilling to contravene Congress's intent by transforming a statute meant to target hackers into a vehicle for imputing liability to workers who access computers or information in bad faith, or who disregard a use policy.").

[86] *Id.*

[87] *See* Royal Truck & Trailer Sales & Servs., Inc. v. Kraft, 974 F.3d 756, 757 (6th Cir. 2020) ("The conduct at issue might violate company policy, state law, perhaps even another federal law. But because Royal concedes that the employees were authorized to access the information in question, it has failed to satisfy the statutory requirements for stating a claim under the CFAA.").

[88] *Id.* at 757–58.

[89] *Id.* at 758.

[90] *Id.* at 759 ("Royal must plead that: (1) Defendants intentionally accessed a computer; (2) the access was unauthorized or exceeded Defendants' authorized access; (3) through that access, Defendants thereby obtained information from a protected computer; and (4) the conduct caused loss to one or more persons during any one-year period aggregating at least $5,000 in value.").

[91] *Id.* at 760; *see also* United States v. Valle, 141 S. Ct. 1648, 523–24 (2021) (explaining that Valle had permission to obtain the database information he then misused).

to a violation of the CFAA because this was not Congress's intention.[92] The *Royal Truck* opinion suggests that if Kraft and Matthews undertook the same act while they were not employed by Royal Truck, their conduct would have violated the CFAA.[93]

The Ninth Circuit is the final circuit that interprets section 1030(a)(2) of the CFAA narrowly.[94] In *United States v. Nosal*, defendant David Nosal left his position at Korn/Ferry, an executive search firm, and encouraged employees of Korn/Ferry to help him start a competing business.[95] The employees logged into a confidential company database with their credentials, downloaded names and contact information, and sent this information to Nosal.[96] The Korn/Ferry employees were authorized to access the database, but the employer forbade disclosing confidential information per company policy.[97] Nosal, who was no longer an employee at Korn/Ferry, violated his former employer's use restrictions when he solicited this proprietary information.[98] Yet, the Ninth Circuit held that Nosal did not violate the CFAA because the employees who actually retrieved and distributed the sensitive information were otherwise authorized to access it.[99]

Even though the claim in *Nosal* is a section 1030(a)(4) claim and not a section 1030(a)(2) claim, the definition of "exceeds authorized access" is applied similarly.[100] As seen in other decisions, the Ninth Circuit acquitted Nosal, following the rule of lenity and an evaluation of the original purpose of the CFAA.[101] The court concluded that the original purpose of the CFAA was to "punish hacking—the circumvention of technological access barriers—not misappropriation of trade secrets—a subject Congress has dealt with elsewhere."[102] The prosecution brought twenty other counts against Nosal, including trade secret theft and conspiracy, to maximize their chance of punishing Nosal's improper

[92] *See Royal Truck*, 974 F.3d at 762 ("In addition to being less faithful to § 1030's text, this latter interpretation has the odd effect of allowing employers, rather than Congress, to define the scope of criminal liability by operation of their employee computer-use policies.").

[93] *Id.*

[94] United States v. Nosal, 676 F.3d 854, 863–64 (9th Cir. 2012).

[95] *Id.* at 856.

[96] *Id.*

[97] *Id.*

[98] *Id.*

[99] *Nosal*, 676 F.3d at 864.

[100] *See id.* (applying "exceeds authorized access" consistently as it appears in multiple sections of the statute).

[101] *Id.* at 863.

[102] *Id.* at 863.

conduct under the law.[103] The CFAA claim, however, failed.[104]

Another Ninth Circuit case, *LVRC Holdings, LLC v. Brekka*, illustrates many of the same principles that govern how the Second, Fourth, and Sixth Circuits all construe "exceeds authorized access" narrowly to limit prosecution under the CFAA.[105] Brekka, a former employee of LVRC Holdings, emailed documents to himself while employed and continued to access proprietary information on LVRC's "LOAD" website after he left the company.[106] The district court granted summary judgment for Brekka, and the Ninth Circuit affirmed on the grounds that Brekka had authorization to email himself the documents while employed, and LVRC did not produce sufficient evidence to prove that Brekka logged in after his employment.[107]

The prosecution argued that because Brekka breached his duty of loyalty to LVRC, he acted "without authorization," but the Ninth Circuit disagreed because of the rule of lenity.[108] Courts have interpreted "authorization" and "exceeds authorized access" in section 1030(a)(2) differently, so the CFAA can be reasonably construed as ambiguous.[109] Furthermore, the court did not consider the circumstances of Brekka's improper conduct, holding that Brekka had permission to access LVRC's computer.[110] Therefore, Brekka did not act "without authorization" and

[103] *See id.* at 856 ("The government indicted Nosal on twenty counts, including trade secret theft, mail fraud, conspiracy and violations of the CFAA.").

[104] *See id.* at 864 ("Accordingly, we affirm the judgment of the district court dismissing counts [under the CFAA] for failure to state an offense. The government may, of course, prosecute Nosal on the remaining counts of the indictment.").

[105] *See generally* LVRC Holdings, LLC v. Brekka, 581 F.3d 1127, 1137 (9th Cir. 2009).

[106] *See id.* at 1129 ("As part of its marketing efforts, LVRC retained LOAD, Inc. to provide email, website, and related services for the facility. Among other duties, LOAD monitored internet traffic to LVRC's website and compiled statistics about that traffic."); *id.* at 1130 ("LVRC then brought an action in federal court, alleging that Brekka violated the CFAA when he emailed LVRC documents to himself in September 2003 and when he continued to access the LOAD website after he left LVRC.").

[107] *See* LRVC Holdings, LLC v. Brekka, No. 2:05-CV-01026-KJD-GWF, 2007 WL 2891565 (Nev. Dist. Ct. Sept. 28, 2007); *see also Brekka*, 581 F.3d 1127 at 1130, 1132 (first alteration in original) ("First, the district court stated that '[i]t is undisputed that when Brekka was employed by Plaintiff that he had authority and authorization to access the documents and emails that were found on his home computer and laptop.' . . . Second, the district court held that LVRC had not put forth evidence from which a reasonable jury could find that Brekka logged into the LVRC website after leaving LVRC's employ.").

[108] *See Brekka*, 581 F.3d 1127 at 1134 (explaining that when a criminal statute is ambiguous, courts should err on the side of lenity when prosecuting a defendant under the statute).

[109] *See* 18 U.S.C 1030(a)(2); 18 U.S.C 1030(e)(6); *see also* Kerr, *supra* note 4, at 1619–21 (discussing how courts interpret "authorization" and "exceeds authorized access" differently); *supra* notes 69, 74, 75, 101 (all finding no CFFA violation on the part of the defendant pursuant to the rule of lenity).

[110] *See Brekka*, 581 F.3d 1127 at 1135 ("Rather, we hold that a person uses a computer "without authorization" under § 1030(a)(2) and (4) when the person has not received permission

he did not "exceed authorized access" because he was entitled to obtain the information.[111] This holding hinged on Brekka's employment status.[112] If Brekka undertook the same act while unemployed, he would have violated the CFAA.[113] This rationale mirrors the Sixth Circuit's unstated implication in *Royal Truck*.[114]

C. The First, Fifth, Seventh, and Eleventh Circuits Interpreted the CFAA Broadly

While the Second, Fourth, Sixth, and Ninth Circuits interpret the CFAA and its "exceeds authorized access" prong in section 1030(a)(2) narrowly, the First, Fifth, Seventh, and Eleventh Circuits interpret it more broadly.[115] Beginning with *EF Cultural Travel BV v. Explorica, Inc*., the First Circuit held that an employee who leverages confidential information unavailable to the public to profit a competitor exceeds authorized access in violation of the CFAA.[116] Explorica developed a "web scraper" computer program to collect pricing information from competitor EF Cultural Travel's (EF) website.[117] EF filed suit against Explorica under section 1030(a)(2) of the CFAA, alleging that Explorica's web scraper exceeded Explorica's authorized access "by providing proprietary information and know-how to [Explorica] to create the scraper."[118]

The First Circuit affirmed Explorica's conviction under the CFAA, holding that it exceeded their authorized use of EF's website by scraping

to use the computer for any purpose . . . or when the employer has rescinded permission to access the computer and the defendant uses the computer anyway.").

[111] *Id.*

[112] *See id.* at 1136–37 (holding that Brekka's employment status helped establish his authorization).

[113] *See id.* at 1136 ("There is no dispute that if Brekka accessed LVRC's information on the LOAD website after he left the company in September 2003, Brekka would have accessed a protected computer 'without authorization' for purposes of the CFAA.").

[114] *See* Royal Truck & Trailer Sales & Servs., Inc. v. Kraft, 974 F.3d 756, 759–61 (6th Cir. 2020) (noting that employees Matthews and Kraft had authorized access to company information and did not exceed that authorized access relying on plain understanding of the CFAA).

[115] *See* Assad, *supra* note 36, at 170–71 (explaining the circuit split); Van Buren v. United States, 141 S. Ct. 1648, 1653–54 (explaining the circuit split).

[116] *See generally* EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 583–84 (1st Cir. 2001), *abrogated by* Van Buren v. United States, 141 S. Ct. 1648 (2021).

[117] *See id.* at 580 ("Zefer ran the scraper program twice, first to retrieve the 2000 tour prices and then the 2001 prices. All told, the scraper downloaded 60,000 lines of data, the equivalent of eight telephone directories of information.").

[118] *Id.* at 583.

their travel codes in an effort to undermine their business.[119] This holding shows that a violation of a website's terms of use can be relevant to a CFAA violation given the circumstances of the violation.[120] The court also determined that Explorica's conduct warranted punishment under the CFAA given Congress's intent to punish "sophisticated intruders" in enacting the CFAA.[121] The First Circuit did not allow a bad-faith actor like Explorica to escape punishment under the CFAA because the court determined that web scraping in bad-faith is analogous to hacking.[122]

Moving to the Fifth Circuit, the court held that purpose and circumstance matter in assessing liability under the CFAA in *United States v. John*.[123] In *John*, former Citigroup employee Dimetriace Eva-Lavon John accessed Citigroup's internal computer and provided her half brother with customer account information to allow him to commit fraud.[124] The Fifth Circuit upheld John's conviction under section 1030(a)(2) of the CFAA because "an employer may 'authorize' employees to utilize computers for any lawful purpose but not for unlawful purposes and only in furtherance of the employer's business."[125] In this case, John exceeded her authorized access because she was not authorized to access Citigroup's data for unlawful purposes.[126] The court distinguished the facts here from *Brekka* because John knew that she was exceeding her authorized access in committing fraud.[127] In *Brekka*, the defendant did not have the same intent as John because Brekka did not know he was violating his employer's policies and participating in illegal activity.[128] In short, the Fifth Circuit determined that the mental state of

[119] *See id.* ("Practically speaking, however, if proven, Explorica's wholesale use of EF's travel codes to facilitate gathering EF's prices from its website reeks of use—and, indeed, abuse—of proprietary information that goes beyond any authorized use of EF's website.").

[120] *See id.* (demonstrating that circumstances matter in authorized access cases).

[121] *Id.* at 585.

[122] *See id.* ("If we were to restrict the statute as appellants urge, we would flout Congress's intent by effectively permitting the CFAA to languish in the twentieth century, as violators of the Act move into the twenty-first century and beyond.").

[123] *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 access has been given are exceeded.").

[124] *Id.* at 269.

[125] *Id.* at 271.

[126] *Id.*

[127] *See id.* at 273 ("An authorized computer user "has reason to know" that he or she is not authorized to access data or information in furtherance of a criminally fraudulent scheme."); *see generally* LRVC Holdings, LLC v. Brekka, 581 F.3d 1127 (9th Cir. 2009).

[128] *See John*, 597 F.3d at 273 ("[W]hen an employee knows that the purpose for which she is accessing information in a computer is both in violation of an employer's policies and is part of an illegal scheme, it would be 'proper' to conclude that such conduct "exceeds authorized access" within the meaning of § 1030(a)(2)."); *see also Brekka*, 581 F.3d at 1132 (failing to satisfy the first element—that Brekka intentionally accessed a computer).

the defendant and their criminal intent should be considered when evaluating the "exceeds authorized access" prong of the CFAA.[129]

Similarly, the Seventh Circuit concluded that an employee's bad-faith intent to harm their employer is relevant to authorization.[130] In *International Airport Centers, LLC v. Citrin*, International Airport Centers' employee Jacob Citrin quit his job and deleted all the data in his employee laptop before returning it to shield improper conduct that he engaged in while on the job.[131] Citrin acted with clear bad-faith, "load[ing] into the laptop a secure-erasure program, designed, by writing over the deleted files, to prevent their recovery."[132] The Seventh Circuit distinguished the facts in *Citrin* from those in *Explorica*. In *Explorica*, the defendant used confidential information to develop a program that stole information from his former employee's website.[133] Even though the website was open to the public, the defendant "exceeded his authorization by using confidential information to obtain better access than other members of the public."[134] In *Citrin*, the employee's breach of loyalty terminated his agency relationship with his employer, thereby terminating the employee's authorization to access the data in his company laptop.[135] Therefore, Citrin exceeded his authorized access under the CFAA.[136]

Another Seventh Circuit case, *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*[137] mirrors the holding in *Citrin*. In *Shurgard*, Safeguard lured away several of Shurgard's employees,

[129] *See John*, 597 F.3d at 271 (concluding the use of information obtained by permitted access to a computer system "may, at least when the user knows or reasonably should know that he or she is not authorized to access a computer and information obtainable from that access in furtherance of or to perpetrate a crime").

[130] *See* Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 420–21 (7th Cir. 2006) (showing the agency relationship was voided by violating the duty of loyalty in bad faith).

[131] *See id.* at 419 (describing Citrin's actions before quitting IAC).

[132] *Id.*

[133] *See id.* at 420 ("[T]he former employee of a travel agent, in violation of his confidentiality agreement with his former employer, used confidential information that he had obtained as an employee to create a program that enabled his new travel company to obtain information from his former employer's website . . . .").

[134] *See id.* at 420–21 ("Citrin's breach of his duty of loyalty terminated his agency relationship . . . and with it his authority to access the laptop, because the only basis of his authority had been that relationship.").

[135] *See id.* at 420–21 ("[Citrin] terminated any rights he might have claimed as IAC's agent–he could not by unilaterally terminating any duties he owed by his principal gain an advantage!").

[136] *See id.* at 420 ("For his authorization to access the laptop terminated when, having already engaged in misconduct and decided to quit IAC in violation of his employment contract . . . .").

[137] *See* Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1122–23 (W.D. Wash. 2000) (alleging former employees appropriated trade secrets stored on employer's computers).

including Eric Leland, who accessed Shurgard's proprietary information via computer while still employed.[138] The court held that Shurgard's employees lost their authorization when they sent proprietary information to Safeguard because they became agents for Safeguard.[139] Under the Restatement (Second) of Agency, the employees terminated their initial agency/principal relationship when they began to act as agents for a competitor.[140]

The Seventh Circuit also considered congressional intent.[141] To support its holding, the court referenced the legislative history of the CFAA, which demonstrates a broad congressional aim to criminalize the improper use of computer information.[142] Furthermore, the Seventh Circuit considered the "motive" of the defendant in affirming a prima facie claim of a violation under the CFAA.[143] Intent matters. If an employee uses a computer to harm their employer's interest, the employee has accessed the computer without authorization, severing the agency/principal relationship.[144] In sum, the Seventh Circuit concluded that Congress intended courts to interpret the CFAA broadly to punish bad-faith conduct, further justifying its conclusion based on the principles of agency law in the Restatement (Second) of Agency.[145]

Concluding with the Eleventh Circuit, in *United States v. Rodriguez*,

[138] *See Shurgard Storage Ctrs., Inc.*, 119 F. Supp. 2d at 1123 (choosing Mr. Leland because of his full access to the plaintiff's confidential business plans and trade secrets); *see also* Kerr, *supra* note 4 at 1632–33 (summarizing the facts).

[139] *See Shurgard Storage Ctrs., Inc.*, 119 F. Supp. 2d at 1123 ("While still employed by the plaintiff, but acting as an agent for the defendant, Mr. Leland sent e-mails to the defendant containing various trade secrets and proprietary information belonging to the plaintiff. Mr. Leland did this without the plaintiff's knowledge or approval.").

[140] Restatement (Second) of Agency § 112 (Am. L. Inst. 1958); *see Shurgard Storage Ctrs., Inc.*, 119 F. Supp. 2d at 1125 ("Under the Restatement (Second) of Agency . . . [u]nless otherwise agreed, the authority of an agent terminates if, without knowledge of the principal, he acquires adverse interests or if he is otherwise guilty of a serious breach of loyalty to the principal.").

[141] *See* Kerr, *supra* note 4, at 1633 (explaining how the court considered congressional intent in the case); *see generally Shurgard Storage Ctrs., Inc.*, 119 F. Supp. 2d 1121.

[142] *See* Kerr, *supra* note 4, at 1633 ("In support of its holding, the court turned to the CFAA's legislative history, which the court argued showed a congressional design broadly to prohibit computer misuse, especially where intellectual property rights were at issue."); *see generally Shurgard Storage Ctrs., Inc.*, 119 F. Supp. 2d 1121.

[143] *See* Kerr, *supra* note 4, at 1633–34 (explaining that access is unauthorized when the employee's motive for using the employer's computer is not work-related); *see generally Shurgard Storage Ctrs., Inc.*, 119 F. Supp. 2d 1121.

[144] *See* Kerr, *supra* note 4, at 1633–34 ("Under Shurgard, whenever an employee uses a computer for reasons contrary to an employer's interest, the employee does not act as the employer's agent and therefore is accessing the employer's computers without authorization."); *see generally Shurgard Storage Ctrs., Inc.*, 119 F. Supp. 2d 1121.

[145] *See Shurgard Storage Ctrs., Inc.* 119 F. Supp. 2d at 1125, 1129 ("This legislative history, although in reference § 1030(a)(2), demonstrates the broad meaning and intended scope of the terms 'protected computer' and 'without authorization' that are also used in the other relevant sections.").

the Eleventh Circuit held that accessing clients' personal information for nonbusiness purposes is unauthorized when it contradicts company policy.[146] Roberto Rodriguez worked as a TeleService representative for the Social Security Administration (SSA).[147] He had access to a database with sensitive personal information, including social security numbers and addresses.[148] The SSA had a policy that prohibited employees from obtaining information from the databases without a business reason, which Rodriguez violated when he accessed the personal records of seventeen individuals for nonbusiness purposes.[149] The clear policy of the SSA, the bad-faith intent of Rodriguez, and the number of violations all played a role in his conviction under the CFAA.[150]

The Eleventh Circuit distinguished the facts of Rodriguez's case from *Brekka* and *John*. In *Brekka*, the employer did not have a policy that prohibited employees from forwarding company documents to their personal email accounts, and Brekka had been authorized to obtain the company documents and to send the emails while working for the company.[151] Rodriguez, on the other hand, violated a clear policy of the SSA by accessing sensitive information for nonbusiness purposes—a policy that his employer emphasized.[152] In *John*, the Fifth Circuit held that the defendant was authorized to view the information she accessed, but use of this information for a criminal purpose was prohibited under the CFAA.[153] Here, Rodriguez's use is irrelevant if he did not have

[146] *See* United States v. Rodriguez, 628 F.3d 1258, 1260 (11th Cir. 2010), *abrogated by* Van Buren v. United States, 141 S. Ct. 1648 (2021) (finding the nonbusiness was related to accessing the personal records of 17 different individuals).

[147] *Id.*

[148] *See id.* ("Rodriguez had access to Administration databases that contained sensitive information, including any person's social security number, address, date of birth, father's name, mother's maiden name, amount and type of social security benefit received and annual income.").

[149] *See id.* The Administration required its employees annually to sign forms about its policy but from 2006 to 2008 Rodriguez refused to sign the forms. *Id.*

[150] *See id.* at 1263 (finding each occurance supports that Rodrigiez exceeded his authorization access).

[151] *See id.* ("The treatment center had no policy prohibiting employees from emailing company documents to personal email accounts, and there was no dispute that Brekka had been authorized to obtain the documents or to send the emails while he was employed."); *see generally* LRVC Holdings, LLC v. Brekka, 581 F.3d 1127 (9th Cir. 2009); United States v. John, 597 F.3d 263 (5th Cir. 2010).

[152] *See Rodriguez*, 628 F.3d at 1260 ("The Administration also required TeleService employees annually to sign acknowledgment forms after receiving the policies in writing. The Administration warned employees that they faced criminal penalties if they violated policies on unauthorized use of databases.").

[153] *See generally John*, 597 F.3d 263.

authorization or if he exceeded authorized access.[154] The Eleventh Circuit held that Rodriguez exceeded his authorized access by obtaining information for a "nonbusiness" reason.[155]

The cases discussed from the First, Fifth, Seventh, and Eleventh Circuits all share a common theme: purpose and circumstance matter when assessing violations under section 1030(a)(2) of the CFAA.[156] This argument is adopted by the dissent in *Van Buren*.[157] Purpose and circumstance include the defendant's mens rea, or criminal intent, factors that may contribute to the defendant's general bad-faith, and company policy.[158] These circuits also agree that Congress intended the CFAA to have a scope beyond mere hackers to punish a wider range of improper conduct.[159] Agency principles can also inform when access is authorized or terminated.[160]

On the other hand, the cases discussed from the Second, Fourth, Sixth, and Ninth Circuits show significant concerns that an overly-broad

[154] *See Rodriguez*, 628 F.3d at 1263 (rejecting Rodriguez's argument that his use of information is irrelevant because he obtained the information without authorization and as a result of exceeding authorized access).

[155] *Id.*

[156] *See supra* text accompanying notes 114–155155.

[157] *See* Van Buren v. United States, 141 S. Ct. 1648, 1663 (2021) (Thomas, J., dissenting) ("The majority postulates an alternative reading of this definitional provision: So long as a person is entitled to use a computer to obtain information in at least *one* circumstance, this statute does not apply even if the person obtains the data outside that circumstance.").

[158] *See, e.g.*, EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 581–82 (1st Cir. 2001), *abrogated by* Van Buren v. United States, 141 S. Ct. 1648 (2021) (holding wherein a violation of company terms was relevant to CFAA violation); *John*, 597 F.3d at 271 (establishing mental state of defendant and criminal intent should be considered when potential CFAA violations); Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 419–20 (7th Cir. 2006) (finding bad-faith intent to harm an employer is relevant to CFAA violation); *Rodriguez*, 628 F.3d at 1263 (concluding that accessing personal information of clients for nonbusiness purposes is unauthorized when it contradicts company policy).

[159] *See Explorica*, 274 F.3d at 585 ("[T]his legislative history makes 'clear that Congress intended the term "loss" to target remedial expenses borne by victims that could not properly be considered direct damage caused by a computer hacker.'") (quoting *In re* DoubleClick Inc. Priv. Litig., 154 F. Supp. 2d 497, 521 (S.D.N.Y. 2001)); *Citrin*, 440 F.3d at 420 ("Congress was concerned with both types of attack: attacks by virus and worm writers."); Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1126 (W.D. Wash. 2000) (rejecting defendant's claim that CFAA is only intended to apply to "outsiders" because the staute is unambiguous with the language "whoever" used in the statute); *Rodriguez*, 628 F.3d at 1263 (incorporating a broad congressional intent to punish hackers into the holdings).

[160] *See, e.g.*, *Explorica, Inc.*, 274 F.3d at 581–83 (finding appellants' actions exceeded authorized access based on evidence of a broad confidentiality agreement and employment-based communications); *John*, 597 F.3d at 271 (discussing the scope of "authorization" under the statute for an employee); *Citrin*, 440 F.3d at 420–21 (citing Arizona agency law where "[v]iolating the duty of loyalty, or failing to disclose adverse interests, voids the agency relationship."); *Shurgard Storage Ctrs., Inc.*, 119 F. Supp. 2d at 1125 ("Under this rule, the authority of the plaintiff's former employees ended when they allegedly became agents of the defendant.") (citing Restatement (Second) of Agency § 112 (1958)); *Rodriguez*, 628 F.3d at 1263 (relating the applicability of agency law to the potential liability of the various defendants).

reading of the CFAA would lead to the criminalization of commonplace acts that technically exceed company policy or the scope of authorized access.[161] Further, these circuits did not think that company policy was relevant to assessing CFAA violations because prosecution under a federal statute should not be influenced by or related to an employer's own policy.[162] These circuits also concluded that Congress only intended for the CFAA to punish hackers, and even if statutory language is ambiguous, the rule of lenity should protect defendants.[163] In deciding *Van Buren*, the United States Supreme Court solved the circuit split in favor of the Second, Fourth, Sixth, and Ninth Circuits.[164]

II. DISCUSSION

A. Van Buren v. United States*: Facts and Procedural History*

The United States Supreme Court granted certiorari over *Van Buren v. United States* to resolve the circuit split that plagued courts for decades, overruling the Eleventh Circuit.[165] The Supreme Court's landmark holding both interpreted the statute and addressed policy implications.[166]

[161] *See supra* text accompanying notes 64–113 (describing relevant case law).

[162] *See, e.g.*, United States v. Valle, 807 F.3d 508, 523–27 (2nd Cir. 2015) (using legislative history to determine Valle's violation of department policy did not "exceed authorized access"); WEC Carolina Energy Sols. LLC v. Miller, 687 F.3d 199, 205 (4th Cir. 2012) ("[I]nterpreting 'so' as 'in that manner' fails to mandate CFAA liability for the improper *use* of information that is accessed with authorization"); Royal Truck & Trailer Sales & Servs., Inc. v. Kraft, 974 F.3d 756, 762 (6th Cir. 2019) (violating company policy is not an automatic violation of the CFAA in view of the congressional intentions); United States v. Nosal, 676 F.3d 854, 857 (9th Cir. 2012) (demonstrating additional examples to support the congressional intent argument why employee policy violation is not dispositive alone); LRVC Holdings, LLC v. Brekka, 581 F.3d 1127, 1135 (9th Cir. 2009) ("The definition of the term 'exceeds authorized access' from 1030(e)(6) implies that an employee can violate employer-placed limits on accessing information stored on the computer and still have authorization to access that computer.").

[163] *See Valle*, 807 F.3d at 525–26 (using the Senate Committee Report to the 1986 to the 1986 amendments to align the CFAA with hackers); *Miller*, 687 F.3d at 201 ("Today, the CFAA remains primarily a criminal statute designed to combat hacking."); *Royal Truck*, 974 F.3d at 760 (providing a dictionary definition of congressional intent); *Nosal*, 676 F.3d at 857 ("If Congress meant to expand the scope of criminal liability to everyone who uses a computer in violation of computer use restrictions . . . we would expect it to use language better suited to that purpose."); *Brekka*, 581 F.3d at 1130 (explaining the CFAA was enacted to enhance the government's ability to prosecute computer crimes and target hackers and criminals).

[164] *See* Van Buren v. United States, 141 S. Ct. 1648, 1652 (2021) (explaining the holding of the case and how it resolved the circuit split).

[165] *See id.* at 1654; *see also* Addicks, *supra* note 35, at 164–68 (evaluating the significance of the *Van Buren* decision in relation to resolving the circuit split).

[166] *See Van Buren*, 141 S. Ct. at 1652 (explaining the major issues that the majority addressed in its holding); *see also* Addicks, *supra* note 35, at 162 ("The Court's ruling not only defined the language of the statute, but addressed numerous policy concerns, ultimately invalidating a limitation on how individuals use their computers and phones for everyday use.").

Nathan Van Buren served as a police sergeant for the Cumming, Georgia Police Department.[167] While working as a sergeant, Van Buren met a man named Andrew Albo, who had a volatile relationship with the department.[168] Nevertheless, Van Buren became friends with Albo and ultimately accepted a bribe from him to perform improper conduct.[169] More specifically, Albo asked Van Buren to search the state law enforcement computer database for a license plate belonging to a woman, identified only as Carson, whom Albo met at a strip club in exchange for $5,000.[170] During the exchange, Albo acted as an agent on behalf of the FBI, who set up this sting operation to see how far Van Buren would go for money.[171]

Van Buren used his patrol-car computer to access the state law enforcement database with his valid, active police credentials.[172] He then searched for and obtained the FBI-created license plate entry that Albo had requested.[173] Van Buren contacted Albo to let him know he completed the search, and the federal government brought felony charges against Van Buren for violating the "exceeds authorized access" clause of section 1030(a)(2) of the CFAA.[174]

At trial in the District Court for the Northern District of Georgia, the evidence proved that Van Buren's department trained him to not use the state law enforcement computer data base for an improper purpose.[175] The court determined that, because Van Buren was aware of the department's policy, he acted in bad-faith and with specific intent to violate the CFAA .[176] Further, the district court held that Van Buren's access of the database violated the CFAA because he used the database for a non-law enforcement purpose in violation of department policy.[177] The district court sentenced Van Buren to eighteen months in federal

[167] United States v. Van Buren, 940 F.3d 1192, 1197 (11th Cir. 2019); *see generally Van Buren*, 141 S. Ct. at 1652–53.

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

[169] *Id.*

[170] *Van Buren*, 940 F.3d at 1197; *Van Buren*, 141 S. Ct. at 1653.

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

[172] *Id.*

[173] *Id.*

[174] *Id.*

[175] *See Van Buren*, 141 S. Ct. at 1653 (explaining the trial court's evidentiary conclusions).

[176] *See Van Buren*, 141 S. Ct. at 1653 ("The trial evidence showed that Van Buren had been trained not to use the law enforcement database for 'an improper purpose,' defined as 'any personal use.'").

[177] *See Van Buren*, 141 S. Ct. at 1653 (alteration in original) ("Consistent with that position, the Government told the jury that Van Buren's access of the database 'for a non[-]law[-]enforcement purpose' violated the CFAA 'concept' against 'using' a computer network in a way contrary to 'what your job policy prohibits.'").

prison.[178]

Van Buren appealed to the Eleventh Circuit, arguing that because he was otherwise authorized to access the state law enforcement database, he did not "exceed his authorized access" as defined in the CFAA.[179] On appeal, Van Buren unsuccessfully argued that the lesser offense of misdemeanor computer fraud should have been considered by the jury and that the Government did not provide sufficient evidence to support his conviction.[180] The court reasoned that if Van Buren committed computer fraud for financial gain, he must be charged with a felony offense, and his acceptance of Albo's bribe of $5,000 clearly shows financial gain.[181] Additionally, the court concluded that the database should only be used for proper law-enforcement purposes, and officers are trained on the difference between proper and improper uses.[182] Van Buren admitted that he was aware that he did not access the database for a proper purpose, and that he had done so because of a bribe.[183] The Eleventh Circuit considered police department policy and Van Buren's bad-faith intent.[184]

In affirming that the Government's evidence sufficiently supported Van Buren's conviction for computer fraud, the Eleventh Circuit acted consistently with its precedent.[185] The Eleventh Circuit heavily relied on *Rodriguez*, holding that "there is no question that the record contained

[178] *See Van Buren*, 141 S. Ct. at 1653 ("The jury convicted Van Buren, and the District Court sentenced him to 18 months in prison.").

[179] *See id.* ("Van Buren appealed to the Eleventh Circuit, arguing that the 'exceeds authorized access' clause applies only to those who obtain information to which their computer access does not extend, not to those who misuse access that they otherwise have.").

[180] *See* United States v. Van Buren, 940 F.3d 1192, 1205 (11th Cir. 2019) ("Van Buren contends that two problems specific to his computer-fraud charge undermine his conviction. He argues, first, that the district court should have instructed the jury on the lesser-included offense of misdemeanor computer fraud, and, second, that the government did not present enough evidence to sustain his conviction.").

[181] *See id.* at 1206–07 ("[V]an Buren had already received $5,000 from Albo and agreed in principle to investigate Carson. And second, even setting aside those facts, which independently establish financial gain, the record reflects that Albo did not provide Van Buren with Carson's purported plate number for the first time until *after* . . . .").

[182] *See id.* at 1208 ("[T]hat the database is supposed to be used for law-enforcement purposes only and that officers are trained on the proper and improper uses of the system.").

[183] *See id.* ("Van Buren also admitted . . . that he knew it was 'wrong' to run the tag search and that he had done so for money.").

[184] *Van Buren*, 940 F.3d at 1208. The district court considered these issues as well. *Id.*

[185] *See* Van Buren v. United States, 141 S. Ct. 1648, 1653–54 (2021) ("While several Circuits see the clause Van Buren's way, the Eleventh Circuit is among those that have taken a broader view. Consistent with its Circuit precedent, the panel held that Van Buren had violated the CFAA by accessing the law enforcement database for an 'inappropriate reason.').

enough evidence for a jury to convict Van Buren of computer fraud."[186] The Eleventh Circuit applied the rule from *Rodriguez*, "that [a] defendant had 'exceeded his authorized access and violated the [computer-fraud statute] when he obtained [the victims'] personal information *for a nonbusiness reason*.'"[187] Further, the Eleventh Circuit acknowledged that decisions such as *Nosal* and *Valle* interpret "exceeds authorized access" differently, but the court adhered to *Rodriguez*, Eleventh Circuit precedent, to convict Van Buren.[188] Van Buren appealed to the Supreme Court, and the Court "granted certiorari to resolve the split in authority regarding the scope of liability under the CFAA's 'exceeds authorized access' clause."[189]

Justice Amy Coney Barrett drafted the majority opinion for the Supreme Court.[190] The Court held in favor of Van Buren, concluding that section 1030(a)(2) of the CFAA "covers those who obtain information from particular areas in the computer—such as files, folders, or databases—to which their computer access does not extend."[191] In turn, contrary to Eleventh Circuit precedent, section 1030(a)(2) of the CFAA "does not cover those who, like Van Buren, have improper motives for obtaining information that is otherwise available to them."[192] The Supreme Court noted that a violation of section 1030(a)(2) has penalties ranging from low-level fines and misdemeanor sentences to up to ten years in prison, depending on the offense.[193] The CFAA also provides for a private cause of action allowing those who were harmed by a CFAA violation to sue for damages and relief.[194]

B. Majority's Textual Analysis of the CFAA

The majority began their analysis with the text of the CFAA, specifically section 1030(a)(2), the "exceeds authorized access" clause, and section 1030(e)(6), which defines "exceeds authorized access."[195]

[186] *Van Buren*, 940 F.3d at 1208.

[187] *Id.* at 1207 (alterations in original); *see also* United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010), *abrogated by* Van Buren v. United States, 141 S. Ct. 1648 (2021).

[188] *See Van Buren*, 940 F.3d at 1208 (explaining that the Eleventh Circuit will adhere to the *Rodriguez* holding because neither the Supreme Court nor the Eleventh Circuit *en banc* has overruled it, even though other courts have rejected the *Rodriguez* holding).

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

[190] *Id.* at 1651.

[191] *Id.* at 1652.

[192] *Id.*

[193] *Id.*

[194] *Id.*

[195] 18 U.S.C. § 1030(a)(2); 18 U.S.C. § 1030(e)(6); *see also Van Buren*, 141 S. Ct. at 1654 ("But we start here where we always do: with the text of the statute.").

The latter featured prominently in the majority's analysis.[196] As defined in section 1030(e)(6), to exceed authorized access in the context of the CFAA "means to access a computer with authorization and to use such access to obtain . . . information in the computer that the accesser is not entitled so to obtain ."[197] The majority found that both parties agreed Van Buren accessed his police computer with authorization because he did so while employed as a police officer.[198] In other words, Van Buren was "entitled" to obtain the license plate information since he had the right to access his police computer as an active police officer.[199] The majority also found that Van Buren improperly obtained license-plate information by improperly using that computer.[200] Next, the majority turned to the statutory interpretation of the word "so" in section 1030(e)(6).[201]

The majority placed a great deal of emphasis on the word "so" within section 1030(e)(6), concluding that the main issue on appeal was whether Van Buren was "entitled so to obtain" the information.[202] This analysis became highly technical. According to *Black's Law Dictionary* and the *Oxford English Dictionary*,"so" means "the same manner as has been stated" or "the way or manner described."[203] Therefore, "the disputed phrase 'entitled so to obtain' . . . asks whether one has the right, in 'the same manner as has been stated,' to obtain the relevant information."[204] The Court agreed with Van Buren's interpretation of this disputed phrase, ruling that "is not entitled *so* to obtain" references "information one is not

[196] *See Van Buren*, 141 S. Ct. at 1654 (explaining how the CFAA's definition of "exceeds authorized access" was crucial to the majority's holding).

[197] 18 U.S.C. § 1030(e)(6); *see Van Buren*, 141 S. Ct. at 1654 (providing the majority's rationale regarding § 1030(e)(6)).

[198] *See Van Buren*, 141 S. Ct. at 1654 ("The parties agree that Van Buren 'access[ed] a computer with authorization' when he used his patrol-car computer and valid credentials to log into the law enforcement database.").

[199] *See id.* ("The parties agree that Van Buren had been given the right to acquire license-plate information—that is, he was 'entitled to obtain' it—from the law enforcement computer database.").

[200] *See id.* ("[The parties] also agree that Van Buren 'obtain[ed] . . . information in the computer' when he acquired the license-plate record for Albo.").

[201] *See* 18 U.S.C. § 1030(e)(6); *Van Buren*, 141 S. Ct. at 1654 ("The term 'exceeds authorized access' means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled *so* to obtain or alter.").

[202] 18 U.S.C. § 1030(e)(6); *see also Van Buren*, 141 S. Ct. at 1654 (indicating the majority's emphasis on the wording of the statute).

[203] *So*, BLACK'S LAW DICTIONARY (5th ed. 1979); *So*, OXFORD ENGLISH DICTIONARY (2d ed. 1989).

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

allowed to obtain *by using a computer that he is authorized to access*."[205] The Supreme Court provided an illustrative example: if a person is entitled to access Folder A, they do not violate the CFAA by accessing Folder A, regardless of purpose or bad-faith intent.[206] This individual would need to access Folder B, a folder that their employer prohibited them from accessing, to violate the CFAA.[207] The majority held that "so" captures all circumstances, so the specific circumstances of improper conduct do not matter for a CFAA violation.[208]

Since "so" references "a stated, identifiable proposition from the 'preceding' text," Van Buren was entitled to obtain the license-plate information from his police computer.[209] In her opinion for the majority, Justice Barrett explains that "'[s]o' is not a free-floating term that provides a hook for any limitation stated anywhere."[210] Section 1030(a)(2) prohibits one from obtaining information that they are not entitled to obtain.[211] Van Buren was entitled to obtain the license-plate information because he was authorized to access his police computer.[212] "So" is crucially important to the CFAA, because it limits the statute to hacking or accessing a computer without authorization.[213] Without the word "so," an individual could escape liability under the CFAA if they had another method of retrieving the information, such as picking up physical documents.[214] In short, the word "so" limits the CFAA to prosecuting those who access information via computer.[215]

The majority criticized the dissent by reversing the emphasis on the word "so," rather than "entitled."[216] To support this assertion, the

[205] *Id.*

[206] *See id.* (recounting the example used in the case).

[207] *See id.* (explaining the relationship between the Court's interpretation of "so" and its holding).

[208] *See id.* at 1655 ("Instead, 'so' captures *any* circumstance-based limit appearing *anywhere*—in the United States Code, a state statute, a private agreement, or anywhere else.").

[209] *Id.*

[210] *Id.*

[211] 18 U.S.C. § 1030(a)(2) (explaining the language of the statute); *see also Van Buren*, 141 S. Ct. at 1655 (interpreting the statutory language).

[212] *Van Buren*, 141 S. Ct. at 1655.

[213] *See id.*

[214] *See id.* at 1656 ("Such a person could argue that he was "entitled to obtain" the information if he had the right to access personnel files through another method (*e.g.,* by requesting hard copies of the files from human resources). With 'so,' the CFAA forecloses that theory of defense.").

[215] *See id.* ("This clarification is significant because it underscores that one kind of entitlement to information counts: the right to access the information by using a computer . . . . Without the word 'so,' the statute could be read to incorporate all kinds of limitations on one's entitlement to information. The dissent's take on the statute illustrates why.").

[216] *See id.* ("The dissent's approach to the word "entitled" fares fine in the abstract but poorly in context."); *see also id.* at 1657 ("In fact, the dissent's examples implicitly concede as much: They omit the word 'so,' thereby giving 'entitled' its full sweep.").

majority noted that when a statute includes an explicit definition of a term, the court must follow the explicit definition even if it differs from ordinary meaning.[217] The term 'exceeds authorized access' is defined as "access[ing] a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."[218] According to this definition, based on the majority's interpretation of the word "so," Van Buren did not exceed his authorized access.[219]

Further, the majority concluded that "without authorization" and "exceeds authorized access," in section 1030(a)(2), must be read together in harmony using a "gates-up-or-down inquiry."[220] With this metaphor, the majority maintained that an individual may violate section 1030(a)(2) in one of two ways.[221] First, one who "accesses a computer without authorization," an "outside hacker," violates section 1030(a)(2).[222] Second, one who accesses a computer "with authorization" and then obtains information that they are "not entitled so to obtain," an "inside hacker," violates section 1030(a)(2).[223] The "gates-up-or-down" metaphor serves to distinguish these two different ways one can violate the statute.[224] Additionally, the majority determined that both must be read consistently such that "purpose restrictions" cannot apply to either

[217] *See Van Buren*, 141 S. Ct. at 1657 ("When 'a statute includes an explicit definition' of a term, 'we must follow that definition, even if it varies from a term's ordinary meaning.'") (quoting Tanzin v. Tanvir, 141 S. Ct. 486, 490 (2020)).

[218] 18 U.S.C. § 1030(e)(6).

[219] *See Van Buren*, 141 S. Ct. at 1657 ("So the relevant question is not whether Van Buren exceeded his authorized access but whether he exceeded his authorized access *as the CFAA defines that phrase*. And as we have already explained, the statutory definition favors Van Buren's reading.").

[220] *Id.* at 1658.

[221] *Id.* at 1658–59 ("Under Van Buren's reading, liability under both clauses stems from 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.").

[222] *Id.* at 1658 ("*First*, an individual violates the provision when he 'accesses a computer without authorization.'") (quoting 18 U.S.C. § 1030(a)(2)); *see also id.* ("The 'without authorization' clause, Van Buren contends, protects computers themselves by targeting so-called outside hackers . . .").

[223] *Id.* ("*Second*, an individual violates the provision when he 'exceeds authorized access' by accessing a computer 'with authorization' and then obtaining information he is 'not entitled so to obtain.'") (first quoting 18 U.S.C. § 1030(a)(2); and then quoting 18 U.S.C. § 1030(e)(6)); *see also id*. ("It does so, Van Buren asserts, by targeting so-called inside hackers . . . .").

[224] *Id*. (explaining that the first way is '"access[ing] a computer without any permission at all,'" while the second way is "access[ing] a computer with permission, but then 'exceed[ing] the parameters of authorized access by entering an area of the computer to which [that] authorization does not extend.'") (first quoting LRVC Holdings LLC v. Brekka, 581 F.3d 1127, 1133; and then quoting United States v. Valle, 807 F.3d 508, 524)).

clause of subsection (a)(2).[225] First, as applied here, Van Buren did not access a computer without authorization, so he was not an outside hacker.[226] Second, Van Buren accessed a computer with authorization, but he did not obtain information that he was "not entitled so to obtain."[227] Therefore, according to the majority, Van Buren did not violate the CFAA.[228]

C. Majority's Consideration of Precedent, Statutory History, and Policy

Next, the majority turned to precedent and statutory history.[229] The original version of the CFAA in 1984 defined the "exceeds authorized access " clause as follows: a person who, "having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend."[230] This definition suggests that Congress intended to take circumstances into account under the CFAA. However, this language has since been removed.[231] Therefore, Congress likely intended for courts to omit the consideration of purpose and circumstances by removing the language that encouraged courts to do so.[232]

To conclude its opinion, the majority discussed policy considerations. Mainly, the majority held that a broad interpretation of the "exceeds authorized access" clause of the CFAA "would attach criminal penalties to a breathtaking amount of commonplace computer activity."[233] Despite ample circuit court precedent upon which it could rely, the majority did not invoke the rule of lenity.[234] Instead, the majority relied on the "text, context, and structure" of Van Buren's argument without the need to resort to the rule of lenity as a fallback.[235] The majority pointed to a

[225] *Id.* at 1659.

[226] *Id.* at 1662 ("The parties agree that Van Buren accessed the law enforcement database system with authorization.").

[227] *See id.* ("Van Buren accordingly did not 'excee[d] authorized access' to the database, as the CFAA defines that phrase, even though he obtained information from the database for an improper purpose."); *see also* 18 U.S.C. § 1030(e)(6) (providing the underlying statute against which these facts are analyzed).

[228] *See Van Buren*, 141 S. Ct. at 1662 ("We therefore reverse the contrary judgment of the Eleventh Circuit and remand the case for further proceedings consistent with this opinion.").

[229] *See id.* at 1660.

[230] *Id.* (citing 18 U.S.C. § 1030(a)(2)).

[231] *See* Precht, *supra* note 52, at 361 (explaining the amendments); *see generally* Kerr, *supra* note 58 (overviewing the amendments).

[232] *See Van Buren*, 141 S. Ct at 1661 ("Congress' choice to *remove* the [CFAA's] reference to purpose thus cuts *against* reading [purpose into the statute].").

[233] *Id.*

[234] *See id.* ("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 . . . .").

[235] *Id.*

number of examples to show how a broad interpretation of the "exceeds authorized access" clause would make "millions of otherwise law-abiding citizens . . . criminals."[236] First, a broad reading of the CFAA would criminalize the act of sending a personal email or checking a news website on a work computer.[237] Second, a broad reading of the CFAA would criminalize any violation of a website's terms of use, including "embellishing an online-dating profile . . . [or] using a pseudonym on Facebook."[238]

Just before concluding its opinion, the majority commented on the intent requirement in section 1030(a)(2).[239] The majority disagreed with the Government's assertion that the statute's intent requirement could lessen the overcriminalization of commonplace activity under the CFAA.[240] This is because those who exceed their authorized access in *de minimus* fashion do so intentionally.[241] For example, an individual who sends a personal email or checks a news website on their work computer does so intentionally.[242] The majority does not consider the bad-faith mental state of the potential defendant in these examples.

Finally, the majority held that an evaluation of purpose or circumstances of the potential CFAA offense "would inject arbitrariness into the assessment of criminal liability" because this only criminalizes access restrictions rather than use restrictions.[243] More specifically, a broad interpretation of the CFAA blurs the line between "accessing" and "us[ing]" under the CFAA.[244] A narrow interpretation of the CFAA prevents arbitrary enforcement because it nullifies the distinction between access and use restrictions.[245] This distinction is not relevant to Van Buren's case because he "us[ed] *a confidential database* for a non-

[236] *Id.*

[237] *See id.* ("So on the Government's reading of the statute, an employee who sends a personal e-mail or reads the news using her work computer has violated the CFAA.").

[238] *See Van Buren*, 141 S. Ct at 1661 (citing Brief of Orin S. Kerr as Amicus Curiae in Support of Petitioner at 10–11).

[239] *See id.* at 1662 (commenting on the intent requirement); *see also* 18 U.S.C. § 1030(a)(2) (stating the intent requirement).

[240] *Id.*

[241] *See id.* ("And while the Government insists that the intent requirement serves as yet another safety valve, that requirement would do nothing for those who intentionally use their computers in a way their 'job or policy prohibits'—for example, by checking sports scores or paying bills at work.").

[242] *Id.*

[243] *Id.*

[244] *See id.* ("On the Government's reading, however, the conduct would violate the CFAA only if the employer phrased the policy as an access restriction.").

[245] *See id.* (explaining the difference between an access and a use restriction).

law-enforcement purpose (an access restriction) . . . and us[ed] *information from the database* for a non-law-enforcement purpose (a use restriction)."[246] Nevertheless, the majority held that this distinction would muddy liability in other scenarios, and it is therefore implausible to consider circumstances or purpose in assessing CFAA liability.[247] The Supreme Court held in favor of Van Buren, reversed the Eleventh Circuit's decision, and remanded the case.[248]

D. Dissent's Textual Analysis of the CFAA

Justice Clarence Thomas dissented, joined by Chief Justice John Roberts and Justice Samuel Alito.[249] The dissent simplified the majority's statutory argument, and explained that an interpretation of the CFAA's "exceeds authorized access" clause is an interpretation of ordinary, plain English.[250] The dissent noted that the majority relied solely on section 1030(e)(6), the provision of the CFAA that defines "exceeds authorized access," to determine Van Buren's liability under the CFAA.[251] Even though the dissent agreed that section 1030(e)(6) is essential to the definition of "exceeds authorized access," it also considered established principles of property law and CFAA's statutory history to interpret the phrase.[252] Further, the dissent concluded that the definition of "exceeds authorized access" in section 1030(e)(6) was congruent with the phrase's ordinary meaning.[253]

First, the dissent pulled out the language "entitled so to obtain" from section 1030(e)(6), and agreed with the majority that Van Buren's liability under the CFAA is dependent on this phrase.[254] In contrast with the majority, the dissent held that Van Buren was not entitled to obtain

[246] *Id.* ("Conduct like Van Buren's can be characterized either way, and employer might not see much difference between the two.").

[247] *See id.* ("An interpretation that stakes so much on a fine distinction controlled by the drafting practices of private parties is hard to sell as the most plausible.").

[248] *See Van Buren*, 141 S. Ct. at 1662 ("We therefore reverse the contrary judgment of the Eleventh Circuit and remand the case for further proceedings consistent with this opinion.").

[249] *Id.* (Thomas, J., dissenting).

[250] *See id.* at 1663 ("The question here is straightforward: Would an ordinary reader of the English language understand Van Buren to have 'exceed[ed] authorized access' to the database when he used it under circumstances that were expressly forbidden?").

[251] *See id.* ("[The majority] notes, instead, that the statute includes a definition for that phrase and that 'we must follow that definition, even if it varies from a term's ordinary meaning.'") (quoting Tanzin v. Tanvir, 141 S.Ct. 486, 490 (2020)).

[252] *See id.* ("The problem for the majority view, however, is that the text, ordinary principles of property law, and statutory history establish that the definitional provision is quite consistent with the term it defines.").

[253] *See id.* (explaining that the CFAA should be read in accordance with its plain language).

[254] *See id.* (citing 18 U.S.C. § 1030(e)(6)).

the license-plate information for Albo by using his police credentials.[255] In plain English, Van Buren was not entitled to access the information because he did not have a "right" to do so.[256] Clearly, Van Buren took a bribe from Albo for personal gain, not for a lawful departmental purpose.[257] Therefore, "without a valid law enforcement purpose, [Van Buren] was *forbidden* to use the computer to obtain that information."[258]

Next, the dissent opined that circumstance must be read into "entitled so to obtain," because the plain definition of "entitled" necessarily involves an assessment of the circumstances of the offense.[259] Criticizing the majority's reading, the dissent maintained that the majority neglected the word "entitled" in favor of exclusively analyzing the word "so."[260] In the dissent's view, "entitled" requires a proper purpose or a right to act in a certain manner.[261] Van Buren did not act as entitled by procuring license-plate information for an improper purpose, and thus he exceeded his authorized access under the CFAA.[262]

To develop this point, the dissent provided a number of examples to illustrate why its definition of entitled makes sense.[263] First, "[a]n employee who is entitled to pull the alarm in the event of a fire is not entitled to pull it for some other purpose, such as to delay a meeting . . . ."[264] A valet is entitled to park a customer's car, but is not entitled to take it for a ride.[265] Similarly, a car rental employee is entitled to access the GPS history of an automobile if it is reported stolen, but is not entitled to access the GPS history for the purpose of stalking.[266] In

[255] *Id.* ("In other words, Van Buren's conduct was legal only if he was entitled to obtain that specific license-plate information by using his admittedly authorized access to the database.").

[256] *Id.* (citing *Allow*, BLACK'S LAW DICTIONARY (5th ed. 1979)).

[257] *See Van Buren*, 141 S. Ct. at 1663 (Thomas, J., dissenting) ("Everyone agrees that [Van Buren] obtained [the license-plate information] for personal gain, not for a valid law enforcement purpose.").

[258] *Id.*

[259] *Id.* (citing 18 U.S.C. § 1030(e)(6)).

[260] *See id.* at 1664 ("Focusing on the word 'so,' the majority largely avoids analyzing the term 'entitled,' concluding at the outset in a single sentence that Van Buren *was* entitled to obtain this license-plate information.").

[261] *See id.* ("Because Van Buren lacked a law-enforcement purpose, the 'proper grounds' did not exist.").

[262] *See id.* (explaining the main conclusion of the dissent).

[263] *See id.* (introducing the examples that the dissent provided).

[264] *Id.*

[265] *See id.* ("A valet who obtains a car from a restaurant patron is—to borrow the language from § 1030(e)(6)—'entitled' to 'access [the car]' and 'entitled' to 'use such access' to park and retrieve it. But he is not 'entitled' to 'use such access' to joyride.").

[266] *See id.* ("[A]n employee of a car rental company may be 'entitled' to 'access a computer'. . . and 'use such access' to locate the car if it is reported stolen. But it would be unnatural to say he is 'entitled' to 'use such access' to stalk his ex-girlfriend.").

these examples, the defendant is not entitled to obtain the information or take action "*at all.*"[267] To be "entitled so to obtain" information, a condition precedent must trigger entitlement. In these situtations, no condition precedent triggered entitlement; each actor exceeded their authorized access.[268] Likewise, in Van Buren's case, no condition precedent triggered entitlement because he did not have a valid law enforcement purpose to access the license plate information.[269] The dissent concluded that the majority should have addressed these issues.[270]

E. Dissent's Consideration of Precedent, Statutory History, and Policy

While the majority did not consider the fundamental rules of property law important in reaching its decision, the dissent pointed to property law as a central factor in convicting Van Buren under the CFAA.[271] The dissent declared that the CFAA protects property because information stored on a computer is intellectual property.[272] Notably, trespass, theft, and bailment are all fundamental property law concepts that take circumstances into account in assessing liability.[273] As for trespass, a land owner providing permission for one to enter land is circumstance-specific.[274] For example, A can give permission to B to draw water from A's land for B's own use, but if B draws water and gives it to C, then B trespassed.[275] For theft, a police officer might have authority to access a bank account to cover business expenses, but the officer commits embezzlement if they take money for themself.[276] In this example, the officer had circumstantial control over the funds, but exceeded their authorized access when the funds were embezzled.[277]

[267] *Id.*

[268] *See id.* (noting that the dissent references a few "real-world scenarios" to illustrate its point about what exceeds a proper purpose).

[269] *See Van Buren*, 141 S. Ct. at 1664 (Thomas, J., dissenting) ("Van Buren was not entitled to obtain this information at all because the condition precedent needed to trigger an entitlement—a law enforcement purpose—was absent.").

[270] *See id.* ("The majority offers no real response.").

[271] *See id.* (explaining the importance of property law in the dissent's rationale).

[272] *See id.* ("Nobody doubts, for example, that a movie stored on a computer is intellectual property. Federal and state law routinely define 'property' to include computer data.").

[273] *See id.* at 1664–65 (explaining the dissent's use of fundamental property law concepts).

[274] *See id.* at 1664 ("When a person is authorized to enter land and entitled to use that entry for one purpose but does so for another, he trespasses.").

[275] *See id.* at 1665 (walking through an example of exceeding authorized access for trespass) (citing Restatement (Second) of Torts, § 168 (2022)).

[276] *See id.* ("To again borrow the language from § 1030(e)(6), a police officer may have authority to 'access' the department's bank account and 'use such access' to cover law enforcement expenses, but he is nonetheless guilty of embezzlement if he 'uses such access' to line his pockets.").

[277] *See id.* ("A person who is authorized to possess property for a limited purpose commits theft the moment he 'exercises unlawful control over' it, which occurs 'whenever consent or authority is exceeded.'") (quoting ALI, Model Penal Code § 223.2(1) 162, 168 (1980)).

Finally, a bailee commits conversion when the bailee uses information in a way that is beyond their authority, including using information in a different way than authorized.[278] For instance, if a defendant leaks photos from a private computer when the defendant was only authorized to recover data from a crashed hard drive, the defendant committed conversion.[279] Based on these examples, the dissent held that "'exceed' and 'authority' . . . are common to other property contexts," and accordingly, these contexts should be considered for assessing liability under the CFAA.[280] Nevertheless, the majority failed to do so.

Next, the dissent addressed the majority's gates-up-or-down inquiry with respect to accessing a computer with or without authorization and then exceeding or not exceeding authorized access.[281] The majority framed this inquiry as black-and-white questions that can be answered with "yes" or "no," but the dissent challenged this.[282] In short, the dissent concluded "discerning whether the gates are up or down requires considering the circumstances that cause the gates to move."[283] For instance, an employee whose job involves working with sensitive data may be authorized to log into to his company laptop while at the office, but not in a foreign country because the data could be compromised due to a faulty network.[284] Circumstances matter, and "there is no reason to believe that if the gates are up in a single instance, then they must remain up indefinitely."[285] Referencing trespass, theft, and bailment, three property law concepts where circumstances matter, the dissent concluded that the majority's gates-up-or-down analysis of section 1030(a)(2) failed to properly harmonize the "without authorization" and "exceeds authorized access" clauses.[286]

Turning to statutory history, the dissent noted that the majority

[278] *See id.* (explaining that circumstances matter in assessing bailment) (citing 8 C. J. S., Bailments § 43, pp. 480–481 (2017)).

[279] *See Van Buren*, 141 S. Ct. at 1664 (Thomas, J., dissenting) ("A computer technician may have authority to access a celebrity's computer to recover data from a crashed hard drive, but not to use his access to copy and leak to the press photos stored on that computer.").

[280] *See id.* at 1665.

[281] *Id.* at 1666 (explaining how the dissent framed its rationale).

[282] *See id.* (challenging the majority).

[283] *Id.*

[284] *See id.* ("An employee who works with sensitive defense information may generally have authority to log into his employer-issued laptop while away from the office. But if his employer instructs him not to log in . . . he accesses the computer without authorization if he logs in anyway.").

[285] *Id.*

[286] *Id.* at 1665; *cf. id.* at 1666 ("In fact, my reading harmonizes *both* clauses with established concepts of property law.") (implying that the majority's reading did not harmonize the "without authorization" and "exceeds authorized access" clauses).

discussed the original text of the CFAA, which incorporated a purpose or circumstantial element to assessing liability.[287] In contrast with the majority, who the dissent described as "evad[ing] th[e] history," the dissent found that the removal of the purpose/circumstantial element actually broadened the CFAA rather than narrowed it.[288] While the majority concluded that removing this element signaled that Congress no longer intended purposes or circumstances to matter under the CFAA, the dissent found that deleting this element had the effect of expanding the law to give courts more leeway to punish under the CFAA.[289] The original term "purposes" limited section 1030(a)(2) to purpose-based constraints.[290] "Not entitled" is broader and more general, so it encompasses a wider array of punishable conduct than "purposes."[291] For instance, under the original language, the employee who logged into their sensitive account overseas would escape liability if they had the purpose of checking their email.[292] The newer, broader text of the CFAA would cover this employee because the "time or manner of his use" was not innocent, even if his purpose was innocent.[293] In sum, Congress intended to broaden the CFAA by eliminating the purpose/circumstantial element, not limit it.[294]

Finally, the dissent evaluated policy considerations, especially the overcriminalization argument made by the majority.[295] The dissent held that the mens rea requirement in section 1030(a)(2) serves to limit culpability because an offender must act with *intent* to be convicted under this prong of the CFAA.[296] Therefore, if an offender believes that their

[287] *Id.* at 1667.

[288] *Id.*

[289] *Van Buren*, 141 S. Ct. at 1668 (Thomas, J., dissenting) ("Often, deleting a word expands, rather than constricts, the scope of a provision.").

[290] *Id.* ("The term 'purpose' limited that clause to purpose-based constraints.").

[291] *Id.* ("By replacing the specific, limited term 'purposes' with the broader, more general phrase 'not entitled,' Congress gave force to those other kinds of constraints.").

[292] *Id.* ("The original text would not cover him, so long as he logged in for a proper purpose like checking work e-mail.") (concluding on coverage after applying the original text of the CFAA to the dissents earlier devised hypothetical).

[293] *Id.* ("The newer text would cover him because his entitlement to obtain or alter data is context dependent.").

[294] *See id.* (explaining the dissent's conclusion on congressional intent).

[295] *Id.* ("Concerned about criminalizing a 'breathtaking amount of commonplace computer activity,' the majority says that the way people use computers today 'underscores the implausibility of the Government's interpretation.'") (quoting *Van Buren*, 141 S. Ct. at 1661 (majority opinion)); *see also Overcriminalization*, NAT'L ASS'N CRIM. DEF. LAWS., https://www.nacdl.org/Landing/Overcriminalization [https://perma.cc/5WGE-ZBWQ] (discussing elements of overcriminalization).

[296] *Id.* ("For example, the statute includes the strict *mens rea* requirement that a person must 'intentionally . . . excee[d] authorized access.'") (alteration in original) (citing 18 U.S.C. § 1030(a)(2)); *see* cases cited, *supra* note 158 (examining defendant's criminal intent when assessing liability under the CFAA).

computer use is tolerated, the offender will fail to satisfy the intent requirement and not be liable under the statute.[297] For instance, an employee who checks the score of a sports game on his computer will not be liable under section 1030(a)(2) as written because the employee likely did not know that checking a score is a violation since this behavior is "common and tolerated."[298] The majority's argument that a broad interpretation of the statute will lead to overcriminalization is more hypothetical than practical.[299] Finally, a number of existing statutes may be harsh, including criminalizing removing a "single grain of sand from the National Mall," but such triviality does not give the court the "authority to alter statutes."[300] Misdemeanor punishments serve to combat overcriminalization.

The majority took a granular approach in its statutory interpretation of the CFAA, while the dissent favored the plain meaning of the statute.[301] The following Part will analyze the two approaches and argue that the dissent's interpretation of the CFAA adheres to the original purpose of the CFAA and its mens rea requirement. It will also evaluate the logic behind taking the circumstances of the offense into account when assessing liability under the CFAA.

III. ANALYSIS

Holding in favor of Van Buren, the majority resolved the circuit split by overruling Eleventh Circuit precedent to support a narrow interpretation of the CFAA's "exceeds authorized access" clause.[302] The respective arguments of the majority and dissent boil down to one key

[297] *Van Buren*, 141 S. Ct. at 1668 (Thomas, J., dissenting) ("The statute thus might not apply if a person *believes* he is allowed to use the computer a certain way because, for example, that kind of behavior is common and tolerated.") (emphasis in original); *see* sources cited, *supra* note 296 (illustrating how an individual's belief affects statute applicability).

[298] 18 U.S.C. § 1030(a)(2); *Van Buren*, 141 S. Ct. at 1668 (Thomas, J., dissenting) ("The Act also concerns only 'obtain[ing] or alter[ing] information *in* the computer,' . . . not using the Internet to check sports scores stored in some distant server (*i.e.*, a different computer.") (citing 18 U.S.C. § 1030(e)(6)).

[299] *Van Buren*, 141 S. Ct. at 1668 (Thomas, J., dissenting) ("I would not give so much weight to the hypothetical concern that the Government *might* start charging innocuous conduct and that courts *might* interpret the statute to cover that conduct.").

[300] *Id.* at 1669.

[301] *Compare id.* at 1656 (majority opinion), *with id.* at 1663-64 (Thomas, J., dissenting); *see also* Addicks, *supra* note 35, at 171–72 (contrasting way the majority and the dissent in *Van Buren* interpreted the CFAA).

[302] *See Van Buren*, 141 S. Ct. at 1662 ("[A]n individual 'exceeds authorized access' when he accesses a computer with authorization but then obtains information located in particular areas of the computer … that are off limits to him.") (reversing the Eleventh Circuit decision); *see also* Addicks, *supra* note 35, at 171–72 (summarizing the majority's holding).

difference: circumstances. Should an analysis of the CFAA's "exceeds authorized access" clause incorporate the circumstances of the offense, or should courts take a more lenient statutory approach?[303] The Supreme Court held the latter, allowing bad actors like Van Buren to escape punishment under the CFAA.[304]

A. Majority's Granular Textual Interpretation Distracts from Plain Meaning

First, the majority's over-reliance on the word "so" is distracting, and this highly technical analysis deviates from the purpose of the statute.[305] Nothing in sections 1030(a)(2) or 1030(e)(6) of the CFAA suggests that the word "so" should be given special weight, or that the word "so" is more important than any other word in the statute.[306] A sound reading of the statute gives equal weight to all words, and combines the meaning of all the words in congruence with the intent of the statute to fairly and justly prosecute potential defendants under the statute.[307] Supreme Court precedent in *Bond v. United States* established that plain meaning matters.[308] Technical jargon and legalese can interfere with a statute's purpose and goals. Congress intended the CFAA to prohibit unauthorized access to important information and data stored on computers.[309] In Van Buren's case, he abused his power as a police officer to impermissibly access license plate information.[310] Applying a plain meaning standard, he exceeded his authorized access to the detriment of the Cumming, Georgia Police Department.[311]

Even if the Court disregarded Van Buren's clear violation of

[303] *See* Assad, *supra* note 36, at 170–73 (illustrating that circuit split is a microcosm of the differences between the majority and the dissent's analysis); *see also* Addicks, *supra* note 35, at 164, 166 (explaining the differences between a broad and narrow approach).

[304] *See Van Buren*, 141 S. Ct. at 1662 (finding Van Buren did not 'exceed authorized access' as defined by the CFAA); *see also* Addicks, *supra* note 35, at 169 (allowing Van Buren to escape punishment).

[305] *Id.* at 1655–56 (referencing the word "so" twelve times); *see also* Goldman, *supra* note 5, at 11 (summarizing the reason for the Court's repeated reference to the term "so").

[306] *See generally* 18 U.S.C. §§ 1030(a)(2), 1030(e)(6).

[307] *See Van Buren*, 141 S. Ct. at 1661–62 (weighing the implications of applying the plain meaning of the statute); *see also* Goldman, *supra* note 5, at 9–11 (explaining the plain meaning approach when construing 'exceeds authorized access').

[308] Bond v. United States, 572 U.S. 844, 861 (2014) ("In settling on a fair reading of a statute, it is not unusual to consider the ordinary meaning of a defined term, particularly when there is dissonance between that ordinary meaning and the reach of the definition."); *see also* Goldman, *supra* note 5, at 9–11 (detailing the plain meaning approach).

[309] *See* Goldman, *supra* note 5, at 1 (detailing congressional intent in enacting the CFAA); *see generally CFAA Background*, *supra* note 39.

[310] *See Van Buren*, 141 S. Ct. at 1653 (explaining Van Buren's disputed actions); *see also* Assad, *supra* note 35, at 176 (providing a factual background of the case at hand).

[311] Assad, *supra* note 35, at 176 ("Van Buren was a sergeant with the Cumming, Georgia Police Department.").

department policy, he still exceeded his authorized access to access the database, or his "right" to access the database under a logical, plain meaning definition of "exceeds authorized access."[312] In *Rodriguez*, the illustrative Eleventh Circuit precedent for this case, company policy can serve as a guide when determining whether an employee had the "right" to exceed authorized access, but it should not be dispositive.[313] Van Buren's violation of department policy can support a conviction under the CFAA, but he must also "exceed authorized access" irrespective of department policy.[314] Van Buren did exceed such authorized access, considering his bad-faith intent, the bribe he took, and his motive to circumvent department policy.[315]

At oral arguments, the parties debated how the statute should be read: should circumstances matter? Van Buren relied heavily on the "words of the statute," in addition to considering what it omitted.[316] Specifically, Van Buren argued that "the definition of 'exceeds authorized access' doesn't talk about improper use," and the omission of proper use was intentional because Congress omitted the purpose element in 1986.[317] Van Buren also contended that legislative history should not resolve ambiguity; rather, a rule of lenity should apply.[318] Next, Van Buren made the overcriminalization argument, pointing to *United States v. Drew*, a

[312] *See Van Buren*, 141 S. Ct. at 1662 ("The parties agree that Van Buren accessed the law enforcement database system with authorization. The only question is whether Van Buren could use the system to retrieve license-plate information."); *see also* Goldman, *supra* note 5, at 9–11 (detailing the plain meaning approach).

[313] United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010), *abrogated by* Van Buren v. United States, 141 S. Ct. 1648 (2021); *see also* Brief for the United States at 13, 16, 17–19, Van Buren v. United States, 141 S. Ct. 1648 (2021) (No. 19-783), 2020 WL 5209541 [hereinafter Brief for the United States, *Van Buren*] (arguing that an offender's title and official job duties impact the extent to which they are authorized to access certain information or data stored on a computer).

[314] *See Rodriguez*, 628 F.3d at 1263 (explaining that a violation of company policy can be a factor to support a CFAA violation); *see also* Brief for the United States, *Van Buren*, *supra* note 313, at 13, 18–19 (explaining circumstances affect whether one is authorized access certain information or data stored on a computer).

[315] *See Van Buren*, 141 S. Ct. at 1653 (outlining Van Buren's history of bad-faith conduct); *see generally* Assad, *supra* note 35, at 176 (describing Van Buren's participation in the sting operation).

[316] *See* Transcript of Oral Argument at 7, Van Buren v. United States, 141 S. Ct. 1648 (2021) (No. 19-783) [hereinafter Oral Argument] (outlining statement of Petitioner urging Court to "look at the words of the statute"); *see also Van Buren*, 141 S. Ct. at 1660 n.11, 1661 (discussing congressional treatment of the now removed "purpose" reference once located in § 1030(a)(2)).

[317] Oral Argument, *supra* note 316, at 7; *see also Van Buren*, 141 S. Ct. at 1660 n.11, 1661 (discussing omission of the purpose element).

[318] *See* Oral Argument, *supra* note 316, at 13 ("And I think . . . because this is a criminal case, we think it's improper, if not, at the very least, very dangerous to rely on legislative history to resolve ambiguity. Instead, what you should look to are things like the Rule of Lenity . . . ."); *see also 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.").

Ninth Circuit case in which the defendant "was prosecuted for misusing MySpace."[319] According to Van Buren, nothing in the statute prohibits such overcriminalization.[320] Justice Thomas questioned the prevalence of such examples.[321] Using the language of the statute, Van Buren asserted the statute "simply asks whether the user is . . . entitled to obtain the information."[322] Van Buren argued that reading circumstances into the statute goes beyond its scope.[323] To the Government, a restrictive "gates-up-or-gates-down" inquiry fails to consider the intent of the offender.[324]

Another sticking point during oral argument was the parties' differing opinions of the precedential value of the United States Supreme Court case *Musacchio v. United States*.[325] The majority contended that *Musacchio* was irrelevant to Van Buren's case because the issue of the case was conspiracy, and it only discussed 18 U.S.C. § 1030(a)(2)(C), a subset of "'the exceeds authorized access prong,'" in dicta.[326] Therefore, *Musacchio* should not be relied upon as binding precedent. Though the *Van Buren* majority recognized that *Musacchio*'s main issue was not the CFAA, *Musacchio*'s language is nevertheless instructional for interpreting the CFAA in *Van Buren*. First, *Musacchio* is a recent Supreme Court case, the highest law in the United States.[327] Second, the

[319] *See* Oral Argument, *supra* note 316, at 9 (citing United States v. Drew*,* 259 F.R.D. 449 (C.D. Cal. 2009); *see also Van Buren*, 141 S. Ct. at 1661–62 (outlining the overcriminalization argument in favor of a narrow interpretation of the CFAA).

[320] *See* Oral Argument, *supra* note 316, at 18 ("[T]he core of the problem is there is no foothold in the statute to inch the statute forward to cover the conduct in this case without also covering all kinds of other violations of purpose-based restrictions that could appear . . . ."); *see also Van Buren*, 141 S. Ct. at 1662 (outlining the overcriminalization argument).

[321] *See* Oral Argument, *supra* note 316, at 8–9 (questioning the practicability of Van Buren's examples).

[322] Oral Argument, *supra* note 316, at 11; *see also Van Buren*, 141 S. Ct. at 1662 (providing examples of the overcriminalization argument).

[323] *See Van Buren*, 141 S. Ct. at 1657 (explaining that the statute's limited scope does not include reading 'circumstances' into it); *see also* Oral Argument, *supra* note 316, at 7 (arguing that a broad interpretation of the CFAA over-criminalizes innocent defendants).

[324] *See Van Buren*, 141 S. Ct. at 1663 (Thomas, J., dissenting) (explaining that the circumstances of the offense should matter considering the plain language of the statute); *see also* Oral Argument, *supra* note 316, at 31 (explaining the gates-up-or-gates down approach).

[325] Musacchio v. United States, 577 U.S. 237, 239 (2016) (prosecuting a defendant under 18 U.S.C. § 1030(a)(2)(C) for continuing to access the computer system of his former company to benefit his current company, a competitor); *see also Van Buren*, 141 S. Ct. at 1660 (refuting the Government's reliance on *Musacchio*).

[326] *See* Oral Argument, *supra* note 316, at 6 ("[T]he Court was simply giving a thumbnail summary of how the statute works. Of course, the question presented here was not presented there. And, in fact, not even the 'exceeds authorized access' prong was at issue there in the conspiracy issue the Court reached."); *see also Musacchio*, 577 U.S. at 239 (explaining the Court's reasoning, not directly related to the CFAA).

[327] Musacchio v. United States, 577 U.S. 237 (2016).

case directly references sections 1030(a)(2) and 1030(e)(6).[328] The Court opined that the CFAA "provides two ways of committing the crime of improperly accessing a protected computer."[329] First, a defendant can obtain access without authorization.[330] Second, a defendant can obtain authorized access but improperly use said access.[331] Applying this standard to Van Buren, he clearly violated the second method. Again, *Musacchio* is not binding precedent for *Van Buren*, but this Supreme Court case is a powerful statement in favor of both the Government's and dissent's reading of the CFAA.[332] The majority erred in nonchalantly dismissing the *Musacchio* argument.[333]

The overcriminalization argument, that is a broad reading of the "exceeds authorized access" clause, was challenged at oral arguments by the Government. "So" does not turn the CFAA into a "sweeping Internet police mandate" as Van Buren suggested.[334] The word "so" clarifies that one violates the CFAA by obtaining information via computer, not by other means.[335] Further, one who violates a website's terms of service is not always in violation of the CFAA because public websites, such as a news site, do not require authorization.[336] Even for sites that do require

[328] *See Musacchio*, 577 U.S. at 239–41 (indicting Musacchio under 18 U.S.C. § 1030(a)(2) and relying on 18 U.S.C. § 1030(e)(6)) in their CFAA interpretation); *see also* Oral Argument at 6, *supra* note 316 (questioning the relevance of the case).

[329] *Musacchio*, 577 U.S. at 240 (interpreting 18 U.S.C. § 1030(a)(2)(C)).

[330] *See id.* at 239–40 (explaining that access without authorization is a violation of the CFAA, a widely accepted principle); *see also* 18 U.S.C. § 1030(a)(2) (stating that accessing a computer without authorization or in excess of authorized access is a violation).

[331] *See Musacchio*, 577 U.S. at 239 ("(1) obtaining access without authorization; and (2) obtaining access with authorization but then using that access improperly."); *see also Van Buren*, 141 S. Ct. at 1653 (explaining the issue in the case was whether Van Buren exceeded his authorized access, although he did have at least some level of authorized access).

[332] *See* Oral Argument, *supra* note 316, at 63–64 (explaining the importance of *Musacchio* to the Government's argument); *see also Van Buren*, 141 S. Ct. at 1660 (minizing the importance of *Musacchio* as precedent for *Van Buren*).

[333] *See* Oral Argument, *supra* note 316, at 7 (arguing that *Musacchio* is not as important as the Government suggests); *see also Van Buren*, 141 S. Ct. at 1660 ("This paraphrase of the statute [in *Musacchio*] does not do much for the Government.").

[334] Oral Argument, *supra* note 316, at 4–5 (referencing the Government's argument that "so" prevents the CFAA from criminalizing commonplace activity such as checking the news via a company laptop).

[335] *See* Oral Argument, *supra* note 316, at 5 ("The word simply clarifies that a use—that the user must be prohibited from obtaining the information merely by a computer."). *Contra Van Buren*, 141 S. Ct. at 1655 ("Instead, 'so' captures *any* circumstance-based limit appearing *anywhere*—in the United States Code, a state statute, a private agreement, or anywhere else.").

[336] *See* Oral Argument, *supra* note 316, at 37 ("First of all, on the public website, that is not a system that requires authorization. It's not one that uses required credentials that reflect some

authorization, like a log-on account, Congress did not intend for such conduct to be criminalized under the CFAA.[337] In accordance with Congress's aim, the CFAA's use of "authorization" requires contextual "individualized consideration," in other words, the circumstances of the offense.[338]

B. Dissent's Interpretation Harmonizes Statutory History and Property Law

Turning to the original purpose of the statute, the dissent's interpretation of the CFAA in *Van Buren* more closely aligns with the CFAA's purpose to punish hackers than the majority's interpretation. Van Buren was not technically a hacker because he was authorized to access his police computer. Both the majority and dissent agreed on this point.[339] Where they differed, however, was whether Van Buren exceeded his authorized access in accessing the license plate information in exchange for a bribe.[340] Using the dissent's rationale, Van Buren functioned as a hacker by using his access for an improper purpose. The majority did not view Van Buren as a hacker because he did not force his way into the database, he accessed it using valid credentials.[341] The dissent's interpretation makes more logical sense and effectively punishes bad-faith conduct. The original purpose of the CFAA was punishing cybercrime to protect governmental data.[342] Van Buren impermisbly sharing sensitive, confidential data would have harmed the Cumming, Georgia Police Department.[343]

Justice Thomas's dissent relied heavily on analogizing the CFAA to traditional property law, which the majority reputed as misplaced and

specific individualized consideration."); *see also Van Buren*, 141 S. Ct. at 1662 (explaining when prosecution under the CFAA is not warranted).

[337] *See* Oral Argument, *supra* note 316, at 37–38 ("What Congress was aiming at here were people who are specifically trusted, people akin to employees, the kind of person . . . that had actually been specifically considered and individual authorized.").

[338] *Id.* at 38.

[339] *See Van Buren*, 141 S. Ct. at 1653 (explaining that Van Buren did not hack into the police database by noting that he used his existing credentials to access it); *see generally* Assad, *supra* note 36, at 176.

[340] *See Van Buren*, 141 S. Ct. at 1663–64 (contrasting the dissent and majority); *see also* Addicks, *supra* note 35, at 170–71 (explaining the majority's rationale in relation to the dissent).

[341] *Van Buren*, 141 S. Ct. at 1663.

[342] *See* Freeman, *supra* note 5 (explaining that the original purpose of the CFAA was to punish cybercrime); *see also CFAA Background*, *supra* note 39,39 (explaining that the original purpose of the CFAA was to punish computer misuse).

[343] *Van Buren*, 141 S. Ct. at 1653 (Van Buren's bad-faith attempting to reveal sensitive information for a non-law enforcement purporse would have harmed the reputation and integrity of the police department); *see generally* Assad, *supra* note 36, at 176.

unnecessary.[344] Legislative history shows that traditional property law is relevant to the CFAA.[345] For instance, Congress developed the CFAA to address inadequacies in existing property law.[346] Since the CFAA arose to fill in the gaps in existing property law, the core principles of property law should apply to the CFAA. Circumstances matter for trespass, theft, and bailment—all fundamental concepts of property law.[347] Considering the invention of the internet completely altered society, it was reasonable for Congress to devise a new statute, rather than fitting "'the square peg of computer fraud into the round hole of theft, embezzlement or even the illegal conversion of trade secrets.'"[348] Congress likely had theft, embezzlement, etc. in mind when enacting the CFAA, supporting the argument that the CFAA should be read in harmony with these property law concepts.[349] Circuit precedent demonstrates a divide as to what role company policy should play in assessing violations of the CFAA.[350] A middle ground approach suggests that company policy should not be dispositive, but should be considered. This middle ground approach is in congruence with the common law of property because the scope of consent matters in

[344] *See Van Buren*, 141 S. Ct. at 1662–63 (analogizing the CFAA to property law); *see also* Oral Argument, *supra* note 316, at 36 ("Section 1030 used the same language to extend the same property-based protection to the private computer records that contain our most sensitive financial, medical, and other data.").

[345] *See Van Buren*, 141 S. Ct. at 1663 (affirming the importance of property law in reading the statute); *cf.* Oral Argument, *supra* note 316, at 36–37 (arguing that 18 U.S.C. § 1030 uses plain language to offer property-based protection to sensitive information stored on computers).

[346] *See* Brief for the United States, *supra* note 313, at 30 ("Congress first enacted Section 1030 because it considered existing criminal laws "ineffective" for addressing 'computer abuse,' in part because 'much of the property involved does not fit well into categories of property subject to abuse or theft.'") (citing H.R. REP. NO. 894 (1984)).

[347] *See Van Buren*, 141 S. Ct. at 1662 (recounting fundamental concepts of property law); *see also* Oral Argument, *supra* note 316, at 36 (referencing property law in relation to language of section 1030 of the CFAA).

[348] *See* Brief for the United States, *supra* note 313, at 31 (citing S. REP. NO. 357, at 13–14 (1996)); *see also* Oral Argument, *supra* note 316, at 14–15 (examining congressional motivations for enacting the CFAA).

[349] *See Van Buren*, 141 S. Ct. at 1665 ("First, state laws *were* used to cover conduct like Van Buren's, but doing so 'require[d] considerable creativity' because those laws typically required either 'physical' entry (which fit poorly with computers) or 'depriv[ing]' a victim of property (which fit poorly where a person 'merely copied' data or engaged in forbidden 'personal uses.'") (citing *Kerr*, *supra* note 4, at 1607–08, 1610–11). The Court's comment suggests that Congress did not intend the language of of the CFAA to replace the circumstance-specific analysis typical to established property law principles.

[350] *See generally* WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199, 205 (4th Cir. 2012); Royal Truck & Trailer Sales & Servs., Inc. v. Kraft, 974 F.3d 756, 762 (6th Cir. 2020); United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010), *abrogated by* Van Buren v. United States, 141 S. Ct. 1648 (2021).

traditional property concepts such as theft.[351]

Leniency, an important argument made by the majority rooted in the Second Circuit (*Valle*) and the Ninth Circuit (*Brekka*), is Van Buren's strongest argument.[352] As established in Part I, the terms "access" and "authorized" have been subject to great debate historically, which suggests ambiguity in the language of the CFAA.[353] Therefore, as the majority argued, the rule of lenity freed Van Buren from prosecution under the CFAA.[354] Notably, the majority determined that the lenity argument was "extra icing on a cake already frosted."[355] In other words, the majority concluded that the rule of lenity was not necessary to free Van Buren, but served as additional support.[356] The rule of lenity only applies to Van Buren's case "if, after considering text, structure, history, and purpose, there remains a grievous ambiguity or uncertainty in the statute, such that the Court must simply guess as to what Congress intended."[357] As for Van Buren's argument, he curiously agreed the word "so" in section 1030(e)(6) *clearly defines* the scope of "exceeds authorized access" in section 1030(a)(2).[358] If true, this definition would prove that no "grievous ambiguity" existed in the CFAA, undermining the rule of lenity's applicability.[359] The plain meaning of section 1030(a)(2) combined with the legislative history and purpose of the CFAA supports that "grievous ambiguity" does not exist in the statute,

[351] *See* Brief for the United States, *supra* note 313, at 34 ("But an inquiry into the scope of consent is familiar to traditional criminal law, as when an employee takes a company-assigned car on a personal vacation or a hotel guest takes the robe from his room.").

[352] *See generally* United States v. Valle, 807 F.3d 508, 523 (2nd Cir. 2015); LVRC Holdings, LLC v. Brekka, 581 F.3d 1127, 1135 (9th Cir. 2009).

[353] *See* Kerr, *supra* note 458, at 1619–22 (discussing the ambiguities of "access" and "authorization" in the CFAA); *see also Brekka*, 581 F.3d at 1135 (looking to a plain-language interpretation of the term "authorization" in the CFAA).

[354] *Van Buren*, 141 S. Ct. at 1661; *see also Valle*, 807 F.3d at 528 (discussing the judiciary's role in addressing the rule of lenity).

[355] *Van Buren*, 141 S. Ct. at 1661 (citing Yates v. United States, 574 U.S. 528, 557 (2015) (Kagan, J. dissenting).

[356] *Van Buren*, 141 S. Ct. at 1661 (arguing that the rule of lenity was not essential to the Court's holding); *see also* Oral Argument, *supra* note 316, at 13 (implicating the rule of lenity).

[357] *See* Brief for the United States, *supra* note 313, at 48 (citing U.S. v. Castleman, 571 U.S. at 172–73); *see also Van Buren*, 141 S. Ct. at 1668 (explaining that Congress could not have foreseen how computers would be used in modern times when Congress first enacted the CFAA).

[358] *See* Oral Argument, *supra* note 316, at 5 ("The word ["so"] simply clarifies that a use – that the user must be prohibited from obtaining the information merely by a computer . . . [b]ut that is all the word does.") (Van Buren argues that the word so has a simple, clear use, contradicting the argument that the statute is geviously ambiguous); *see also* 18 U.S.C. § 1030(e)(6) (defining scope of "authorized access").

[359] Brief for the United States, *supra* note 313, at 48; *see also* Oral Argument, *supra* note 316, at 13–14 (referencing how courts interpret ambiguity in criminal statutes).

even if minor ambiguity does.[360] Therefore, Van Buren's lenity argument, while compelling, should fail.

The word "intentionally" in section 1030(a)(2) supports the Government's position that circumstances matter, and hinders Van Buren's overcriminalization argument. Van Buren contended that nothing in the statute prevents the criminalization of everyday activity, but the word "intentionally" does.[361] To use Van Buren's case as an example, he acted with "intent" to exceed authorized access because he understood the scope of his authority did not extend to accessing a license plate through the police department database for an unlawful purpose.[362] However, if Van Buren did not understand the scope of his authority, he could evade prosecution under the CFAA. For instance, an employee who checks the score of a sports game at work did not "intentionally" violate the CFAA because the employee likely thought taking a minute to check a score was authorized by their employer.[363] Likewise, an employee who checks the news on a work laptop did not "intentionally" exceed their authorized access through such a *de minimus* act that they believed their employer would not punish.[364] Van Buren, on the other hand, clearly acted with bad-faith intent to impermissibly distribute license plate information for a bribe, an act that he knew his employer would punish, and an act that he knew exceeded his authorized access.[365] This point, the "intentional" mental state requirement in section 1030(a)(2), is erroneously overlooked by Van Buren and the majority,

[360] *See* Brief for the United States, *supra* note 313, at 48 (arguing that "grievous ambiguity" did not exist in the CFAA); *see also* Oral Argument, *supra* note 316, at 47 (arguing that the CFAA is not ambiguous).

[361] *See Van Buren*, 141 S. Ct. at 1661 (explaining the overcriminalization effect of a broad interpretation of the CFAA); *see also* Brief for the United States, *supra* note 313, at 39 (discussing the statute's mens rea requirement).

[362] *See* Brief for the United States, *supra* note 313, at 39 ("Here, the trial evidence established that petitioner had been trained on the permissible uses of his access to the GCIC system and that he knew that accepting money to run a license plate for Albo was 'wrong.'"); *see also Van Buren*, 141 S. Ct. at 1653 (explaining that Van Buren received traning on proper purposes for accessing the database and therefore was aware he had an improper purpose).

[363] *See* Brief for the United States, *supra* note 313, at 39 ("Third, while petitioner has not contested that he 'intentionally' exceeded his authorized access, someone without the same clear understanding of the limits of her authority could."); *see also Van Buren*, 141 S. Ct. at 1662 (explaining that the Government's interpretation requirement would not be of assistance to someone checking sports game scores while using their work computer).

[364] *Contra Van Buren*, 141 S. Ct. at 1661–62 (challenging that commonplace activity would not be punished under the CFAA); *see also* Oral Argument, *supra* note 316, at 22 (explaining that adopting the Government's broad interpretation, even checking social media should be punishable under the CFAA).

[365] *See Van Buren*, 141 S. Ct. at 1653 (documenting Van Buren's bad-faith conduct); *see also* Brief for the United States, *supra* note 313, at 10 (outlining Van Buren's malintent).

and is a key point that the Government should have emphasized even more to persuade the Supreme Court majority.

C. Amendment to the CFAA Is Unnecessary Due to Its Mens Rea Element

It is reasonable to suggest that the CFAA should be amended to clarify its language and to explicitly punish conduct like Van Buren's. At oral argument, Van Buren even mentioned that the CFAA could be amended to encapsulate Van Buren's conduct.[366] While amendment to the CFAA could be useful, and is a reasonable option for Congress to take given the controversy and debate surrounding the CFAA, amendment is not necessary due to the "intent" element discussed above. Amendment could allow Congress to clarify its intentions, but congressional intent is not a dispositive issue in assessing liability.[367] The "intent" requirement punishes offenders like Van Buren but does not punish everyday offenders like an employee who checks the news or sports on their personal computer. This is contrary to what the Supreme Court majority suggested.[368]

The CFAA did not always have an "intentional" mens rea requirement, but this requirement has stood since Congress amended the CFAA in 1986.[369] Part of the 1986 amendments to the CFAA included raising the "mens rea requirement from 'knowingly' to 'intentionally.'"[370] This amendment had the effect of limiting the potential offenders under the CFAA because offenders needed to satisfy a more culpable mental state under the 1986 amendment.[371] The Model Penal Code defines both a purposeful or intentional mental state and a knowing mental state.[372] While these definitions are not dispositive and can vary by jurisdiction, the definitions are useful because they show how criminal mental states

[366] *See* Oral Argument, *supra* note 316, at 25 ("So, if Congress decides somehow that is not enough and it wants the CFAA to also be available in situations like this, it could amend the statute."). *Contra Van Buren*, 141 S. Ct. at 1668 (suggesting that the CFAA need not be amended further).

[367] *See Van Buren*, 141 S. Ct. at 1661 (explaining that congressional intent affects statutory interpretation, it is not the only such factor); *see also* Brief for the United States, *supra* note 313, at 43 (explaining that plain meaning can outweigh congressional intent).

[368] *See* Brief for the United States, *supra* note 313, at 43 (explaining that the language of the statute is more significant than congressional intent). *Contra Van Buren*, 141 S. Ct. at 1663 (suggesting that such everyday conduct would not be criminalized under a broader interpretation of the CFAA).

[369] *See generally* Goldman, *supra* note 5, at 1–5 (tracing the history of the CFAA); *CFAA Background*, *supra* note 39 (tracing the history of the CFAA).

[370] Brief for the United States, *supra* note 313, at 28.

[371] *See infra* text accompanying notes 373–377 (demonstrating that an "intentional" mental state captures a smaller range of conduct than a "knowing" mental state).

[372] *See* Model Penal Code § 2.02(2)(a)–(b) (AM. L. INST., Off. Draft & Rev. Comments 1985) (defining the purposeful/intentional and knowing mental states for a "model" jurisdiction).

are often defined. To paraphrase, a defendant acts purposefully or intentionally when the defendant is aware of the circumstances surrounding the offense and the defendant *consciously engages* in conduct to cause an intended result.[373] Purposefully or intentionally is the highest culpable mental state of the four listed in the Model Penal Code.[374] A defendant acts knowingly when the defendant is aware of the circumstances surrounding the offense and is *aware* that his actions would cause an intended result.[375] The difference between these two mental states is that the former requires the defendant to act with an objective to harm whereas the latter only requires the defendant to be aware that harm would result.[376] Therefore, contrary to Van Buren's suggestion, the CFAA does in fact have a built-in mechanism that limits liability— a heightened mens rea requirement.[377]

Applying these mental state standards to Van Buren, he acted with intent or purpose, not mere knowledge. Van Buren consciously took a bribe and accessed sensitive information in his department's database for the purpose of distributing it to Albo.[378] Van Buren intended to violate the policies of his department by sharing sensitive data.[379] He knew that releasing the data to Albo was a violation, but he intended to do so

[373] *Id.* § 2.02(2)(a)

> A person acts purposely with respect to a material element of an offense when:
> (i) if the element involves the nature of his conduct or a result thereof, it is his conscious object to engage in conduct of that nature or to cause such a result; and
> (ii) if the element involves the attendant circumstances, he is aware of the existence of such circumstances or he believes or hopes that they exist.

[374] *See* Model Penal Code § 2.02(2)(a)–(d) (AM. L. INST., Off. Draft & Rev. Comments 1985) (defining four mental states: purposefully, knowingly, recklessly, and negligently in decreasing order of culpability).

[375] *Id.* § 2.02(2)(b)

> A person acts knowingly with respect to a material element of an offense when:
> (i) if the element involves the nature of his conduct or the attendant circumstances, he is aware that his conduct is of that nature or that such circumstances exist; and
> (ii) if the element involves a result of his conduct, he is aware that it is practically certain that his conduct will cause such a result.

[376] *See id*. (differentiating between the mental states); Brief for the United States, *supra* note 313, at 28 (discussing the history of the CFAA's mental state requirement).

[377] *See* Brief for the United States, *supra* note 313, at 28, 39 (tracing and explaining the CFAA's intent requirement).

[378] *See* Van Buren v. United States, 141 S. Ct. 1648, 1653 (2021) (describing compensation Albo would pay to Van Buren for running the search); *see also* Assad, *supra* note 36, at 176 (describing the chain of events leading Van Buren to run the search pursuant to Albo's request).

[379] *See Van Buren*, 141 S. Ct. at 1652 (explaining that Van Buren attempted to intentionally release data to the detriment of the police department); *see also* United States v. Van Buren 940 F.3d 1192, 1198 ("In addition, Van Buren confessed he had run a tag search for Albo and he knew doing so was 'wrong.').

nonetheless.[380] If Van Buren acted with mere knowledge, he would have to be aware that distributing the license plate information would harm the department, rather than a conscious objective to harm. If Van Buren did not take a bribe for his acts, and was merely doing a favor for a friend, he would have a better argument that his act only satisfied the "knowingly" mental state. However, since Van Buren took a bribe in violation of department policy, and then intended to release sensitive information also in violation of department policy, it is easy to argue that he acted with the conscious objective to harm his department's integrity.[381] If the facts of the case were changed such that Van Buren only knowingly violated department policy (i.e., distributed a license plate to a family member for the purpose of helping someone in need), this would demonstrate a less culpable mental state, one that would not be punishable under the CFAA's strict intentional mental state requirement. In conclusion, Van Buren intentionally exceeded his authorized access by distributing confidential police data, an act that the CFAA punishes.

IV. Impact

A. Majority's Interpretation Does Not Punish Bad-Faith Actors

The majority's decision to reverse Van Buren's conviction under the CFAA sets the precedent that bad-faith actors who improperly distribute sensitive data will not necessarily be punished under the CFAA.[382] This decision has drastic effects for employers who cannot rely on the CFAA to protect their businesses from the bad-faith acts of employees. Specifically, employers need to be even more careful in writing their department policies to ensure that bad-faith conduct such as Van Buren's is prohibited.[383] Under the majority's interpretation, Van Buren cannot

[380] *See Van Buren*, 141 S. Ct. at 1653 (explaining that Van Buren acted with an intentional mental state); *see also* Brief for the United States, *supra* note 313, at 40 ("Petitioner's conduct here-intentionally abusing his individualized access privilege to misappropriate confidential computer data-is precisely the type of conduct at which Section 1030 is directed.").

[381] *See Van Buren*, 141 S. Ct. at 1653 (explaining that the facts establish that Van Buren accessed information for an improper use); *see also* United States v. Van Buren 940 F.3d 1192, 1198 ("Finally, Van Buren conceded he understood the purpose of running the tag was to discover and reveal to Albo whether Carson was an undercover officer."); Brief for the United States, *supra* note 313, at 36 (explaining that Van Buren had been trained in proper uses of the system, which he violated).

[382] *See* Brief for the United States, *supra* note 313, at 40 (explaining the issues with allowing bad-faith conduct to go unpunished under the CFAA); *see also* Patricia C. Collins, *'Van Buren v. United States': Supreme Court Eliminates a Remedy for Employers*, LEGAL INTELLIGENCER (June 18, 2021), https://www.law.com/thelegalintelligencer/2021/06/18/van-buren-v-united-states-supreme-court-eliminates-a-remedy-for-employers/ [https://perma.cc/5EN5-FDBN] (noting how the majority's holding is problematic).

[383] *See* Collins, *supra* note 382 ("While it is important to have written workplace policies

even be prosecuted for a civil violation of the CFAA.[384] Employers must prohibit the improper distribution of sensitive information in their contracts to recover equitable relief if an employee releases such information, harming the company's reputation and profits.[385] Such carefully written contracts will likely require expensive lawyers, putting a significant burden on smaller companies and startups particularly technology startups whose most significant assets are their software platform and digital code. The CFAA is not employers' only route to seek remedy for conduct such as Van Buren's, since conversion, trade secret, or duty of loyalty claims may apply.[386] Nevertheless, the Supreme Court's decision needlessly and improperly deprives employers from seeking remedy under the CFAA and fails to deter bad-faith conduct such as Van Buren's via criminal punishment. The CFAA "is unquestionably the most important federal statute protecting American computer systems and the data stored on those systems," and the Supreme Court severely limited its scope.[387]

DePaul's Center for Intellectual Property Law & Information Technology (CIPLIT®), argued that the CFAA must criminalize "malicious behavior" that infringes on "possessory interests."[388] It contends that the majority's decision does not "harmonize the rule of law with computer technology" because Van Buren violated the department's "superior possessory interest" in sensitive law enforcement data.[389] Since the CFAA is a statute that protects intellectual property, "traditional notions of consent to use of property" should be applied under the

regarding use of computers and electronic information, a violation of those policies alone will not be enough to state a claim for civil or criminal liability under the CFAA."); *see also* Oral Argument, *supra* note 316, at 18 (explaining that contract, employee handbook, course syllabus, and oral restrictions all serve to limit authorized access beyond the CFAA).

[384] *See* Collins, *supra* note 382 ("Under the holding in Van Buren this conduct on the part of the employee is not a violation of the CFAA, and for that reason cannot form the basis of a civil claim."); *see also Van Buren*, 141 S. Ct. at 1652 (explaining civil liability in the statute).

[385] *See* Collins, *supra* note 382 ("Employee contracts should require return of any information (including electronic information and data) upon termination, and prohibit the employee from keeping copies. This will provide the employer with a breach of contract claim."); *see also* Oral Argument, *supra* note 316, at 34 (explaining that contract-based restrictions limit the scope of unauthorized use).

[386] *See* Collins, *supra* note 382 ("Common law claims such as conversion or breach of the duty of loyalty may also apply to remedy the wrong.").

[387] Brief of the Managed Funds Ass'n, *supra* note 11, at 3.

[388] *See* Brief for Karen Heart and Anthony Volini of CIPLIT as Amici Curiae Supporting Respondent at 1, Van Buren v. United States, 141 S. Ct. 1648 (2021) (No. 19-783) [hereinafter Brief for Karen Heart and Anthony Volini of CIPLIT].

[389] *Id.* at 1, 2.

CFAA.[390] A failure to incorporate common law theft into the reading of the CFAA allows bad actors like Van Buren to go unpunished.[391] The CFAA can and should prohibit the "publication of confidential data."[392] An employer's right to protect their company's sensitive data must be protected.[393] Not only does the majority's narrow view of the CFAA fail to punish bad actors who disseminate confidential information for improper purposes, but it also sets the precedent that such actors can escape criminal punishment for their intentional bad acts.[394]

B. Negative Impacts on Law Enforcement and Governmental Agencies

Simply put, the Supreme Court's decision negatively impacts law enforcement.[395] It does so for two main reasons. First, the decision sets the precedent that an improper dissemination of sensitive police department data by an officer is not punishable under the CFAA.[396] Second, the decision hampers law enforcement's ability to successfully protect the sensitive computer data of others.[397] Federal law enforcement agencies heavily rely on storing massive amounts of highly sensitive information in computer databases.[398] Further, many "authorized" users have access to such systems, including hundreds and thousands of

[390] *Id.* at 5.

[391] *See id.* at 3 ("Prior to enactment of the CFAA, various precedents supported the principle that stealing employer . . . property supports a criminal charge . . . includ[ing] theft of employer money or misuse of employer assets for personal benefit so long as the misuse is clearly not authorized by the employer."); *see also Van Buren*, 141 S. Ct. at 1663 (explaining the importance of punishing Van Buren's bad-faith conduct).

[392] Brief of Karen Heart and Anthony Volini of CIPLIT, *supra* note 388, at 15.

[393] *Cf.* Brief for the United States, *supra* note 313, at 7 (explaining the sensitive nature of the data found in the system); *see also* Brief of the Managed Funds Ass'n, *supra* note 11, at 4 (explaining the need to protect sensitive data files for private businesses).

[394] *See* Brief for the United States, *supra* note 313, at 40–43 (arguing that bad-faith conduct like Van Buren's must be punished under the CFAA). *Contra Van Buren*, 141 S. Ct. at 1662 (explaining why the majority failed to punish Van Buren for his bad-faith conduct).

[395] *See* Brief of the Federal Law Enforcement Officers, *supra* note 11, at 6 (explaining how confining the applicability of the CFAA to external hackers may harm law enforcement).

[396] *See* Brief for the United States, *supra* note 313, at 40–43 (explaining that Van Buren's conduct should be punished under the CFAA). *Contra Van Buren*, 141 S Ct. at 1662 (explaining why the majority did not punish Van Buren's conduct under the CFAA).

[397] *See* Brief for the United States, *supra* note 313, at 40–43 (explaining the important role law enforcement has in enforcing data protection of others); *see also Van Buren*, 141 S. Ct. at 1666 (explaining how the majority's interpretation complicates the process of protecting sensitive law enforcement data).

[398] *See* Brief of the Federal Law Enforcement Officers, *supra* note 11, at 6 ("Like most modern organizations, federal law enforcement agencies rely heavily on computerized systems to fulfill their core mission of protecting the public and the Nation."); *see also* Oral Argument, *supra* note 316, at 26 (explaining that government, financial, and healthcare employees all have access to very sensitive personal information).

federal, state, and local officers, such as Van Buren.[399] Further, civilians including "crime analysts, dispatchers, forensic technicians, and records manage[rs]" have access to these sensitive databases.[400] Since these databases are so robust and accessible by many actors, departments must have sufficient authority to protect them.[401] Bad actors who misuse such information could threaten the safety of civilians, hamper ongoing investigations, and even compromise national security.[402] In Van Buren's case, distributing license-plate information to Albo might seem trivial, but permitting such conduct could allow even more significant and serious threats to public safety to go unpunished under the CFAA.[403]

As a police officer, Van Buren owed a duty to serve and protect the public.[404] He clearly violated this duty and went unpunished under the CFAA. Van Buren was "specifically trusted" and "individually authorized" to use the police department databases, but then abused this trust and exceeded his authorized access.[405] Law enforcement agencies, among other governmental entities, have access to "all sorts of highly personal information for use in performing their jobs."[406] Abusing this information to make money, commit a crime, or harass others can cause significant damage and harm.[407] Both public and private businesses are at risk if such improper acts go unpunished. Those with the privilege to

[399] *See* Brief of the Federal Law Enforcement Officers, *supra* note 11, at 9 ("According to the Bureau of Justice Statistics, as of 2016 there were more than 132,000 full-time federal law enforcement officers employed by 83 federal agencies, along with hundreds of thousands of state and local officers."); *see also* Oral Argument, *supra* note 316, at 55 (explaining the detriment of police officers abusing their trust).

[400] Brief of the Federal Law Enforcement Officers, *supra* note 11, at 9–10.

[401] *Cf. id.* (explaining the need to protect sensitive databases); Oral Argument, *supra* note 316, at 26 (explaining the need to protect sensitive databases across a variety of industries).

[402] *See* Brief of the Federal Law Enforcement Officers, *supra* note 11, at 10 ("As a result of the nature of the data stored on law enforcement computer systems and the critical role those systems play in law enforcement's routine activities, malicious actors who misuse such confidential information could create significant threats to the safety of individuals and to the integrity of ongoing investigations."); *see generally* Brief of Karen Heart and Anthony Volini of CIPLIT, *supra* note 388, at 7–9 (arguing the need to punish bad-faith actors).

[403] *See* Brief for the United States, *supra* note 313, at 35 ("The implication is that this case, which involves conduct at the core of Section 1030, presents the only guardrail against those hypothetical future decisions."); *see also* Oral Argument, *supra* note 316, at 51 (explaining the danger that insiders present to releasing sensitive data).

[404] *See* Cumming Police Department, https://cummingpd.net [https://perma.cc/NR9Z-HXLU] (last visited April 15, 2023) ("We are here to serve our City and its Citizens.").

[405] Oral Argument, *supra* note 316, at 38.

[406] *Id.* at 14.

[407] *See id.* ("But, if they use that [highly personal information] for personal purposes to make money, protect or carry out criminal activity, [or] to harass people they don't like, they can do enormous damage."); *see also* Oral Argument, *supra* note 316, at 51 (arguing insiders are particularly prone to releasing sensitive data because they have access to it).

access sensitive data need to be held accountable if they breach their trust.[408]

This argument extends beyond law enforcement agencies, including all levels of government, bank, and healthcare employees.[409] Government databases store biometric data, including fingerprints, facial recognition tools, and DNA.[410] Improper use of such data can corrupt dual-factor authentication processes and lead to widespread fraud.[411] In addition, the Department of Homeland Security's databases contain social security numbers, addresses, telephone numbers, occupations, credit card numbers, and criminal histories.[412] Other governmental agencies, such as the Department of Housing and Urban Development and the National Institute of Health's Clinical Research Information System, contain similarly sensitive data, with the latter concentrating on medical history.[413] Such sensitive data needs to be protected and secured at all costs, but *Van Buren* suggests that one could leak this data for an improper purpose and evade liability under the CFAA.

C. Negative Impacts on Businesses

The majority's decision has severe complications for the investment industry.[414] The Managed Funds Association (MFA), a not-for-profit organization that represents the global alternative investment industry,

[408] *See* United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010) (overruled in part) (explaining that bad-faith actors like Rodriguez should be punished under the CFAA).

[409] *See* Brief of the Federal Law Enforcement Officers, *supra* note 11, at 6 (including a wide variety of entities that need protection under the CFAA); *see also* Oral Argument, *supra* note 316, at 26 (arguing that government, finance, and healthcare employees have access to very sensitive personal data and are able to disclose it).

[410] *See* Brief of *Amici Curiae* Electronic Privacy Information Center (EPIC) and Fifteen Technical Experts and Legal Scholars in Support of Respondent, Van Buren v. United States, 141 S. Ct. 1648 (2021) (No. 19-783) at 16 [hereinafter Brief for EPIC et al.] ("Government databases increasingly store some of the most sensitive personal information, including biometric data such as fingerprints, facial recognition templates, and DNA profiles."); *see also* Oral Argument, *supra* note 316, at 26 (explaining that many entities store sensitive data).

[411] *See* Brief for EPIC et al., *supra* note 410, at 16 ("Those who improperly access biometric data can create fraudulent copies of the biometric traits to mislead a biometric sensor or identify their biometric doppelganger-someone who shares enough biometric traits to trick a biometric sensor."); Oral Argument, *supra* note 316, at 55 (explaining that insiders pose a particular threat to sensitive data).

[412] *See* Brief for EPIC et al., *supra* note 410, at 14 ("For example, the Department of Homeland Security maintains several databases that hold individuals' names, Social Security numbers, dates of birth, addresses, telephone numbers, citizenship information, gender, occupation, driver's license information, credit card numbers, travel itineraries, and criminal histories.").

[413] *See* Brief for EPIC et al., *supra* note 410, at 15 (citing specific entities that need their sensitive data protected); *see also* Oral Argument, *supra* note 316, at 26 (citing more entities that need to be protected).

[414] *See* Oral Argument, *supra* note 316, at 26 (citing the need to protect sensitive financial data); *cf.* Brief of the Managed Funds Ass'n, *supra* note 11, at 4 (implying that sensitive financial data requires the utmost protection).

concluded that the majority's narrow interpretation of the CFAA harms investment managers and fund investors.[415] Employees, contractors, vendors, suppliers, and third parties all have access to investment firms' technologically complex and robust financial databases.[416] These "inside" employees are essentially immune from punishment under the CFAA according to the majority.[417] Investment databases contain information such as non-public personal financial information, proprietary market research and data analysis, sensitive trading strategy information, labor-intensive stock price history data reports, and other key financial records.[418] This information is essential to the success of the firm, and its improper dissemination puts the entire firm at risk. While the MFA's argument is specific to the financial investment industry, it is easy to extrapolate their rationale to other businesses and industries.[419] Most businesses have sensitive, proprietary digital data that needs to be kept safe on computers for the well-being of the business.[420] The majority in *Van Buren* harmed these businesses by allowing employees like Van Buren to leak such data and get away with

[415] *See* Brief of the Managed Funds Ass'n, *supra* note 11, at 4 ("The theft of such intellectual property or proprietary information harms investment managers, fund investors, potentially other market participants and the economic competitiveness of U.S. firms to the extent that such property is exported to a foreign competitor."); *see also* Brief for the United States, *supra* note 313, at 40 (explaining that Van Buren's bad-faith conduct must be punished under the CFAA).

[416] *See* Brief of the Managed Funds Ass'n, *supra* note 11, at 4, 7 (explaining that many individuals are able to log in to sensitive investment management databases with sensitive information, and these individuals need to be held accountable if they improperly use or distribute this data); *see also* Oral Argument, *supra* note 316, at 55 (explaining the insider threat to sensitive data).

[417] *See* Brief of the Managed Funds Ass'n, *supra* note 11, at 5 ("[I]f the line between authorized and unauthorized activity is *only* defined with reference to technological controls protecting against outside hackers, then it becomes nearly impossible for any user of a computer system with access credentials . . . to violate the CFAA, *no matter how egregious* his conduct . . . ."); *see also* Oral Argument, *supra* note 316, at 55 (arguing that insiders with access credentials should not be immune from CFAA liability).

[418] *See* Brief of the Managed Funds Ass'n, *supra* note 11, at 7 (detailing the specific types of sensitive data that need protection); *see also* Oral Argument, *supra* note 316, at 26 (listing the industries that most need protection).

[419] *See e.g.*, Bob Violino, *Data Privacy Rules Are Sweeping Across the Globe, and Getting Stricter*, CNBC (Dec. 22, 2022, 11:21 AM), https://www.cnbc.com/2022/12/22/data-privacy-rules-are-sweeping-across-the-globe-and-getting-stricter.html [https://perma.cc/U2W8-FU3H] ("Businesses, especially those in highly regulated sectors such as financial services, health care and government – and those that operate in multiple countries – are faced with a growing number of data privacy regulations.").

[420] *See* Brief of the Managed Funds Ass'n, *supra* note 11, at 6 (explaining that business have data that needs protection); *see generally* Collins, *supra* note 382 (explaining that businesses need protection).

it under the CFAA.[421]

More oversight, not less, is needed to protect personal privacy and the digital assets of entities. The majority's decision puts an individual's personal information, including home address, financial data, and health history at greater risk of leak.[422] The same goes for entities, whose sensitive financial data, financial tools, and trade secrets are at greater risk of leaks.[423] Recent statistics show that cybercrime is only increasing in prevalence, and both Congress and the Supreme Court should keep in mind the importance of deterring cybercrime and the improper distribution of sensitive data.[424] In particular, fraud and identity theft reports have steadily risen since 2017.[425] While the dissent in *Van Buren* took an important stance against cybercrime, the majority unfortunately enabled it.[426]

CONCLUSION

In *Van Buren v. United States*, the Supreme Court overly relied on a granular interpretation of the "exceeds authorized access" clause as defined in section 1030(e)(6) of the CFAA. The majority overread the statute to the detriment of individuals and companies who need their sensitive digital information properly protected. The Court allowed Van Buren, a bad-faith actor, to escape punishment under the CFAA. In contrast, the dissent would have upheld Van Buren's conviction, taking

[421] *See* Van Buren v. United States, 141 S. Ct. 1648, 1662 (2021) (holding that Van Buren did not violate the CFAA); *see generally* Collins, *supra* note 382 (explaining that businesses need protection).

[422] *See* United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010), *abrogated by* Van Buren v. United States, 141 S. Ct. 1648 (2021) (explaining the implications that the Eleventh Circuit discussed); *see also* Brief of the Managed Funds Ass'n, *supra* note 11, at 7 (explaining that a narrow interpretation of the CFAA puts personal financial information at risk).

[423] *See generally* Brief of the Managed Funds Ass'n, *supra* note 11, at 4 (explaining that financial companies are especially at risk); Brief of the Federal Law Enforcement Officers, *supra* note 11, at 13 (explaining that insider threats are not limited to governmental agencies).

[424] *See generally* INTERNET CRIME REPORT 2021, *supra* note 20; *Facts + Statistics: Identity Theft and Cybercrime*, INS. INFO. INST., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#:~:text=At%20least%20422%20million%20individuals,5%20percent%20decrease%20from%202021. [https://perma.cc/CD9Q-E2S8] (last visited Apr. 8, 2023) (showing that cybercrime is increasing in prevalence).

[425] *See Facts + Statistics*, *supra* note 424 (explaining that fraud and identity theft reports have risen); *see also* INTERNET CRIME REPORT 2021, *supra* note 20 (explaining that cybercrime is on the rise).

[426] *Cf. Van Buren*, 141 S. Ct. at 1663 ("As a police officer, Nathan Van Buren had permission to retrieve license-plate information from a government database, but only for law enforcement purposes. Van Buren disregarded this limitation when, in exchange for several thousand dollars, he used the database in an attempt to unmask a potential undercover officer."); *see generally* Brief of the Federal Law Enforcement Officers, *supra* note 11 (explaining the issues with the majority's interpretation).

into account the plain meaning of the statute, legislative history, and the fundamentals of property law. The CFAA's "intent" element should be construed such that bad-faith actors like Van Buren are punished, whereas those who commit *de minimus* violations would not be punished. Under the CFAA, circumstances of the offense should matter. The majority's narrow interpretation runs counter to the increasing importance of cybersecurity and data protection in modern American society. The effects of this decision could be drastic.