William & Mary Business Law Review

Volume *14 (2022-2023)*
Issue 1

Article 6

11-2022

Keeping Gates Down: Further Narrowing the Computer Fraud and Abuse Act in the Wake of Van Buren

George F. Leahy

KEEPING GATES DOWN: FURTHER NARROWING THE COMPUTER FRAUD AND ABUSE ACT IN THE WAKE OF *VAN BUREN*

GEORGE F. LEAHY[*]

ABSTRACT

Internet-connected devices have become essential parts of personal and professional life. As these devices have grown in importance and prevalence in the workplace, so too have federal computer regulations come into the spotlight. Prior to the Supreme Court's Decision in Van Buren v. United States*, the Circuit Courts of Appeals were split on the interpretation of the "exceeds authorized access" clause of the Computer Fraud and Abuse Act (CFAA), a commonly invoked federal law that imposes criminal and civil liability for computer misuse. Although the Court's narrow holding clarified the definition of "exceeds authorized access," the Court did not specify what forms of access restrictions, if exceeded, create a CFAA cause of action.*

This Note examines enforceable access restrictions for the purposes of CFAA liability in the wake of the Supreme Court's Decision in Van Buren v. United States. *This Note argues that the unresolved issue of CFAA enforceable access restrictions should be further narrowed to include only technological or code-based limitations. This narrowing would be in line with both the Court's reading of the CFAA and the original legislative purpose of the CFAA. Because the CFAA was primarily implemented as a computer hacking statute, its application should be limited only to when an individual breaks through a technological barrier to access information and, conversely, the CFAA should not be enforced where an individual breaches merely contractual or other non-code-based*

[*] JD Candidate, 2023, William & Mary Law School; BA, 2020, Elon University. The Author would like to thank his family and friends for their love and support, as well as the *William & Mary Business Law Review* staff for their assistance in preparing this Note for publication.

access restrictions. Narrowing the CFAA in this way would also ensure heightened cybersecurity measures for companies that manage highly sensitive information and safeguard consumer data privacy in the absence of cohesive U.S. cybersecurity and data privacy laws.

TABLE OF CONTENTS

INTRODUCTION

Three people, Employee A, Employee B, and Employee C, sit down at their desks and power on their work computers. Each uses the credentials provided to them by their employer to log in. As they wait for their desktops to load, a fourth employee walks over and tells them about an embarrassing document that he found saved on Drive X, a network drive located on the employer's server.[1] Interested, and despite knowing that the employee handbook prohibits accessing Drive X for non-work purposes, the three employees try to find and open the folder that contains the embarrassing document.

Employee A attempts to open Drive X. Nothing in either Employee A's work contract or communications with her employer preclude her from accessing the folder or Drive X, but the system administrator has restricted A's access to both Drive X and the folder using the employer's server software, making Employee A unable to open the folder. However, Employee A conveniently has an advanced degree in computer science and attends hackathon competitions in her spare time. In fact, Employee A has developed a software tool that changes access permissions on the same types of servers that her employer uses. Employee A uses this tool to change the server's access permissions, enables herself access to Drive X and the folder, and downloads the embarrassing document.

Employee B finds the folder next and attempts to open it. The system administrator has not set any software-based access restrictions on Employee B's account. However, Employee B's employment contract includes a clause that explicitly states he may not access files or folders on Drive X. Nevertheless, Employee B opens Drive X and downloads the embarrassing document.

Finally, Employee C finds the document and attempts to open it. Employee C's employment contract does not preclude him from accessing Drive X or any of the folders or files therein, nor has the system administrator disabled Employee C's access using the server software. However, following a viral internet post

[1] A network drive is a drive, similar to a physical hard drive, that computers or servers on the same local or internet network are jointly able to access. *Network Drive*, COMPUTER HOPE (Mar. 12, 2022), https://www.computerhope.com/jargon/n/network-drive.htm [https://perma.cc/AR9E-8XZ8].

by Employee C containing a copy of a different document stored on Drive X one month earlier, Employee C received a cease-and-desist letter from his employer requesting that he no longer use or access any of the folders or files on Drive X. Nevertheless, Employee C opens Drive X, finds the folder, and downloads the embarrassing document.

All three employees publish the document on the internet, causing their employer's sales to rapidly diminish. The next day, all three employees are fired for violating the policies contained within the employee handbook. Their problems do not end there, however. As soon as they arrive at their homes, all three are served with a complaint. The company has sued each of them, and a prosecutor is considering bringing charges against them, for intentionally accessing a computer, "exceed[ing] authorized access, and thereby obtain[ing] . . . information from [a] protected computer" in violation of the Computer Fraud and Abuse Act (CFAA).[2] Which of the employees is potentially liable? The answer may depend on which court the cases are filed in.

The Supreme Court recently ended a circuit split and held that individuals exceed authorized access to a computer system in violation of the CFAA when they use their authorized access to then obtain information from "files, folders, or databases . . . to which their computer access does not extend."[3] In its decision, the Court clarified that an individual does not exceed authorized access when they merely have an improper motive for using a system or file that is otherwise available to them.[4] Rather, the "exceeds authorized access" clause of the CFAA applies when an individual enters a system using otherwise authorized means to access an off-limits file, folder, or database within that system.[5] However, the Court did not specify what kinds of access restrictions (the means by which the file is made off-limits to the user), constitute a CFAA violation for "exceeding authorized access" if bypassed by the user.[6]

[2] 18 U.S.C. § 1030(a)(2).

[3] Van Buren v. United States, 141 S. Ct. 1648, 1652 (2021).

[4] *Id.*

[5] *Id.*

[6] *Id.* at 1659 n.8 ("For present purposes, we need not address whether this inquiry turns only on technological (or 'code-based') limitations on access, or instead also looks to limits contained in contracts or policies.").

Applying this to the above scenario, none of the employees would have violated the CFAA if they had access to Drive X for a legitimate business purpose but used it instead to download the embarrassing document, if doing so was merely contrary to their workplace policies.[7] However, each of the employees had their access to Drive X restricted or limited—either code-based restrictions in the case of Employee A, contract-based restrictions in the case of Employee B, or employer communications-based restrictions in the case of Employee C.[8] After *Van Buren*, it is clear that Employee A violated the CFAA,[9] but it is unclear whether Employee B, Employee C, or both, exceeded their authorized access by violating their respective access restrictions.[10]

As such, while *Van Buren* resolved a circuit split concerning whether using authorized access for an improper purpose was considered "exceeding authorized access" for the purposes of the CFAA,[11] it left the potential for other disparate interpretations of the "exceeds authorized access" clause when it chose not to clarify the role of access limitations or restrictions in CFAA liability.[12] Thus, an individual who logs into a system with authorization but then intentionally accesses a file that is off-limits has clearly violated the CFAA because their use "exceeds authorized access."[13] However, the statutory language of the CFAA does not define what types of boundaries make a file off-limits,[14] an issue that the Court recognized but declined to resolve.[15] Consequently, courts in some circuits might find that violations of either an employment agreement or a cease-and-desist letter that requests an individual not access particular files would

[7] *See id.* at 1652.

[8] *See* 18 U.S.C. § 1030(e).

[9] In footnote 8 of *Van Buren*, the language "*only* on technological . . . *or instead also* . . . contracts or policies" implies that the Court does see technological or code-based access restrictions as valid for the purposes of the CFAA but leaves open the question of access limitations in contracts or policies. *See Van Buren*, 141 S. Ct. at 1659 n.8.

[10] *See id.*

[11] *See id.* at 1654.

[12] *See* discussion *infra* Part V; *see, e.g.*, Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1069 (9th Cir. 2016) (indicating that cease-and-desist orders represent actionable access limitations).

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

[14] *See* 18 U.S.C. § 1030(e).

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

create a CFAA cause of action,[16] while courts in other circuits might take a different view.[17]

To resolve this potential split, CFAA liability for exceeding authorized access should only be imposed where an individual breaks through a technological or code-based access restriction.[18] Because the CFAA is primarily a computer hacking statute, narrowing actionable access restrictions to only code-based restrictions would be in line with the CFAA's original purpose.[19] Further, imposing liability only for violations of code-based access restrictions would provide several public policy benefits, including heightened corporate cybersecurity measures and increased protection of consumer privacy.[20]

This Note begins with a discussion of the development and history of the CFAA in Part I.[21] Part II then examines the former circuit split in CFAA decisions, with a particular focus on the parties that filed suit and the access restrictions that were alleged to impose CFAA liability.[22] This is followed in Part III with a description and analysis of the Supreme Court's decision in *Van Buren*,[23] which adopted a narrow view of the CFAA and developed a "gates-up-or-down inquiry" in considering CFAA applicability.[24] Part IV examines the unanswered issue of enforceable access restrictions by reviewing decisions made by lower courts and arguments from amicus briefs and academic literature.[25] Part V argues that the Court should adopt an even narrower approach to the issue of enforceable access restrictions and limit

[16] *Facebook, Inc.*, 844 F.3d at 1069.

[17] WEC Carolina Energy Sols. LLC v. Miller, 687 F.3d 199, 201 (4th Cir. 2012).

[18] *See* discussion *infra* Part V.

[19] *See, e.g.*, Samuel Kane, *Available, Granted, Revoked: A New Framework for Assessing Unauthorized Access Under the Computer Fraud and Abuse Act,* 87 U. CHI. L. REV. 1437, 1445 (2020) (noting that "Congress was primarily concerned about the threat of computer hacking."); Melissa Anne Springer, *Social Media and Federal Prosecution: A Circuit Split on Cybercrime and the Interpretation of the Computer Fraud and Abuse Act*, 86 U. CIN. L. REV. 315, 319 (2018) ("Congress originally intended the CFAA to prosecute hackers' unauthorized access.").

[20] *See* discussion *infra* Section V.C.

[21] *See infra* Part I.

[22] *See infra* Part II.

[23] *See infra* Part III.

[24] Van Buren v. United States, 141 S. Ct. 1648, 1658–59 (2021).

[25] *See infra* Part IV.

them only to breaking technological or code-based barriers, rather than mere violations of contractual terms or formal requests.[26]

I. The History and Language of the Computer Fraud and Abuse Act

A. The Pre-CFAA Application of Traditional Law

Along with the widespread introduction of computer systems into various public settings in the 1980s came "hackers," individuals who "coopt[ed] computers for illegal ends."[27] Prior to the adoption of the CFAA, prosecutors attempted to impose criminal charges against hackers under traditional property crime theories.[28] Although the crimes of trespass and burglary—both based on the concept of entry into the property of another without permission—represented logical applications of criminal law to the new use of computers, they functionally did little to punish illegal computer misuse.[29] This is largely because trespass and burglary statutes that imposed liability only when a person physically entered onto the property of another would not apply to a hacker who did not *physically* enter the computer.[30]

Early attempts to apply federal theft laws to hacking violations were more successful but ultimately arrived at similarly problematic conclusions.[31] Although changing access privileges to a computer or taking digital information such as files or software from another person's computer logically aligns with the taking of that person's property,[32] difficulty arises with the impermanent nature of digital information; while one may obtain the property of another if they hack into another person's computer with a stolen password and download a copy of highly valuable

[26] *See infra* Part V.

[27] *Van Buren*, 141 S. Ct. at 1652.

[28] Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1605 (2003).

[29] *Id.* at 1606.

[30] *Id.* at 1607 (noting that "it appears that no criminal prosecution has ever used burglary or general criminal trespass statutes to prosecute computer misuse.").

[31] *Id.* at 1608–10.

[32] *See id.*

software, the copying of such software does not necessarily deprive the original owner of its own copy of the software and consequently might not meet the definition of a traditional theft statute.[33]

B. Enactment of the CFAA and Subsequent Expansion

Following the increase in prosecution of computer-based crime in the 1970s and 1980s,[34] the difficult fit of federal and state-level property and theft schemes,[35] and calls for updated laws related to computer crime,[36] Congress passed the CFAA in 1986 as a criminal law that prevented unauthorized access to government computers.[37] Since that time, the CFAA has been substantially broadened in both application and scope.[38] In the early 1990s, Congress amended the CFAA to provide for civil causes of action and expanded computer activities covered by the CFAA.[39] The current form of the CFAA criminalizes and provides civil causes of action for various computer-related activities, including, *inter alia*, accessing federal government computers without authorization, trafficking passwords, engaging in computer-related extortion, and accessing a computer without authorization or in a manner that "exceeds authorized access"[40] in order to obtain information from any "protected computer."[41] The latter provision is the focus of this Note and the basis of the claim in *Van Buren*.[42]

[33] *Id.*

[34] Van Buren v. United States, 141 S. Ct. 1648, 1652 (2021).

[35] *See* Kerr, *supra* note 28, at 1608–10.

[36] *See id.* at 1613.

[37] The CFAA was initially introduced as an amendment to the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, which was subsequently amended in 1986 and became the Computer Fraud and Abuse Act of 1986. *Id.* at 1598 n.11; *see* Pub. L No. 98-743, 98 Stat. 2190–92 (1984) (codified as amended at 18 U.S.C. § 1030).

[38] *See Van Buren*, 141 S. Ct at 1652; *CFAA Background*, NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS, https://www.nacdl.org/Content/CFAABackground [https://perma.cc/NWR3-6QHY].

[39] In addition to these factors, amendments to the CFAA in the 1990s expanded the scope of the law to include not only governmental or banking computers but also those that connected to interstate commerce. *Van Buren*, 141 S. Ct. at 1652.

[40] *See* 18 U.S.C. § 1030(a)(1)–(7).

[41] *Id.* § 1030(a)(2)(C).

[42] *See generally Van Buren*, 141 S. Ct. 1648, 1652–53 (2021).

Although the terminology "protected computer" that appears in subsection 1030(a)(2)(C) initially centered on access to financial or government computers,[43] the current definition under the CFAA includes any computer "used in or affecting interstate or foreign commerce or communication,"[44] which the Supreme Court has noted expands relevant portions of the CFAA to cover "all information from all computers that connect to the Internet."[45] Given that a staggering number of devices are connected to the internet,[46] and that the number of devices grows by the billions each year,[47] the CFAA may affect an exponentially increasing number of users, employees, and corporations.[48]

II. SPLIT CIRCUITS

Prior to the Court's decision in *Van Buren*, the U.S. Circuit Courts of Appeals were split[49] on the application of the authorized access clauses of the CFAA.[50] Unfortunately, little in the Congressional record clarified the terms "without authorization" and "exceeds authorized access," leading to a split interpretation of

[43] *See id.* at 1652 ("Initially, subsection (a)(2)'s prohibition barred accessing only certain financial information.").

[44] 18 U.S.C. § 1030(e)(2)(B).

[45] *Van Buren*, 141 S. Ct. at 1652 (citing 18 U.S.C. § 1030(a)(2)(C), (e)(2)(B)).

[46] The estimated number of devices connected to the internet varies between sources but has far surpassed the human population as of 2014, at an estimated 10 billion. David Puglia, *Are Enterprises Ready for Billions of Devices to Join the Internet?*, WIRED, https://www.wired.com/insights/2014/12/enterprises-billions-of-devices-internet/ [https://perma.cc/GG24-3SRM].

[47] Much of the growth of internet-connected devices can be attributed to the growing network of physical objects that exchange data between each other and across systems over the internet, also known as the Internet of Things (IoT). *What is IoT?*, ORACLE, https://www.oracle.com/internet-of-things/what-is-iot/ [https://perma.cc/MAR3-HDMM]. Sources estimate that 127 new devices are connected to the internet every second. *The IoT Rundown for 2020: Stats, Risks, and Solutions*, SEC. TODAY (Jan. 13, 2020), https://securitytoday.com/Articles/2020/01/13/The-IoT-Rundown-for-2020.aspx?Page=2 [https://perma.cc/8Z42-GT3H].

[48] *See* 18 U.S.C. § 1030(a)(1)–(7).

[49] *Compare* United States v. Rodriguez, 628 F.3d 1258, 1260–63 (11th Cir. 2010), *with* United States v. Nosal, 676 F.3d 854, 856–64 (9th Cir. 2012).

[50] The pertinent portion of the CFAA reads: "(a) Whoever— . . . (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . (C) information from any protected computer." 18 U.S.C. § 1030(a)(2)(c).

18 U.S.C. § 1030(a)(2).[51] This split generally centered on the adoption of either a narrow or broad interpretation of the CFAA's "exceeds authorized access" clause.[52] The circuit courts that adopted a broad interpretation generally took the position that the "exceeds authorized access" clause included violations of both access restrictions (where the user was not granted access to a particular application, file, or database but attempted to access it regardless) and use restrictions (where the user was granted access to the particular application, file, or database for a particular purpose but then used it for an improper purpose).[53] Other circuit courts took a narrower approach and distinguished between the two, restricting CFAA claims to only violations of access restrictions.[54]

A. The Narrow View

In *United States v. Nosal*, the Ninth Circuit adopted a narrow interpretation of the CFAA and held that "exceed[ing] authorized access" under the CFAA was limited to access restrictions and did not include use restrictions.[55] There, the defendant worked for an executive search firm.[56] After the defendant left the company, he recruited former colleagues who still worked at the firm to help him start a competing company.[57] The defendant's colleagues used their log-in credentials to access

[51] Kane, *supra* note 19, at 1445 (noting that "both sides can summon congressional commentary supporting their respective approaches.").

[52] *Id.* at 1444; *see also* 18 U.S.C. § 1030(a)(2). *Compare Rodriguez*, 628 F.3d at 1260, *with Nosal*, 676 F.3d at 856–64. It should be noted that the Seventh Circuit adopted an even broader approach in *International Airport Centers, L.L.C. v. Citrin*, which, focusing on access restrictions more broadly, applied agency theory principles in determining whether an individual was authorized to access a computer system, and held that an employee who breached his duty of loyalty terminated his agency relationship and therefore terminated his authorization to access his laptop and was liable under the CFAA. 440 F.3d 418, 420–21 (7th Cir. 2006); *see* Kane, *supra* note 19, at 1449.

[53] *See* Kane, *supra* note 19, at 1445; *see, e.g.*, United States v. John, 597 F.3d 263, 272 (5th Cir. 2010).

[54] *See, e.g.*, *Nosal*, 676 F.3d at 863–64; LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1132 (9th Cir. 2009).

[55] *Nosal*, 676 F.3d at 864; *see* 18 U.S.C. § 1030(a)(2).

[56] *Nosal*, 676 F.3d at 856.

[57] *Id.*

their employer's database and transferred confidential information to the defendant.[58] The employees were still authorized to access the search firm's database but knew that a company policy prohibited the disclosure of confidential information.[59] The Ninth Circuit reversed the defendant's CFAA convictions, and noted that "[b]ecause 'protected computer' is defined as a computer affected by or involved in interstate commerce—effectively all computers with Internet access—the government's interpretation of 'exceeds authorized access' makes every violation of a private computer use policy a federal crime."[60]

The Ninth Circuit's opinion in *Nosal* built upon its similarly narrow view of the CFAA in *LVRC Holdings LLC v. Brekka.*[61] There, Brekka was an employee of LVRC Holdings LLC (LVRC) but also operated two other business ventures.[62] In the course of his work for LVRC, Brekka had an LVRC computer and email address but also routinely sent documents he created for LVRC to his personal email address.[63] There were neither employment agreements nor employee guidelines that would prohibit an LVRC employee from emailing documents to a personal computer.[64] Later that year, Brekka ceased working for LVRC and left the company.[65] However, a few months later, a different LVRC employee noticed that someone had accessed LVRC's accounts using Brekka's log-in information.[66] LVRC brought an action against Brekka, and alleged that he had violated the CFAA when he emailed LVRC documents to his personal account and when Brekka accessed the LVRC accounts after he had left the company.[67]

On review, the Ninth Circuit determined that Brekka had not accessed LVRC computers without authorization, as defined by subsection (a)(2) of the CFAA, when he sent himself personal e-mails.[68] This was because, according to the Ninth Circuit, accessing

[58] *Id.*

[59] *Id.*

[60] *Id.* at 859 (citing 18 U.S.C. § 1030(e)(2)(B)).

[61] *See id.*; LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1129 (9th Cir. 2009).

[62] *LVRC Holdings LLC*, 581 F.3d at 1129.

[63] *Id.*

[64] *Id.*

[65] *Id.* at 1130.

[66] *Id.*

[67] *Id.*

[68] *Id.* at 1133.

a computer "without authorization" would be to access a computer without any permission whatsoever, while "exceed[ing] authorized access" would be to access a computer with authorization but then use that authorization to access information that the person is not entitled to access.[69] Consequently, Brekka had authorization to access the computer when he sent the emails to himself—he was permitted and required to use the computer by his employer.[70] The court did note that if Brekka had, in fact, logged into the LVRC account after he had left the company, he would have accessed a computer without authorization under the CFAA,[71] but there was insufficient evidence to create a material issue of fact as to whether Brekka was the individual who had accessed the LVRC site using Brekka's old log-in information.[72]

The Second Circuit also adopted a narrow view of the CFAA, and held that a defendant did not violate the CFAA by merely using his authorized computer access for personal reasons.[73] There, the defendant was arrested on various theories of conspiracy to kidnap several individuals.[74] The defendant, a New York police officer, was also charged with a violation of section 1030(a)(2) of the CFAA for accessing a New York Police Department (NYPD) database to obtain sensitive information about individuals solely for personal use, in violation of NYPD rules that stated such databases were to be used only for an officer's official duties.[75] The Second Circuit found evidence that supported both narrow and broad interpretations of the CFAA,[76] but ultimately held that the defendant had not "exceeded authorized access" when he used the NYPD system for a personal purpose[77] and noted that a broad construction of the CFAA might result in excessive prosecution.[78]

[69] *Id.* (quoting 18 U.S.C. § 1030).

[70] *Id.*

[71] *Id.* at 1136.

[72] *Id.* at 1137.

[73] United States v. Valle, 807 F.3d 508, 511 (2d Cir. 2015).

[74] *Id.* at 512.

[75] *Id.* at 512–13.

[76] *Id.* at 511–12.

[77] *Id.* at 528.

[78] *Id.* (noting that "[w]hile the Government might promise that it would not prosecute an individual for checking Facebook at work, we . . . should not

B. The Broad View

In comparison to their sister courts, the Fifth, Seventh, and Eleventh Circuits adopted a broader view of the "exceeds authorized access" clause of the CFAA.[79] In *United States v. John,* the Fifth Circuit affirmed the conviction of a defendant under the CFAA for "exceeding authorized access" to a protected computer.[80] There, the defendant was an account manager at Citigroup, where she had access to her employer's internal computer system and account information.[81] The defendant used this access to print customer account information, which was then to be used by an accomplice to fraudulently charge those customers.[82]

Although the defendant suggested the adoption of a narrow interpretation of the CFAA and argued that she did not exceed authorized access by using her employer's computers to view and print account information to which she was allowed access in the course of her official duties, the court disagreed.[83] The court held that an individual may "exceed authorized access" for the purposes of the CFAA where an employer has authorized employees to "utilize computers for any lawful purpose but not for unlawful purposes and only in furtherance of the employer's business."[84] Consequently, the court affirmed the defendant's conviction because her access to customer account information was designated by her employer's official policy to be used only for business purposes, and thus the defendant's use for criminal purposes exceeded her authorization in violation of the CFAA.[85]

In *United States v. Rodriguez*, the Eleventh Circuit followed a similarly broad interpretation of the CFAA to that of the

uphold a highly problematic interpretation of a statute merely because the Government promises to use it responsibly.").

[79] *See* United States v. John, 597 F.3d 263, 273 (5th Cir. 2010); United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010); Int'l Airport Ctrs. L.L.C. v. Citrin, 440 F.3d 418, 420–21 (7th Cir. 2006).

[80] *John*, 597 F.3d at 269–70.

[81] *Id.* at 269.

[82] *Id.*

[83] *Id.*

[84] *Id.* at 271.

[85] *Id.* at 272; 18 U.S.C. § 1030(a)(2).

Fifth Circuit, and held that a defendant violated the CFAA when he accessed his employer's computerized information for nonbusiness reasons, even in the absence of a subsequently criminal use of such information.[86] There, the defendant worked for the Social Security Administration and, as part of his normal duties, had access to Administration databases that contained sensitive personal information.[87] At trial, the defendant admitted to using the Administration's databases seventeen times to obtain addresses and birthdates for nonbusiness reasons, in violation of a policy established by his employer, and was subsequently convicted of seventeen misdemeanor violations of the CFAA.[88] The Eleventh Circuit affirmed the defendant's conviction, and held that, for the purposes of the CFAA, an individual exceeds authorized access under subsection 1030(a)(2) when they abuse their access to an employer's information and then use that information for reasons that are not permitted by the employer's policy, regardless of whether the use was criminal in nature.[89]

III. RESOLVING THE SPLIT: *VAN BUREN*

A. Facts of the Case

On June 3, 2021, the Supreme Court finally resolved the circuit split and adopted a narrow interpretation of the "exceeds authorized access" terminology of the CFAA in *Van Buren v. United States*.[90] In *Van Buren*, defendant Nathan Van Buren was a Georgia police sergeant who befriended a man named Andrew Albo against warnings from the police department that Albo was "volatile."[91] Eventually, Van Buren asked Albo for a personal loan.[92] Albo covertly taped Van Buren's request and brought it to the local sheriff, where he alleged that Van Buren was attempting to "shake him down" for money.[93] The recording reached the Federal

[86] United States v. Rodriguez, 628 F.3d 1258, 1260 (11th Cir. 2010).

[87] *Id.* at 1260.

[88] *Id.*

[89] *Id.* at 1263–64.

[90] 141 S. Ct. 1648, 1652 (2021).

[91] *Id.* at 1653.

[92] *Id.*

[93] *Id.*

Bureau of Investigation (FBI), which decided to test Van Buren's monetary motivations.[94] The FBI told Albo to ask Van Buren to search for a license plate using a state law enforcement database through Van Buren's patrol car computer in exchange for money, which Van Buren did.[95] Van Buren had been trained by the police department not to use the database for personal reasons, and consequently knew that his search for Albo would be considered use of the police computer system for an "improper purpose" in violation of department policy.[96] Soon thereafter, Van Buren was convicted of a felony violation of the CFAA for "exceed[ing] [his] authorized access" to the police database.[97]

On appeal, the Eleventh Circuit applied its precedential broad interpretation of the CFAA, affirmed Van Buren's CFAA conviction, and held that Van Buren had exceeded his authorized access to the police computer in violation of the CFAA when he accessed the police database for an "inappropriate reason."[98] Acknowledging the circuit court split on the application of liability under the CFAA, the Supreme Court granted certiorari.[99]

B. The Court's Narrow Analysis

The Court began by noting that the CFAA primarily arose out of the growing public use of computers and an associated public interest in hacking-related crimes.[100] The Court then differentiated between two clauses of subsection (a)(2) of the CFAA.[101] Under the Court's interpretation, an individual violates the CFAA when he accesses a computer without authorization *or* "exceeds authorized access"[102] by accessing a computer that he is

[94] *Id.*

[95] *Id.*

[96] *Id.*

[97] *Id.*

[98] *Id.* at 1653–54 (quoting United States v. Van Buren, 940 F.3d 1192, 1208 (11th Cir. 2019)).

[99] *Id.* at 1654.

[100] *Id.* at 1652.

[101] *Id.* The pertinent portion of the CFAA reads: "(a) Whoever . . . (2) intentionally accesses a computer without authorization or exceeds authorized access . . . ." 18 U.S.C. § 1030(a)(2).

[102] *Van Buren*, 141 S. Ct. at 1654 (quoting 18 U.S.C. § 1030(e)(6)).

authorized to use and then obtains information that he is "not entitled so to obtain."[103] Noting that both Van Buren and the Government agreed that Van Buren had accessed his police computer with authorization by using his valid credentials on a department-issued database, the Court turned its inquiry to the second prong of the CFAA: exceeding authorized access.[104]

Reviewing the definition of "exceeds authorized access," the Court ultimately adopted Van Buren's interpretation of the clause.[105] Under Van Buren's view, an individual exceeds authorized access when he uses a computer that he is authorized to access in order to obtain information that he is restricted from accessing.[106] Under this definition, Van Buren had not exceeded his authorized access by using the law enforcement database to look up license plates;[107] rather, Van Buren had used his authorized access to log in to the system, and had obtained information that he was authorized to access, since he was not completely restricted from accessing license plate information in and of itself.[108]

Importantly, the Court created a basic framework for lower courts to apply when analyzing potential violations of the CFAA: the "gates-up-or-down inquiry."[109] Under 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."[110] The former refers to the "without authorized access" clause and the latter refers to the "exceeds authorized access" clause.[111] A user without authorized access has the external gates down—they cannot enter the system at all.[112] In contrast, a user who exceeds authorized access has the external gate up but an internal gate

[103] *Id.* (quoting 18 U.S.C. § 1030(a)(2), (e)(6)).

[104] *Id.*

[105] *Id.* at 1655. The CFAA defines "exceeds authorized access" as "to access a computer with authorization and to use such access to obtain . . . information in the computer that the accessor is not entitled so to obtain." 18 U.S.C. § 1030(e)(6).

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

[107] *See* 18 U.S.C. § 1030(a)(2)(c).

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

[109] *Id.* at 1658–59.

[110] *Id.*

[111] *Id.*

[112] *Id.*

down—they can enter the system but not access certain files within it.[113]

The Court's narrow view of the CFAA directly benefits general internet users,[114] as it clarifies that the CFAA imposes criminal or civil liability only where a user accesses a file or system to which they are explicitly restricted from accessing but not where the user merely accesses a computer in a way that is not directly in line with agreed upon terms of use.[115] This benefit also applies to security researchers, who may no longer fear litigation of CFAA violations for testing security vulnerabilities.[116]

However, the decision makes it unclear exactly when companies, service providers, or others will be able to enforce agreements that aim to limit a user's handling of authorized information;[117] without clarification from the Court, some circuits might limit CFAA enforcement to technological barriers to access, while others might allow CFAA causes of action based on contractual violations.[118]

IV. Room for Improvement

Although *Van Buren* solidifies the Supreme Court's narrow interpretation of the CFAA's "exceeds authorized access" provision,[119] the Court left unanswered questions about access limitations.[120] *Van Buren* held that a person "exceeds authorized access" to a computer in violation of the CFAA when they access that computer with authorization, but then access an off-limits file or other pieces of information.[121] Consequently, Van Buren did not violate the CFAA because he obtained information that he was authorized

[113] *See id.*; 18 U.S.C. § 1030(a)(2).

[114] *See Van Buren*, 141 S. Ct. at 1658–59.

[115] *See id.*

[116] *See* Aaron Mackey & Kurt Opsahl, *Van Buren is a Victory Against Overbroad Interpretations of the CFAA, and Protects Security Researchers*, Elec. Frontier Found. (June 3, 2021), https://www.eff.org/deeplinks/2021/06/van-buren-victory-against-overbroad-interpretations-cfaa-protects-security [https://perma.cc/2HKR-FAT3].

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

[118] *See id.*

[119] *Id.* at 1658–59.

[120] *Id.* at 1659 n.8.

[121] *See id.* at 1652.

to access, even though he used it for an improper purpose.[122] However, the Court did not specify exactly when files are considered off-limits to an otherwise authorized user.[123] In particular, the *Van Buren* Court noted that it "need not address whether this inquiry turns only on technological (or 'code-based') limitations on access, or instead also looks to limits contained in contracts or policies."[124] This leaves open the question of when and what kinds of contracts or policies are included as access restrictions, violations of which would impose CFAA liability.[125]

Circuit court decisions have answered this question in varying degrees of ambiguity.[126] In *Facebook, Inc. v. Power Ventures, Inc.*, the Ninth Circuit found a cease-and-desist letter sufficient to create an access restriction, a violation of which constituted a CFAA violation for unauthorized use.[127] There, Power Ventures, Inc. (Power) was a company that operated a social networking site that aggregated its users' information from other social media sites, including Facebook.[128] In an effort to draw traffic to its own site, Power solicited Facebook users to share a promotion intended to direct Facebook users to Power's platform.[129] Although Power had initially been granted access to Facebook's computers, the court noted that Facebook expressly rescinded that permission when it sent a cease-and-desist letter to Power.[130] Consequently, the court held that the cease-and-desist letter constituted an access restriction and that Power knowingly accessed Facebook's computers without authorization, in violation of the CFAA.[131]

In the absence of further direction from Congress or the Supreme Court, a corporation in the Ninth Circuit could potentially create an actionable CFAA claim under either prong of the

[122] *See id.*

[123] *See id.*

[124] *Id.* at 1659 n.8.

[125] *See id.*

[126] *See, e.g.*, Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1067 (9th Cir. 2016); WEC Carolina Energy Sols. LLC v. Miller, 687 F.3d 199, 204 (4th Cir. 2012).

[127] *Facebook, Inc.*, 844 F.3d at 1069.

[128] *Id.* at 1062.

[129] *Id.* at 1063.

[130] *Id.* at 1067.

[131] *Id.* at 1069.

CFAA based on a cease-and-desist letter.[132] Following *Facebook v. Power Ventures*, such communications clearly revoke access to the extent that a user's continued use of the defined computer service would be done "without authorization" and would violate the CFAA.[133] Applying the *Van Buren* gates-up-or-down inquiry, then, a cease-and-desist letter would put the outer gate down: the user in question could not access the computer system at all.[134] However, the same logic could be applied to the "exceeds authorized access" clause.[135] If a corporation sent a user a cease-and-desist letter that requested they discontinue use of a particular program or service but allowed them access to the computer system to use other programs or services, it would appear that the Ninth Circuit would consider that an equally viable access restriction,[136] violation of which would constitute "exceed[ing] authorized access"—the outer gate would be up, but an inner one would be down.[137] Consequently, courts following this line of reasoning would find triable issues of fact for CFAA violation claims even where the accessor has no password or other technological access limitations to overcome.[138]

Other courts have indicated a focus on a code-based approach in determining whether access was authorized.[139] In *WEC Energy Solutions LLC v. Miller*, the Fourth Circuit found that Miller did not violate the CFAA when he downloaded his employer's proprietary information, resigned, and then used such information in a presentation for a competitor.[140] Although the court's decision focused on the "without authorization" clause of the CFAA,[141] its holding was based on the fact that Miller had access to his employer's computer system and therefore had the technical ability

[132] *See generally id.* at 1062–63, 1069.

[133] *Id.* at 1069; 18 U.S.C. § 1030(a)(2).

[134] *See* Van Buren v. United States, 141 S. Ct. 1648, 1658–59 (2021).

[135] *See id.*; *Facebook, Inc.*, 844 F.3d at 1069.

[136] *See Van Buren*, 141 S. Ct. at 1658–59; *Facebook, Inc.*, 844 F.3d at 1069.

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

[138] *See Facebook, Inc.*, 844 F.3d at 1069.

[139] *See, e.g.*, WEC Carolina Energy Sols. LLC v. Miller, 687 F.3d 199, 205–06 (4th Cir. 2012).

[140] *See id.* at 201–02.

[141] *See id.* at 204.

to access the documents in the first place.[142] After noting that "[t]he CFAA is concerned with the unauthorized access of protected computers"[143] and that "access" is defined as "[t]o gain admission to,"[144] the court held that Miller did not violate the CFAA because he had technical access to his employer's computers.[145] The court then briefly noted that the exceeds "authorized access" clause was interpreted under similar definitions to that of the "without authorized access" clause,[146] and stated that an employee exceeds authorized access "when he gains admission to a computer without approval."[147] Following this analysis, then, it would appear that the *Miller* court would interpret not only the word "access" as the same in the context of both clauses of the CFAA but also access limitations (referred to as "approval");[148] if technical access to a computer, in general, was a determinative factor for the "without authorized access" clause, then, going one step further, technical access to a particular file within a system might be determinative of the "exceeds authorized access" clause.[149]

In the absence of clear guidance as to whether an individual accesses a computer system without authorization or exceeds their authorized access when violating an employment policy or if code-based access to a system is the determinative factor,[150] courts in different circuits might remain split on whether large corporations or service providers can pursue CFAA litigation where there were contractual or communicative obligations not to use a particular service or access a particular file, even where the user had otherwise authorized access and did not attempt to break through a technological barrier.[151]

[142] *See id.* at 207.

[143] *See id.* at 204.

[144] *Id.* (quoting *Oxford English Dictionary* (3d ed. 2011)).

[145] *Id.*

[146] *Id.*

[147] *See id.* (using the same dictionary definitions for terms in both clauses).

[148] *See id.*

[149] *See id.*; *see also* Patricia L. Bellia, *A Code-Based Approach to Unauthorized Access Under the Computer Fraud and Abuse Act*, 84 GEO. WASH. L. REV. 1442, 1457 (2016).

[150] *See supra* notes 126–49 and accompanying text.

[151] *See supra* Part II.

V. The Path Forward: Further Narrowing the CFAA to Cover Only Technological Access Limitations

The "exceeds authorized access" clause of the CFAA should be further narrowed and limited to violations of only technological or code-based access restrictions, rather than violations of restrictions contained in contracts or cease-and-desist orders.[152] This reading of the CFAA is in line with the Supreme Court's overall narrow view of the CFAA[153] and corresponds with the legislative intent of the CFAA as anti-hacking legislation.[154] Limiting CFAA violations in this way would also provide substantial public policy benefits by both incentivizing strengthened cybersecurity policies and protecting consumer data.[155]

A. Code-Based Access Restrictions Fall in Line with the Court's Analysis in Van Buren

As the Court noted in *Van Buren*, if "exceeds authorized access" imposed criminal liability under the CFAA to every person who violated a computer-use policy, millions of everyday computer users, such as employees who access their employer's computers for personal use against a computer-use policy or internet users who violate a website's terms of service would be considered criminals—an idea the Court correctly dismissed.[156] Despite finding violations of "computer-use" policies or "a website's terms of service" to be nonviolations of access restrictions under the CFAA,[157] the Court did not clarify which contractual agreements *would*.[158] So, under precedent such as *Facebook, Inc. v. Power Ventures, Inc.*,[159] courts within the Ninth Circuit, for example, would clearly not prosecute mere violations of end-user

[152] *See generally* Van Buren v. United States, 141 S. Ct. 1648, 1652–55 (2021).

[153] *See id.*

[154] *See, e.g.*, Kane, *supra* note 19, at 1445 (noting that "Congress was primarily concerned about the threat of computer hacking"); Springer, *supra* note 19, at 319 ("Congress originally intended the CFAA to prosecute hackers' unauthorized access").

[155] *See* discussion *infra* Section V.C.

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

[157] *Id.*

[158] *Id.* at 1659 n.8.

[159] *See* Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1069 (9th Cir. 2016).

agreements under the CFAA but might do so for users who received cease-and-desist emails or letters requesting that they no longer access particular areas or features of the platform.[160] To use the Court's gates analogy, then, in the Ninth Circuit, entering an otherwise raised gate would not be illegal if the person entering broke an agreement with the owner to not enter,[161] but it would be if there was merely a sign that read "[Specific Person] May Not Enter."[162]

Limiting the scope of the CFAA to code-based access restrictions would thus be more in line with the Court's gates-up gates-down approach; by limiting a user's access to particular resources on a computer or network using software, the gate is either up or it is down—a person either has digital access to the file (they enter the open gate) or they are digitally barred from accessing the file (the gate is down and they must break through it by somehow voiding their digital restriction).[163] If the gates remain open, and a user has the capability of accessing a particular file or service, a verbal or written promise or request not to access that file is about as effective at preventing misuse of that information as a "please only take one" sign above candy on Halloween is at preventing children from taking more than one; it is a constructive gate, at best.[164] If the gates remain closed and a user cannot access unless they break a technological barrier, the user will undeniably have greater difficulty accessing the file and the digital gate remains down, protecting the information within.[165]

B. Code-Based Access Restrictions Support the Legislative Intent of the CFAA

Further narrowing the CFAA to include only technological access limitations also aligns with the legislative intent of the

[160] *Compare id.* (finding a cease-and-desist letter to constitute a viable access restriction), *with Van Buren*, 141 S. Ct. at 1659 n.8 (declining to determine if violations of "*only* . . . technological (or 'code-based') limitations on access, or instead also . . . limits contained contracts or policies" trigger the "exceeds authorized access" clause of the CFAA); *see also* 18 U.S.C. § 1030.

[161] *See Van Buren*, 141 S. Ct. at 1658–59.

[162] *See id.*

[163] *See id.*

[164] *See id.*

[165] *Cf.* Brief of Professor Orin S. Kerr as Amicus Curiae in Support of Petitioner at 12–13, *Van Buren*, 141 S. Ct. 1648 (No. 19-783) [hereinafter Brief of Professor Orin S. Kerr].

CFAA in preventing computer hacking,[166] rather than merely preventing employees or end users from accessing certain files against a policy or agreement.[167] Although the legislative history of the CFAA has been criticized for failing to provide strong definitions of "without authorization" and "exceeds authorized access,"[168] both scholars and the Supreme Court itself agree that the original legislative intent of the CFAA was to curb computer hacking.[169] In fact, the Court clarified that the CFAA was designed primarily to affect digital transactions, and that only "one kind of entitlement to information counts: the right to access information by using a computer."[170] Conversely then, it would follow that one form of access limitation would count: denying the right to access information by using computerized means.[171] The overall analysis in the *Van Buren* decision appears to mirror this argument despite footnote eight's declination to define viable access limitations.[172] The Court consistently criticizes the effectivity of computer-use policies, implying that users commonly ignore policies both put in place by their employers and public websites more broadly.[173]

C. Code-Based Access Restrictions Are Beneficial to Public Policy

Limiting enforceable access restrictions to technological ones would also provide public policy benefits in two ways. First, by limiting enforceable access restrictions to technological or code-based ones, corporations would be incentivized to heighten their

[166] *See, e.g.*, Kane, *supra* note 19, at 1445.

[167] *See id.*

[168] *See id.*

[169] *See, e.g.*, *id.* (noting that "Congress was primarily concerned about the threat of computer hacking"); Springer, *supra* note 19, at 319 ("Congress originally intended the CFAA to prosecute hackers' unauthorized access"); *Van Buren*, 141 S. Ct. at 1652 ("After a series of highly publicized hackings captured the public's attention . . . . Congress passed the CFAA . . . .").

[170] *Id.* at 1656. The Court also noted that the CFAA is "concerned with what a person does on a computer; it does not excuse hacking into an electronic personnel file if the hacker could have walked down the hall to pick up a physical copy." *Id.*

[171] *See id.*

[172] *See generally id.* at 1652–56.

[173] *See id.* at 1661–62.

own cybersecurity measures.[174] If CFAA violations are only actionable where the user breaks through a code-based limitation, employers might be more likely to secure sensitive information on a user-by-user basis to ensure not only that the data will be secured, but also that they can file a cause of action if that data is taken.[175] This, in turn, would provide the additional benefit of protecting consumer data, especially in the absence of significant state or federal data privacy laws.[176]

However, if contract or policy-based access limitations or restrictions trigger CFAA violations, corporations might forego potentially costly steps to technologically limiting individual employees' access to sensitive files.[177] If the CFAA were interpreted as allowing contract-based access restrictions, then altering an employment agreement or handbook to disallow employees from accessing particular drives, for example, might prove a potentially cheaper option than blocking individual employees' access to that drive through software security measures.[178] While this might provide benefits to the employer insofar as they could keep costs low and recover damages against an employee for violating the policy,[179] it would do little to prevent a company insider from accessing and potentially leaking sensitive information in the first place.[180] This presents a potential danger for

[174] *See generally* Bradyn Fairclough, *Privacy Piracy: The Shortcomings of the United States' Data Privacy Regime and How to Fix It*, 42 J. CORP. L. 461, 463 (2016).

[175] *See generally id.*

[176] Although the Biden Administration has expressed interest in developing the nation's cybersecurity laws, current U.S. data privacy and cybersecurity laws remain piecemeal, and often vary state by state. *See* Exec. Order No. 14028, 86 Fed. Reg. 26,633 (May 12, 2021); Fairclough, *supra* note 174, at 463 ("The United States utilizes a 'sectoral model' to regulate how businesses use private, consumer information. A sectoral model utilizes legislation, regulation, and self-regulation.").

[177] Estimated costs of cybersecurity measures depend substantially upon the size of the company or entity, and the services it provides. A basic firewall, which filters internet network traffic, can cost between $1,500 and $15,000 per year; other important measures can raise this cost dramatically. *See How Much Does Cyber Security Cost? Common Cyber Security Expenses & Fees*, PROVEN DATA RECOVERY, https://www.provendatarecovery.com/blog/cyber-security-cost-expenses-fees/ [https://perma.cc/CFN9-MH6H].

[178] *See id.*

[179] *See* 18 U.S.C. § 1030(g).

[180] *See Insider Threat—Cyber*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/insider-threat-cyber [https://perma.cc/CHC4-MJLN]

the employee, the employer, and third parties who may be affected by the loss or sharing of data.[181]

Second, limiting the scope of the CFAA's "exceeds authorized access" clause would protect consumers by preventing a mere transfer of access restrictions from terms of use policies into more formal cease-and-desist letters or contracts.[182] In dismissing the applicability of terms-of-service agreements, the Supreme Court centered its argument on the content of the access limitations, rather than the form of such agreements;[183] instead of focusing on the fact that terms-of-service agreements are written agreements between the service provider and the end user, the Court implied that the ineffectiveness of such agreements stemmed from the user's lack of interest in their contents.[184] Signed employee handbooks might be considered in a similar vein.[185] However, without clarification from the Court, the ambiguity of enforceable access restrictions might create needless litigation between service providers or corporations and end users or employees over attempted access restrictions contained in cease-and-desist letters or specific contractual provisions.[186] For example, in an employment-employee relationship, where the vast majority of CFAA claims originate,[187] employers might merely move access restrictions from work policy documentation or presentations to employment contracts in order to enforce terms via the CFAA that would otherwise be unenforceable following the ruling in *Van Buren*.[188]

("The Department of Homeland Security National Cybersecurity and Communications Integration Center advises that 'insider threats, to include sabotage, theft, espionage, fraud, and competitive advantage are often carried out through abusing access rights, theft of materials, and mishandling physical devices.'"); *see also* Brief of Professor Orin S. Kerr, *supra* note 165, at 12–13.

[181] *See* Brief of Professor Orin S. Kerr, *supra* note 165, at 12–13.

[182] *See id.*

[183] *See Van Buren*, 141 S. Ct. 1661–62.

[184] *See id.*

[185] *See id.* at 1662.

[186] *See* Mackey & Opsahl, *supra* note 116 ("[L]eaving the question open means that we will have to litigate whether and under what circumstance a contract or written policy can amount to an access restriction in the years to come."); *cf.* hiQ Labs, Inc. v. LinkedIn Corp., 31 F.4th 1180, 1187 (9th Cir. 2022).

[187] Springer, *supra* note 19, at 315; Jonathan Mayer, *Cybercrime Litigation*, 164 U. PA. L. REV. 1453, 1480–81 (2016).

[188] *See* Springer, *supra* note 19, at 320; *see also* Brief of Professor Orin S. Kerr, *supra* note 165, at 12–13; *cf.* Mackey & Opsahl, *supra* note 116 ("Service

CONCLUSION

The Supreme Court's decision in *Van Buren* is a major step in clarifying federal cybersecurity laws and narrowing an overly broad statute that imposes civil and criminal penalties.[189] Not only does the decision resolve the previous circuit split on the scope of the CFAA, but it also precludes the prosecution of individuals for using software or files merely in a way that their employer or other entity does not want them to be used.[190] However, the Court chose not to delineate what kinds of access restrictions were enforceable under the CFAA. [191] As such, the CFAA might cover not only technological barriers, such as code-based prevention of the use or access of particular data, but also contractual terms, or other legal requests such as cease-and-desist letters.[192] Given that decisions from the Circuit Courts of Appeals apply different standards and considerations in determining which access restrictions are valid for purposes of CFAA liability, it is possible that individuals could be convicted or held civilly liable for violations of the CFAA in one state, but not another.[193]

It is also likely that, if violations of contracts or policies violate the CFAA, service providers or other large corporations or employers that provide information access to consumers or employees will use this vague definition of access restrictions to merely move access restrictions into employment contracts or send cease-and-desist letters to employees or end users who access files in an unwanted manner, rather than adopting a robust security system or specific access restrictions that would provide greater file security more broadly.[194] Thus, these entities would be able to pursue litigation against individuals who use data in a manner that conflicts with contracts, cease-and-desist letters, or other contractual limitations—a potentially slippery slope in an ever-digitally connected world.[195]

providers will likely argue that this is the sort of non-technical access restriction that was left unresolved by Van Buren.").

[189] *See Van Buren*, 141 S. Ct. 1648, 1652 (2021).

[190] *See id.*

[191] *Id.* at 1659 n.8.

[192] *Id.*

[193] *See id.*

[194] *See* discussion *supra* Section V.C.

[195] *See* discussion *supra* Section V.C.