Western New England Law Review

Volume 44 | Issue 1 Article 5

2022

SIGNS INSCRIBED ON A GATE: THE IMPACT OF VAN BUREN V. UNITED STATES ON CIVIL CLAIMS UNDER THE COMPUTER FRAUD AND ABUSE ACT

Scott T. Lashway

Matthew M.K. Stein

WESTERN NEW ENGLAND LAW REVIEW

Volume 44 2022 Symposium

SIGNS INSCRIBED ON A GATE: THE IMPACT OF *VAN BUREN V. UNITED STATES* ON CIVIL CLAIMS UNDER THE COMPUTER FRAUD AND ABUSE ACT

SCOTT T. LASHWAY & MATTHEW M.K. STEIN*

This Article addresses the impact of the U.S. Supreme Court's June 2021 decision in Van Buren v. United States *on what constitutes "authorization" to access a computer under the Federal Computer Fraud and Abuse Act (CFAA)—a law that imposes both criminal and private civil liability for violations—and concludes that, so far, the* Van Buren *decision has not rendered the CFAA toothless. The Introduction briefly explains the history of the CFAA, a summary of why it was enacted, how organizations have relied upon it as an important tool to protect themselves from computer hackers and increased cybersecurity risks, and a Circuit of Appeals split about what it means to "exceed authorization." The Article then, in a section titled "Exceeding Authorized Access: All That Is Not Permitted Is Forbidden," tells the sordid tale of what happened to Van Buren and how the U.S. Supreme Court resolved his case, ultimately by reversing the Court of Appeals's ruling affirming his CFAA conviction in an attempt to resolve the circuit split. It concludes in "Protecting Systems with a Sign on the Doorposts" by examining the two cases that, through December 2021, considered the authorization issue and what they indicate about the future of the post-*Van Buren *CFAA.*

INTRODUCTION

Enacted in the 1980s amid rising use of personal computers and

* Scott Lashway is the co-chair of Manatt, Phelps & Phillips, LLP's privacy and data security practice and managing partner of the firm's Boston office. Matthew Stein is a special counsel in that practice and office. They can be reached at slashway@manatt.com and mstein@manatt.com, respectively.

concerns about hacking,[1] the Computer Fraud and Abuse Act (CFAA) imposes criminal penalties on anyone who accesses protected computers without authorization or beyond what they are authorized to access.[2] Indeed, concerns about a "hacker mentality" and public indifference initially motivated Congress to act:

> [T]here is a tremendous attitudinal problem that gives the Committee some concern. People can relate to mugging a little old lady and taking her pocketbook, but the perception is that perhaps there is not something so wrong about taking information by use of a device called a computer even if it costs the economy millions now and potentially billions in the future.[3]

A private right of action was later added[4] to "boost the deterrence of the statute by allowing aggrieved individuals to obtain relief."[5] The CFAA has been amended eleven other times since its enactment.

Armed with a private right of action, companies historically used the CFAA to respond to incursions into their computing systems.[6] Even though civil CFAA claims require showing a loss of $5,000 or more related to the unauthorized access, in many situations that is a low threshold to meet, whereas other elements of the claim are easier to prove than what is required for a common-law trespass claim.[7] For example, to

1. *See, e.g.*, H.R. REP. NO. 98-894, at 8–12 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3691; S. REP. NO. 99-432, at 2–3 (1986), *reprinted in* U.S.C.C.A.N. 2479, 2484.

2. 18 U.S.C. § 1030. The Computer Fraud and Abuse Act (CFAA), as initially enacted, criminalized knowingly accessing computers to obtain financial records of financial institutions or information the United States determined must remain secret for national defense or foreign relations purposes or to use, modify, destroy, or disclose information in a United States government computer. Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, § 2102, 98 Stat. 1837. It was amended in 1986 to criminalize access with an intention to defraud and to change the criminalized conduct from "knowingly" accessing to "intentionally" accessing. Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, § 2, 100 Stat. 1213 (codified as amended at 18 U.S.C. § 1030). The latter change was made "to focus Federal criminal prosecutions on those whose conduct evinces a clear intent to enter, without proper authorization, computer files or data belonging to another." S. REP. NO. 99-432, at 6.

3. H.R. REP. NO. 98-894, at 12. "But the reason we were hoping it might not be made public is because it gives everyone else in town the same idea. They want to try it also to see if they can do the same thing someone else did." *Id.* at 11 (quoting Dr. Wilbur Miller).

4. Violent Crime Control and Law Enforcement Act of 1994, Pub. L. No. 103-322, § 290001, 108 Stat. 1796 (codified as amended at 18 U.S.C. § 1030(g)).

5. S. REP. NO. 101-544, at 6–7 (1990), *reprinted in* 1990 U.S.C.C.A.N. 1723, 1732.

6. Patricia L. Bellia, *Defending Cyberproperty*, 79 N.Y.U. L. REV. 2164, 2241 (2004) ("[N]etwork resource owners wishing to block unwanted uses of their systems have relied mainly on trespass-to-chattels and CFAA claims.").

7. Kyle W. Brenton, *Trade Secret Law and the Computer Fraud and Abuse Act: Two Problems and Two Solutions*, 2009 U. ILL. J.L. TECH. & POL'Y 429, 447 n.131.

make out a trespass claim, a plaintiff often has to plead that its ownership in the computer system was interfered with, or that it was temporarily dispossessed or deprived, or that the system's quality or value was impaired.[8] A CFAA claim does not require any of that. Instead, as commonly pled by companies, the CFAA requires a private plaintiff to plead that (1) the defendant accessed a protected computer without authorization, intentionally or knowingly with intent to defraud; (2) the defendant obtained information, obtained something of value, or caused damage; and (3) the plaintiff experienced a loss of at least $5,000 (loss here defined as a reasonable cost to the victim).[9]

Civil actions have brought "the development of a body of civil precedents interpreting the Act broadly"[10] and concerns about their impact on criminal CFAA proceedings.[11] It also led to a circuit split on whether access could be limited to certain purposes.[12] For example, in those circuits that rejected a purpose limitation on access under the CFAA, one arguably could access a protected computer for almost any reason with impunity under the CFAA if that person was authorized to access the protected computer.[13]

That circuit split has led to the potential for inequitable results for the same conduct. In 2019, the Ninth Circuit determined that a company that scraped data from a social networking website may not face civil liability,[14] while the Eleventh Circuit upheld a felony conviction and an

8. *See* RESTATEMENT (SECOND) OF TORTS §§ 217–18 (AM. L. INST. 1965) (listing the elements of trespass to chattel).

9. 18 U.S.C. §§ 1030(a)(2)(C), (a)(4), (a)(5)(B), (a)(5)(C), (c)(4)(A)(i)(I), (e)(8), (g). Even though the CFAA has the word "fraud" in its title, not all claims brought under it sound in fraud and require satisfying the heightened pleading standard for claims sounding in fraud. *See, e.g.,* NetApp, Inc. v. Nimble Storage, Inc., 41 F. Supp. 3d 816, 833–34 (N.D. Cal. 2014). In addition, CFAA civil claims can be predicated on other acts, such as transmitting malware to intentionally cause damage or transmitting threats to cause damage to a protected computer if done with the intention to extort something of value, or on other damages, such as a physical injury, modifying or impairing medical examination or treatment, or damaging a computer used by or for the United States for purposes of administering justice, defense, or national security. 18 U.S.C. §§ 1030(a)(5)(A), (a)(7)(A), (c)(4)(A)(i)(II), (c)(4)(A)(i)(III), (c)(4)(A)(i)(V); *see also* § 1030(a), (c)(4)(A)(i).

10. Brenton, *supra* note 7, at 429.

11. *E.g.*, Bellia, *supra* note 6, at 2258.

12. Van Buren v. United States, 141 S. Ct. 1648, 1653, 1653 n.2 (2021).

13. The exception may be if the person knowingly transmitted code or a command that damaged the protected computer because that provision of the CFAA does not turn on whether the access was authorized. 18 U.S.C. § 1030(a)(5)(A). The activity could also give rise to "other causes of action, such as copyright infringement, misappropriation, unjust enrichment, conversion, breach of contract, or breach of privacy." hiQ Labs, Inc. v. LinkedIn Corp. 938 F.3d 985, 1004 (9th Cir. 2009), *vacated*, 141 S. Ct. 2752 (2021). Discussion of those other claims is beyond the scope of this Article.

14. *hiQ Labs*, 938 F.3d at 1003–04. "Scraping involves extracting data from a website

eighteen-month prison sentence for a police officer who accessed a police database using his credentials merely because his reason for doing so was improper.[15]

That police officer was Sergeant Nathan Van Buren, and his conviction led to the Supreme Court's attempt to resolve the circuit split.[16]

I. EXCEEDING AUTHORIZED ACCESS: ALL THAT IS NOT PERMITTED IS FORBIDDEN

Van Buren was convicted by a jury in federal court for honest-services wire fraud and for violating the CFAA.[17]

His case began with a "friendly relationship" he developed with a widower, despite warnings from senior members of his police department to be careful in dealing with the widower.[18] Court opinions suggest the warnings were well founded. The widower "allegedly fancied younger women, including minors and prostitutes," he "allegedly paid prostitutes to spend time with him and then often accused the women of stealing the money he gave them," and he allegedly "surreptitiously recorded and harassed" "[a]t least one woman."[19] Van Buren "often handled the disputes between [the widower] and various women."[20] Based on that relationship, and facing financial difficulties, Van Buren asked the widower for a loan.[21] To the widower, things were different: the request was a "shak[e] down for his money," he told detectives, providing a recording of his conversations with Van Buren.[22]

After the recording and complaint made its way to the FBI, a plan was hatched. The widower "was to give Van Buren some cash, and in exchange, [he] was to ask Van Buren to tell him whether Carson, a woman he supposedly met at a strip club, was an undercover police officer."[23] The widower did so, couching it as a desire "to know . . . before he would pursue her further [romantically]. Van Buren agreed to help."[24] The two

and copying it into a structured format, allowing for data manipulation or analysis"; it is "typically done by a web robot or 'bot.'" *Id.* at 991 n.3.

15. *Van Buren*, 141 S. Ct. at 1653. The Supreme Court vacated the Ninth Circuit's decision in *hiQ Labs* for reconsideration in light of its decision in *Van Buren*. *See generally* hiQ Labs, Inc. v. LinkedIn Corp., 141 S. Ct. 2752 (2021).

16. *See generally* Van Buren v. United States, 141 S. Ct. 1648 (2021).

17. United States v. Van Buren, 940 F.3d 1192, 1198 (11th Cir. 2019), *rev'd*, 141 S. Ct. 1648 (2021).

18. *Van Buren*, 141 S. Ct. at 1653.

19. *Van Buren*, 940 F.3d at 1197.

20. *Id.*

21. *Id.*

22. *Id.* (quoting the widower's statement to law enforcement).

23. *Id.*

24. *Id.*

discussed Van Buren searching the police database for the woman's license plate, and he did—but for "a fake license plate number created by the FBI" and supplied by the widower.[25]

The FBI confronted Van Buren. He confessed to lying to the widower about why he asked for the money, he confessed to receiving money from the widower to run the plate search, and he confessed that "he knew doing so was 'wrong.'"[26] He was convicted.

On appeal, the Eleventh Circuit affirmed Van Buren's conviction for violating the CFAA, reasoning under circuit precedent that misuse, or use for an improper purpose, of a computer or database that the user is lawfully permitted to access can violate the CFAA: a purpose limitation.[27] To that court, authorization to access a computer can be for a limited purpose, and any purpose not permitted is forbidden and may even be the basis for a felony.

The Supreme Court granted certiorari, ultimately reversing the Eleventh Circuit. To the Court, authorization acted as a gatekeeping function, and individuals were either authorized to access a system or they were not.[28] The purpose in using the system was immaterial—there is no purpose limitation—and because Van Buren was authorized to access the database, he did not violate the CFAA.[29]

Along the way, the Court made three important observations. First, a purpose-based limitation criminalizes ordinary conduct, such as when "an employee . . . sends a personal e-mail or reads the news using her work computer" in contravention of her employer's policy that "computers and electronic devices can be used only for business purposes."[30] That would turn "millions of otherwise law-abiding citizens [into] criminals."[31]

Second, a purpose-based limitation can be arbitrary. The CFAA protects only against misuse of access and not against misuse of information obtained through that access.[32] Depending upon how a policy is written, the same conduct could be prohibited, but only one potentially criminalized under the CFAA.[33] That is because determining an individual's purpose in accessing a system requires understanding their

25. *Id.* at 1197–98.

26. *Id.* at 1198.

27. *See id.* at 1207–08. The Eleventh Circuit also vacated Van Buren's conviction for honest-services wire fraud, based on improper jury instructions. *See id.* at 1203–05.

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

29. *See id.* at 1662.

30. *Id.* at 1651, 1661.

31. *Id.*

32. *Id.* at 1662.

33. *Id.*

motive and intended use. Mere access, without more, is effectively testing access rights, which is inherent to giving access to a system.

Third, although the CFAA's authorization tests only a "gates-up-or-down inquiry," caring not why the authorization is used, the authorization need not be code-based.[34] Left open is if authorization can be granted, or limited, by a contract or policy, despite longstanding urging to require code-based authorization as the test for access rights under the CFAA.[35] Someone with the technical ability to access a system or a portion of a system may yet violate the CFAA if, say, a contract prohibits from them from doing so.

II. PROTECTING SYSTEMS WITH A SIGN ON THE DOORPOSTS

As Congress intended,[36] the CFAA has become an important tool in companies' arsenals to protect their information. And even though *Van Buren* answers some questions about the CFAA's scope, it leaves more critical questions unanswered that impact how companies use the CFAA in civil litigation. For example, must the gates be technical, or can the restrictions be based *solely* on a contract or policy? What happens if, because of a mistake, something that should have been behind a technical gate restricting access was not? And in that scenario, what if a contract, term of use, or policy forbade the access?

Two decisions following *Van Buren* show that the CFAA retains its importance and teeth, even with the purpose inquiry foreclosed: access may not be authorization, and authorization or its limits could be inferred from context and terms of use.

On the idea that having access may not mean having authorization: In *Bowen v. Porsche Cars, N.A., Inc.*, a motion to dismiss ruling, a court upheld claims that alleged automatic installation of a software update to a car infotainment system (which allegedly caused the infotainment system to malfunction and constantly reboot) violated the CFAA.[37] The software updates were transmitted to the car's satellite antenna, generally used to listen to satellite radio in the car, and related generally to the satellite radio functionality in the infotainment system.[38]

34. *Id.* at 1658–59, 1659 nn.8–9. Code-based authorization is a form of access control that relies upon someone's individual account credentials and account access privileges, which are among commonly used technical controls to protect information, or other technical information to determine if the person should be allowed to access information on a computer.

35. *See, e.g.*, Brief of Professor Orin S. Kerr as Amicus Curiae in Support of Petitioner at 7, Van Buren v. United States, 141 S. Ct. 1648 (2021) (No. 19-783), 2020 WL 4003433; Bellia, *supra* note 6, at 2253–58.

36. *See* S. REP. NO. 101-544, at 6–7 (1990), *reprinted in* 1990 U.S.C.C.A.N. 1723, 1732.

37. Bowen v. Porsche Cars, N.A., Inc., No. 21-CV-471-MHC, 2021 WL 4726586, at *1, *4–6 (N.D. Ga. Sept. 20, 2021).

38. *Id.* at *1.

But to the court, "nothing in the facts alleged implies that access to the antenna or consent to receive satellite radio transmissions is the same as an authorization to directly access, much less modify, the [infotainment system]," which is "a distinctly different device" from the satellite antenna and more than a mere satellite radio receiver.[39] So, the car manufacturer allegedly exceeded its authorization to access the infotainment system by causing the update to be installed.[40] Consistent with *Van Buren*, but not made under its framework,[41] this analysis breaks down a single system with a single authorization—a single computer system in the car to which access to connect was authorization—into components, each with its own potential authorization.

On the idea that limits to authorization could be inferred from context and terms of use: In *Vox Marketing Group v. Prodigy Promos*, a summary judgment decision, the plaintiff had made pricing proposals and packing lists available to its current and potential customers on the internet, behind a username/password gate.[42] Visits to the site, or to specific proposals or lists, required entering credentials.[43] But as the court relays, at some point the password protection was disabled for the pricing proposal and packing list URLs, making each accessible to anyone on the internet,[44] no password needed.

Later, a competitor received a copy of a pricing proposal, saw the proposal URL on the sheet, and discovered that the homepage of the site was protected by a username and password (which it did not have), but that the specific URL was not and it could download the pricing

39. *Id.* at *5.

40. The court's reasoning focuses on the vehicle owners' alleged lack of consent to installation of the update, and not whether the manufacturer was authorized to proceed in the manner it did. *Id.* at *4–5. It may be because the court was limited at the pleading stage and could not consider, for example, terms of use accompanying use of the infotainment system or satellite radio functionality in the car or whether the vehicle owner had taken affirmative steps to install the updates. *See id.* In doing so, the court distinguished similar cases about updates where the device owner or user had taken affirmative steps to download or install the updates. *Id.* at *4.

41. *See* Van Buren v. United States, 141 S. Ct. 1648, 1662 (2021) ("[A]n individual 'exceeds authorized access' when he accesses a computer with authorization but then obtains information located in particular areas of the computer—such as files, folders, or databases—that are off limits to him.").

42. Vox Mktg. Grp. v. Prodigy Promos, No. 18-CV-632, 2021 WL 3710130, at *1 (D. Utah Aug. 20, 2021).

43. *Id.*

44. *Id.* Although the issue did not arise in *Vox Marketing*, courts have held that cloud tenancies—virtual computers created on public cloud computing systems—can qualify for protection under the CFAA. *See, e.g.*, Allscripts Healthcare, LLC v. Andor Health, LLC, No. 21-704, 2021 WL 4425767, at *2–3 (D. Del. Sept. 27, 2021) (upholding CFAA claim brought by cloud tenant, but not by owner of the public cloud system).

proposal.[45] This competitor then discovered that because each URL for a proposal or packing list ended with a string of numbers, by changing the numbers, it could view multiple proposals and packing lists, allegedly accessing the site more than 20,000 times.[46]

The court concluded that these facts could demonstrate the competitor's accessing of those URLs was without authorization, even though they were not password protected: the competitor allegedly learned of the site and the URLs for pricing proposals and packing lists through unlawful conduct, knew the information was competitively sensitive, and knew the site itself had a password—yet it accessed the information anyway.[47]

Bowen and *Vox Marketing* make clear that having the ability to access may not mean having authorization, and that context can determine the scope and extent of authorization.[48] *Van Buren* and *Vox Marketing* leave unsaid, as courts often do, that the stakes for a CFAA violation are split between two extremes. There are high stakes: you could be convicted of a felony, as Van Buren himself learned, with jail time and significant collateral consequences.[49] On the other hand, the same provision could expose you to limited monetary liability in a civil suit.[50] *Bowen*, a civil suit, makes that point implicitly, distinguishing the criminal case in *Van Buren* with a wave of the hand: "Suffice it to say that the Supreme Court's decision that the police officer could use the law enforcement database to retrieve the license plate in question has no application to the issues before this Court."[51]

45. *Vox Mktg.*, 2021 WL 3710130, at *1–2.

46. *Id.* at *2.

47. *Id.* at *4–5.

48. This is not necessarily a slam dunk argument. Some courts have held, expressly or implicitly, that access *can be* authorization. *See, e.g.*, Castellano Cosmetic Surgery Ctr., P.A. v. Rashae Doyle, P.A., No. 21-CV-1088, 2021 WL 3188432, at *1–2, 10 (M.D. Fla. July 28, 2021) (finding that testimony that defendant had access to the system to download reports at issue foreclosed finding a likelihood of success on the merits on preliminary injunction, even though there was testimony that the defendant did not have authorization to access or download those particular reports and the system lacked the ability to provide tiered access); Speckman v. Fabrizio, 547 F. Supp. 3d 239, No. 21-CV-602, 2021 WL 2793053, at *5 (N.D.N.Y. July 6, 2021) (concluding that, under the CFAA, having credentials to change passwords means authorization to change the passwords).

49. Van Buren v. United States, 141 S. Ct. 1648, 1653 (2021).

50. *Compare* 18 U.S.C. § 1030(c)(1)(B) (setting forth a potential sentence of up to twenty years for violations of § 1030), *with id.* § 1030(g) (permitting individuals injured by violations of § 1030 to recover compensatory damages and injunctive relief in civil suits).

51. Bowen v. Porsche Cars, N.A., Inc., No. 21-CV-471, 2021 WL 4726586, at *1, *4 (N.D. Ga. Sept. 20, 2021). *Bowen* may do so because *Van Buren* focused on a different provision of the CFAA, *see id.* at *4, *4 n.3, or because both Van Buren and the government agreed that Van Buren was authorized to access the system and in *Bowen* that was disputed, *compare id.* at *4, *with id.* at *5. Whatever the reason, *Bowen* distinguishes *Van Buren* with a

To the *Vox Marketing* court, a mistake in a civil claim is not fatal: someone who uses a URL not behind a password wall can still violate the CFAA if the URL is *not intended* to be public and the person who accessed it discovered it through unlawful means. Indeed, that decision ratchets up the likelihood of a CFAA violation if the person knows the information at the URL is sensitive or confidential and that the site owner intended it to be behind a security wall of some kind.

In short, if "the information [a defendant] accessed exceed[s] what [the plaintiff] had previously authorized[,] *Van Buren*, in turn, does not legally bar [the] claim."[52] The CFAA still has teeth.

flourish.

52. Leitner v. Morsovillo, No. 21-CV-3075, 2021 WL 2669547, at *4 (W.D. Mo. June 29, 2021) (upholding post-*Van Buren* CFAA claim).