GATES OF COMPUTER TRESPASS

Angela L. Zhao[†]

ABSTRACT

While legal scholarship on the Computer Fraud and Abuse Act (CFAA) has scrutinized the meaning of its "authorized access" and "exceeds authorized access" provisions, none have weighed the impact of Van Buren v. US's explicit acceptance of the "narrow view"—a "gates-up-or-down" inquiry—and rejection of the "broad view" interpretation on computer trespass cases. This Note argues that the gates-up-or-down inquiry is inapt because the Court fails to define what are the gates. It proposes that the inquiry must include both code-based and user-authenticated based gates. This "double-door" approach resolves uncertainties in applying the test and curtails the overexpansion of prosecutorial power through the unauthorized access provisions over the past several decades. A legislative amendment to the CFAA must codify the double-door approach to prevent inconsistent interpretations of the narrow view among the lower courts.

I. INTRODUCTION

Known as an "infamously problematic" piece of legislature, the Computer Fraud and Abuse Act (CFAA) has been the subject of controversial caselaw, legal scholarship, and legislative reform since its inception in 1984.[1] While the CFAA was initially a federal statute meant to deter cybercrime and punish the archetypal computer hacker, it came to prosecute low-level violations and threatened the legality of everyday computer usage.

The Supreme Court case and the focus of this note, *Van Buren v. United States,* was an attempt to clarify and potentially narrow the meaning of a specific provision of the CFAA that criminalizes a computer user who "exceeds authorized access" to a computer. The holding states that a violation of the "exceeds authorized access" provision hinges upon whether one can or cannot access a computer or area within it. One must ask: are the gates up for the user so they can access a computer or area within it, or are they down so

DOI: https://doi.org/10.15779/Z38GT5FG8R

[†] J.D. 2023, University of California, Berkeley, School of Law. Sincere thanks to Professor Sonia Katyal, the 2021 Law & Technology Writing Workshop at Berkeley Law, and the Berkeley Technology Law Journal Editors.

[1] *Computer Fraud and Abuse Act Reform*, ELEC. FRONTIER FOUND. (last visited Dec. 8, 2021), https://www.eff.org/issues/cfaa [https://perma.cc/WJN6-3ZJV].

as to deny computer entry? The Court called this the "gates-up-or-down" inquiry.[2]

This Note is the first to raise concerns with *Van Buren's* "gates-up-or-down" inquiry and proposes a normative solution that clarifies the test. The inquiry rightly establishes the CFAA as a trespass statute, but leaves two crucial questions unresolved: what exactly is the "gate" and what constitutes an attempt to bypass it, so as to trigger liability? While legal scholars have constructed numerous interpretive paradigms of the "exceeds authorized access" provision that can help define what the "gates" are, this note explores their impotence after *Van Buren*.

Part II of this Note describes the CFAA and its legislative background. Part III looks at *Van Buren* and the problems the Court created in its attempt to clarify the "exceeds authorized access" provision. Part IV then advocates a normative argument that *Van Buren's* "gates-up-or-down" inquiry should have two gates instead of one to trigger a CFAA violation. Only the proposed "double-door" test is rigorous enough to apply the "gates-up-or-down" inquiry to past and future cybercrime cases. In doing so, the "double-door" test also reigns in the problematic overexpansion of the CFAA's prosecutorial domain since its inception almost 40 years ago.

II. BACKGROUND

A. HISTORY OF THE CFAA AND ITS OVEREXPANSION

The CFAA was enacted in 1984 and was once called "the most important piece of U.S. legislation used to combat computer crime."[3] The CFAA prohibits computer conduct by an individual acting "without authorization" or who "exceeds authorized access."[4] According to political lore, the statute originates from the release of the blockbuster movie *WarGames* in 1983. The movie tells the story of a high school student who mistakenly accesses the computer system containing the US nuclear arsenal, thinking it was a video game.[5] *WarGames* instilled fear into the minds of national policymakers about

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

[3] PETER G BERRIS, CYBERCRIME AND THE LAW: COMPUTER FRAUD AND ABUSE ACT (CFAA) AND THE 116TH CONGRESS 34 (2020). (citing Daniel Etcovich & Thyla Van Der Merwe, *Coming In From The Cold: A Safe Harbor From the CFAA and the DMCA § 1201 for Security Researchers,* BERKMAN KLEIN CTR. RSCH. PUBL'N NO. 2018-4 7 (2018).

[4] *Id.* at 4.

[5] Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARV. J.L. & TECH. 429, 492 (2012) ("There is some evidence that when the CFAA was originally enacted in 1984, it was partially in response to the situations depicted in the action film WarGames.").

the potential dangers of computer usage. According to one report, President Ronald Reagan watched it at Camp David and asked advisors if the movie could happen in real life.[6] Congress passed the CFAA soon after.[7]

As the main federal computer fraud statute, the CFAA imposes both civil and criminal liability on anyone who accesses a computer without authorization.[8] Originally, it was intended to criminalize computer hackers; the precursor bill that addressed "computer crime" suggests that the term was understood as "hacking" or "trespassing" into computers and data.[9] The CFAA was also meant to safeguard information only in financial institution and government computers. In 1994, Congress expanded the law to include a private civil cause of action, but the CFAA's scope remained narrow because the internet was not yet in commercial use.[10] But from then on, Congress's intent to expand the CFAA was clear: two years later it amended the language to replace financial institution and government computers with any "protected computer," significantly broadening the scope to virtually all computers connected to the internet.[11] Courts have reinforced the expansiveness of this amendment by defining "computer" to include smart appliances, fitness trackers, and other sensor-embedded devices that are connected to the internet—known as the "internet of things"—as well as web servers that manage website data.[12]

Gradually, federal prosecutors took advantage of the loosening scope of the CFAA. They diverged from prosecuting the archetypal cyber hacker who engaged in sophisticated digital trespass, and sought out less serious conduct such as password theft and mobile phone unlocking.[13] In a survey of every

[6] Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARV. J.L. & TECH 429, 492 (2012).("There is some evidence that when the CFAA was originally enacted in 1984, it was partially in response to the situations depicted in the action film WarGames."); *see also* Kevin Bankston, *How Sci-Fi Like 'WarGames' Led to Real Policy During the Reagan Administration,* NEW AMERICA (Oct. 11, 2018) https://www.newamerica.org/weekly/how-sci-fi-wargames-led-real-policy-during-reagan-administration/ [https://perma.cc/8343-JSQB].

[7] BERRIS, *supra* note 3 at 2.

[8] *Id.*

[9] Brief for Electronic Frontier Foundation, Center for Democracy & Technology & New America's Open Technology Institute as Amici Curiae Supporting Petitioner at 4, Van Buren v. United States, 141 S. Ct. 1648, 1658 (2021) (No. 19-783).

[10] *See* Edward R. McNicholas, Frances Faircloth & Shong Yin Yin, *(Un)Authorized Access to Computers in the Wake of Van Buren v. United States*, PLI CHRON.: INSIGHTS AND PERSPS. FOR THE LEGAL CMTY. 4, (2021); Berris, *supra* note 3, at 1.

[11] Patricia L Bellia, *A Code-Based Approach to Unauthorized Access Under the Computer Fraud Abuse Act,* 84 GEO. WASH. L. REV. 1442, 1463 (2016)).

[12] Berris, *supra* note 3, at 5.

[13] Jonathan Mayer, *Cybercrime Litigation*, 164 U. PA. L. REV. 1452, 1482–84 (2016).

CFAA case litigated, 29% of CFAA criminal cases were government computer system related, and over half of the defendants in those cases were government employees who had valid credentials but abused the system.[14] These cases frequently involved law enforcement personnel like officer Van Buren.[15] As these cases and the statistic shows, the focus shifted from prosecuting outside hackers to insiders who were not trespassing, but rather abusing their privileges.

The civil side has not fared better. The majority of civil cases involve routine commercial disputes between and within companies, and such litigation has turned civil cybercrime into a "quasi-intellectual property regime" more concerned about information than computer system integrity.[16] Congress, the courts, and criminal and civil litigants have all contributed to the overexpansion of the CFAA beyond its original aims.

B. 18 U.S.C. § 1030(A)(2): THE "EXCEEDS AUTHORIZED ACCESS" PROVISION

While the CFAA prohibits seven categories of computer conduct such as cyber espionage and password trafficking, the specific part at issue in *Van Buren* is the provision that covers 18 U.S.C. § 1030(a)(2).[17] This section imposes criminal and civil liability for anyone who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer."[18] The statute defines the term "exceeds authorized access" to mean "to access a computer *with authorization* and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."[19]

However, the statute fails to define "without authorization." In the context of computer access, "without authorization" can have numerous meanings. It could refer to forging one's authentication token, like stealing a password. Alternatively, it could refer to using a computer for improper means, like accessing a company database for personal use. The statute neither specifies

[14] *Id.* at 1485.

[15] *Id.* (stating that "remarkably" law enforcement was the most common class of defendant in cases where a government employee repurposed their access to a workplace computer system).

[16] *Id.* at 1482.

[17] The CFAA prohibits seven categories of conduct: Cyber Espionage 18 U.S.C. § 1030(a)(1), Obtaining Information by Unauthorized Computer Access § 1030(a)(2), Government Computer Trespassing § 1030(a)(3), Computer Fraud § 1030(a)(4), Damaging a Computer § 1030(a)(5), Password Trafficking § 1030(a)(6), and Threats and Extortion § 1030(a)(7).

[18] 18 U.S.C. § 1030(a)(2).

[19] *Id.* (emphasis added).

who determines authorization nor how authorization is determined, and thus leaves the "exceeds authorized access" provision undefined. Senate Reports filed with the amendment in 1986 suggest Congress intended that "without authorization" applied to outside hackers, while "exceeds authorized access" applied to insiders, like employees who are authorized to use a computer but who are prohibited from accessing specific areas and files within it.[20] Yet, courts have not accepted this evidence suggesting legislative intent, and have struggled to interpret the meaning of both "without authorization" and "exceeds authorized access."

C. CIRCUIT SPLIT IN § 1030(A)(2) INTERPRETATION

The courts have muddled the meaning of § 1030(a)(2) by adopting two competing paradigms of the "exceeds authorized access" provision, which ultimately overexpanded its scope. The difference between "without authorization" and "exceeds authorized access" has become "paper thin" and "elusive" in the courts.[21] This section summarizes the two competing paradigms, the narrow view and the broad view.

1. *The Narrow View*

The Second, Fourth, and Ninth Circuits have held that to exceed authorized access, a user must first enter a computer or program they have authorized access to and then cross a "technical barrier," such as a password prompt, to access a protected area within the computer.[22] This interpretation is known as the narrow view paradigm.[23]

For example, in *WEC Carolina Energy Solutions LLC v. Miller,* Miller, a former employee of WEC Carolina Energy Solutions (WEC), downloaded proprietary information from a company computer before resigning from his position.[24] Miller went on to work for a competitor and used the proprietary

[20] Berris, *supra* note 3, at 7.

[21] Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 420 (7th Cir. 2006).

[22] Aravind Swaminathan et al., *Prison Time for Personal Use of Company Computers? Supreme Court Grants Cert to Decide Whether Noncompliance With a Company's Terms of Use Constitutes a Violation of the Computer Fraud and Abuse Act*, ORRICK (May 5, 2020), https://www.orrick.com/en/Insights/2020/05/Prison-Time-for-Personal-Use-of-Company-Computers-Supreme-Court-Grants-Cert-to-Decide-Whether-Nonco [https://perma.cc/VR26-PB6H]; *see also* United States v. Valle*,* 807 F.3d 508, 511–513 (2d Cir. 2015); United States v. Nosal, 676 F.3d 854, 856–857, 863–864 (9th Cir. 2012) (en banc); WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199, 206 (4th Cir. 2012).

[23] Avi Weitzman, *Supreme Court to Resolve Longstanding Circuit Split Over Scope of Federal Anti-Hacking Statute*, GIBSON DUNN (Apr. 22, 2020), https://www.gibsondunn.com/supreme-court-to-resolve-longstanding-circuit-split-over-scope-of-federal-anti-hacking-statute/ [https://perma.cc/7VKU-F3S5].

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

information in a presentation to a competitor's customer.[25] Despite WEC's policies that limited unauthorized use of and personal downloading of proprietary information, the Fourth Circuit held that a user "exceeds authorized access" only when he has "approved access" to a computer, but uses his access to obtain information outside the bounds of his approved access.[26] Miller therefore did not violate the CFAA because he downloaded information he had employee access to, and had not circumvented any technical barrier.[27]

2. *The Broad View*

In contrast, the First, Fifth, Seventh, and Eleventh Circuits have adopted a more expansive understanding of the provision. In addition to prohibiting the circumvention of technical barriers, they have also defined "exceeds authorized access" as including violations of contract-based and purpose-based limitations on authorized access to computer information. [28] For example, "click-wrap" agreements, in which a website user assents to a website's terms and conditions by clicking a button that says "I agree," often set restrictions on the use of a website and its features.[29] Under the broad view, violating such use restrictions would "exceed authorized access" and therefore violate the CFAA. As another example, if an employee signs an agreement to only access work related websites and email on their work computer, but then proceeds to login to social media or browse Netflix, they would exceed their authorized access. This interpretation is known as the broad view paradigm.[30]

Contract-based limitations control what a user can and cannot access on a computer through the terms of a contract. For example, in *United States v. Rodriguez*, a Social Security Administration employee's job contract restricted him from using the agency's database for personal reasons.[31] Rodriguez looked up a person's home address and birthday for personal reasons, and was convicted of violating the CFAA by going against his employee contract.[32]

Purpose-based limitations control a user's access depending on the user's purpose for accessing the computer or information on the computer. An

[25] *Id.*

[26] *Id.* at 204.

[27] *Id.*

[28] Swaminathan, *supra* note 22.

[29] Bellia, *supra* note 11, at 1455–56.

[30] Report of the Brief for the Reporters Committee for Freedom of the Press et al. as Amici Curiae Supporting Petitioner at 11, Van Buren v. United States, 141 S. Ct. 1648, 1658 (2021) (July 8, 2020) (No. 19-783).

[31] United States v. Rodriguez, 628 F.3d 1258, 1260 (2010).

[32] *Id.*

example is *US v. Morris,* where Morris, a graduate student in computer science at Cornell University, created a "worm" in computer programs to exploit security vulnerabilities that allowed users to send and receive information across the internet.[33] While Morris argued that he had authorized access to the affected programs his "worm" exploited, the court held that Morris gained access without authorization because he did not use the programs "in any way related to their intended function." [34] Purpose-based restrictions can be contingent upon norms of use, like in *Morris*, or they can come from the computer owner's policies.

The broad view's capacious definition of "exceeds authorized access" became highly controversial. Critics of the broad view cite dissatisfactory outcomes when applied to cases. In *US v. Drew,* a woman named Lori Drew was charged with violating the CFAA after making a fake MySpace account to spy on her daughter's friends, violating MySpace's terms of service that required users to input accurate personal information.[35] Although the court correctly reasoned that the CFAA would become void for vagueness if it was read to cover MySpace's terms of service, *Drew* became a cautionary tale of the CFAA's overexpansive scope.[36] *Drew* incites a legitimate fear of government prosecutorial power under the CFAA: if the government can prosecute people who violate a website's terms and conditions, then the CFAA gives prosecutors a tool to criminalize nearly anyone they want.[37]

One of the most infamous computer crime cases, *U.S. v. Swartz,* spurred scathing critiques of the broad view among legal scholars and internet experts. Internet activist Aaron Swartz was indicted under the wire fraud statute and the CFAA after downloading millions of academic articles from JSTOR.[38] Under the broad view of the "exceeds authorized access" provision, Swartz did not have authorized access due to JSTOR's policy that limited the number of articles a user could download at any given time.[39] Swartz was a research fellow at Harvard who wanted to make the articles publicly available.[40] He

[33] United States v. Morris, 928 F.2d 504, 504 (2d Cir. 1991).

[34] *Id.* at 510.

[35] United States v. Drew, 259 F.R.D. 449, 452 (C.D. Cal 2009).

[36] *Id.*

[37] Brief of Professor Orin S. Kerr as Amicus Curiae in Support of Petitioner at 35, Van Buren v. United States 141 S. Ct. 1648 (No. 19-783) (stating that "The power to prosecute people for violating express restrictions on computers is a power to prosecute anyone the government thinks needs prosecuting").

[38] Indictment, United States v. Swartz, 2012 WL 4341933 at ¶ 0.

[39] *Id.* at ¶¶ 4, 15, 37.

[40] John Schwartz, *Internet Activist, a Creator of RSS, Is Dead at 26, Apparently a Suicide,* N.Y. TIMES (Jan. 12, 2013), https://www.nytimes.com/2013/01/13/technology/aaron-swartz-internet-activist-dies-at-26.html [https://perma.cc/3AE2-PARE].

travelled to MIT, accessed a school closet, and hardwired his laptop directly to the network to download articles; he continued to do so even after MIT blocked his IP and MAC addresses.[41] The FBI and the US Attorney's Office argued that Swartz "exceed[ed] authorized access" by acting with an unlawful purpose, even though he had legitimate access to JSTOR due to his position at Harvard.[42] Facing up to thirty-five years in prison and $1 million in fines, he committed suicide before his trial, galvanizing a demand for legislative reform to the CFAA.[43]

In 2013, a bill named "Aaron's Law" was introduced in Congress to codify the narrow view paradigm to prevent a repeat of the tragedy surrounding Swartz's death.[44] It sought to replace "exceeds authorized access" with "access without authorization," which was defined as obtaining information by "knowingly circumventing one or more technological or physical measures that are designed to exclude or prevent unauthorized individuals from obtaining that information."[45] Under the narrow view, Swartz would not have violated the CFAA since his research fellowship gave him the technological key to JSTOR's website. However, Aaron's Law failed to pass.[46] Courts therefore continued to reinforce the existing patchwork of interpretations, making the confusion around the statute's "exceeds authorized access" provision seem unresolvable.

An enduring criticism of the broad view is that intellectual property laws, as well as state laws and civil contract law, already set restrictions on computer usage, and can thus already deter bad actors.[47] For example, a website's terms and conditions page is a civil contract, and so contract law remedies are available when users violate its restrictions on website use.[48] In another example, 18 U.S.C. § 1832 (2012) is a criminal law that prohibits trade secret theft, including computer crime cases involving "insider" theft of confidential information. These laws are better equipped to handle computer users who violate purpose-based or contract-based restrictions than the CFAA, which was meant to deter sophisticated technical cyber hacking. Existing state and

[41] *Id.* at ¶ 17.

[42] *See id.* at ¶ 38–39 (charging that Swartz unlawfully obtained information from a protected computer in violation of the CFAA).

[43] Kaveh Waddell, *"Aaron's Law" Reintroduced as Lawmakers Wrestle Over Hacking Penalties*, ATLANTIC, (Apr. 21, 2015), https://perma.cc/274S-8Q82.

[44] AARON'S LAW ACT OF 2013, H.R. 2454, 113th Cong. (2013).

[45] *Id.*

[46] *Id.*

[47] *See* Annie Lee, *Algorithmic Auditing and Competition Under the CFAA: The Revocation Paradigm of Interpreting Access and Authorization*, 33 BERKELEY TECH L.J. 1307, 1340 (2018).

[48] Orin S Kerr, *Norms of Computer Trespass*, 116 COLUM. L. REV. 1143, 1170 (2016).

civil law deterrence mechanisms should play a larger role in shaping and ultimately limiting the scope of the CFAA.

3. *Cases Where Neither Paradigm Fits*

In some CFAA cases, courts failed to apply either the broad or narrow view paradigm when interpreting the "exceeds authorized access" provision, which made its meaning even more unclear. One such case, *U.S. v. Auernheimer,* involved a data breach that resulted in exposing 114,000 AT&T customer emails.[49] Andrew "Weev" Auernheimer wrote a script called the "iPad 3G Account Slurper" that enabled him to harvest email addresses of AT&T account holders who logged into AT&T's website with an iPad.[50] Each iPad had a unique SIM ID number that was automatically added to the end of the website URL, allowing a user's email to populate automatically on the login page. Auernheimer discovered that by using a script that automatically generated SIM ID numbers and then adding them to the end of the AT&T website URL, he could identify thousands of account holders' email addresses.[51] As a result of reporting the data breach and AT&T's website security vulnerabilities to the media, he was convicted of violating the CFAA and sentenced to forty-one months in prison.[52]

While the parties in *Auernheimer* argued different interpretations of the "exceeds authorized access" provision, the grand jury ultimately found Auernheimer guilty of violating the CFAA.[53] The government argued that Auernheimer violated the provision because he trespassed through the AT&T login portal; the portal acted like a front door to a house, even if it was unlocked and anyone could push it open by typing in URL strings.[54] Auernheimer unsuccessfully argued that the information was publicly available online, and was not a trespass.[55] Here, Auernheimer's unlawful trespass does not fit neatly into either the narrow or broad view paradigm of the CFAA. Auernheimer did not violate the narrow view paradigm, because typing a URL string does not break through a code-based barrier. Yet, neither did he violate the broad view paradigm, because a URL is not a contract or purpose-based

[49] United States v. Auernheimer, 748 F.3d 525, 531 (3d Cir. 2014).

[50] *Id.* at 530–31.

[51] *Id.* at 530.

[52] *Id.* at 532.

[53] *Id.*

[54] Brief for Appellee at 34, *Auernheimer*, 748 F.3d 525 (No. 13-1816), 2013 WL 5427839.

[55] *See* U.S. v. Auernheimer, 2012 WL 5389142 at *6 (D.N.J.,2012) (denying defendant's argument that he had a First Amendment right to transmit publicly available information and serve the public by exposing AT&T's nonexistent security system).

limitation of a website's use. *Auernheimer* exemplifies a growing pool of circumstances where the digital boundaries of authorized computer access are unclear, to the point that neither the narrow nor broad view of "authorized access" applies.

The need to demarcate the boundaries of "exceeding authorized access" became more dire as more opinions vacillated between the broad and narrow view. Criminal and civil litigants exploited this uncertainty for decades, ultimately expanding the CFAA's scope to criminalize people who were far removed and less culpable than the archetypal cyber hacker.[56] Due to the broad view paradigm in particular, the courts had created a "legal minefield" for many types of computer users such as ethical hackers, researchers, and journalists, as well as the average employee who browsed YouTube from a corporate computer.[57]

D. Previous Scholarship on Paradigms of CFAA Interpretation

Due to the dangers of the broad view, legal scholars have advocated for narrowing the meaning of the "exceeds authorized access" provision, with many advocating for their own, even more granular meanings of the narrow view paradigm. For example, Professor Patricia Bellia at the University of Notre Dame Law School has argued that the courts have exercised a more nuanced set of five interpretive paradigms rather than two, and further argues that the best paradigm is neither the broad nor narrow view, but one called the "code-based" paradigm.[58] This section compares the code-based paradigm and another leading framework, the "authentication-based" paradigm. Setting forth the foundational interpretive theories of the "exceeds authorized access provision" is crucial to understanding why an entirely novel interpretive paradigm is necessary in the wake of *Van Buren*.

1. *Code-Based Paradigm*

Numerous scholars have advocated for the code-based paradigm as a more precise definition of the narrow view. The code-based paradigm asks whether a user has "breach[ed] a code-based barrier to the system or to certain information on it." [59] Code-based specifically refers to computers or information on computers that are protected by access codes, like password portals, that are "designed to block the user from exceeding his privileges on

[56] *See* Mayer, *supra* note 13, at 1480.

[57] *See* Lee, *supra* note 47, at 1310.

[58] Bellia, *supra* note 11, at 1457 (concluding that the lower courts use four different approaches: agency, norms-of-access, policy, contract, and code-based paradigms).

[59] Bellia, *supra* note 11, at 1457.

the network."[60] Professor Orin Kerr at UC Berkeley School of Law, an expert in computer crime law, was an initial advocate for this paradigm. However, he has since rejected the code-based approach, arguing that the "code-based" formulation is vague.[61] Even so, the approach's focus on technical barriers in computers is important because the most severe types of cybercrime achieve unauthorized access using technically sophisticated techniques to bypass barriers.

2. *Authentication-Based Paradigm*

Professor Kerr has argued that authentication, or requiring verification that the user is the one who has access rights to the information accessed, is the "most desirable basis" for defining computer trespass under the CFAA.[62] He distinguishes code-based access from authorization-based access, arguing that the key point of authentication is "not that some code was circumvented, but rather that the computer owner conditioned access on authentication of the user and the access was outside the authentication."[63] Access that bypasses an authentication gate is unauthorized access.[64] What determines an authentication gate is "a matter of social understanding rather than technology," and often asks whether computer information is perceived to be publicly accessible or private.[65] "Virtual speed bumps" that make access more difficult, like hidden addresses and IP address blockers, should not affect authorized access, because the spaces these barriers attempt to conceal are considered open and public under the norms of the internet.[66] While no cases contain an explicit use of the term "authentication," courts often grapple with social norms surrounding computer use and must decide what constitutes computer access and trespass given the technological capabilities at any given time.

[60] Orin Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1644–46 (Nov. 2003).

[61] *Id.*

[62] Kerr, *supra* note 48, at 1147.

[63] *Id.* at 1164.

[64] *Id.*

[65] *Id.* at 1173.

[66] *Id.* at 1147, 1168 (arguing that an IP block is not a real barrier because users have multiple IP addresses due to having multiple devices, can often change their IP address, or shield it using a proxy server or Virtual Private Network).

III. *VAN BUREN V. UNITED STATES*

A. CASE SUMMARY

Police officer Nathan Van Buren received a bribe to run a license-plate check on a vehicle, from an acquaintance who suspected that an undercover officer owned the vehicle.[67] At the time, Van Buren did not know that the bribe was part of an Federal Bureau of Investigation undercover sting operation.[68] After running the license-plate check, Van Buren was arrested and convicted under the CFAA for "exceed[ing] authorized access" to the law enforcement database.[69] Trial evidence showed that Van Buren was trained to not use the database for an "improper purpose," which included personal use.[70] On appeal in the Eleventh Circuit, Van Buren argued that the "exceeds authorized access" clause only applied to those who obtain information that should have been inaccessible, not to the misuse of information that was accessible, as was in case.[71] The Eleventh Circuit affirmed the trial court's decision and held that Van Buren was not entitled to run a license-plate check in the police database for personal purposes.[72]

The Supreme Court granted certiorari to clarify the meaning of the "exceeds authorized access" provision of the CFAA. Reversing the Eleventh Circuit's ruling by a 6-3 decision, the Court held that the CFAA did not apply to Van Buren under a narrow reading of the statute.[73] Justice Barrett wrote the majority opinion, holding that under the narrow view, liability under the "unauthorized access" and "exceeds authorized access" provisions "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."[74] The opinion imports the same meaning into both the "without authorization" and "exceeds authorized access" clauses, though mainly references the latter given its central focus to the case.[75] The court rejected the broad view that "exceeds authorized access" meant using one's authorized access to information for an improper purpose.[76] The majority in *Van Buren* held that a

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

[68] *Id.*

[69] *Id.*

[70] *Id.*

[71] *Id.*

[72] *Id.* at 1653–54.

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

[74] *Id.* at 1658–59.

[75] *Id.* at 1658.

[76] *Id.*

CFAA violation only occurs when a user obtains information in areas of the computer that are "off limits to him."[77]

Justice Barrett focused on the literal meaning of the statute. She looked at the CFAA's definition of "exceeds authorized access" which refers to a user obtaining information "that the accessor is not entitled so to obtain."[78] Justice Barrett paid special attention to the word "so," describing it as "a term of reference that recalls 'the same manner as has been stated.'"[79] She further wrote the "manner as has been stated" is the manner of obtaining information through a computer that one is authorized to access.[80] Van Buren had access to the database as well as vehicle information within it, and thus the "gate" in the "gates-up-or-down" inquiry was lifted for him.

Paradoxically, even though the Court appears to adopt a narrow view, footnotes eight and nine call into question how to define the "gates" of the "gates-up-or-down" inquiry. Footnote eight states "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."[81] The Court avoids taking a concrete stance on whether the "gates-up-or-down" inquiry is based on technological restrictions like password portals, or restrictions based on contract and policy terms. [82] Meanwhile, the following footnote, footnote nine, suggests hinging authorization on "authentication," which refers to passwords or user credentials, drawing language from the Password Trafficking § 1030(a)(6) provision of the CFAA.[83]

Finally, Justice Barrett eliminates the broad view by arguing that it would criminalize "millions of otherwise law-abiding citizens," and extend to "trivial" computer use like "embellishing an online-dating profile" and "using a pseudonym on Facebook," directly rejecting the prosecution's argument in *Drew*.[84] In doing so, the Majority sides with legal scholars' significant critique of the broad view, and condemns the unfavorable outcomes of cases like *Swartz* that expanded prosecutorial discretion under the CFAA.

Justice Thomas wrote the dissent, which Chief Justice Roberts and Justice Alito joined. Justice Thomas argued that the CFAA should impose liability

[77] *Id.* at 1662.

[78] *Id.* at 1649.

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

[80] *Id.*

[81] See *id.* at n. 8.

[82] See *id.*

[83] See *id.* at n. 9.

[84] *Id.* at *1658*.

when a person uses information that they are entitled to access for an improper purpose, and that the majority's reading of the "exceeds authorized access" provision was too narrow.[85] Justice Thomas uses the analogy of a valet parking attendant: the attendant may have access to drive the car, but they would "exceed authorized access" if they took the car for a joy ride.[86] The dissent argued that authorized access should hinge upon whether a computer user exceeded the scope of the computer owner's consent.[87]

B. LEGAL COMMUNITY AFTER *VAN BUREN*

The legal community was generally receptive to *Van Buren* and its narrowing of the scope of the "exceeds authorized access" provision, because it resolved the decades-long circuit split while endorsing prevalent critiques of the broad view.[88] However, legal scholars and practitioners continue to debate the significance of footnote eight and attempt to reconcile it with the rest of the opinion. Professor Kerr argues that *Van Buren* establishes the CFAA as a trespass statute, while footnote eight leaves to the lower courts the "hard line-drawing" job of defining gates that can trigger liability.[89] In the wake of *Van Buren,* courts must now delineate between provider-imposed restrictions that are more like "speed bumps" and real barriers to access that are "gates" that can trigger CFAA liability.[90]

Practitioners advise employers that the gates of the "gates-up-or-down" inquiry are based on technical restrictions, but under footnote eight, they could also be based on policy or contract restrictions.[91] Because Van Buren only addressed purpose-based violations, and did not address violations of contractual and policy-based restrictions, employers can still pursue remedies in such cases.[92] This could be the focal point of future CFAA litigation of the "exceeds authorized access" provision.[93] Practitioners see *Van Buren* as a way

[85] *Van Buren,* 141 S. Ct. at 1657.

[86] *Id.* at 1662.

[87] *Id.* at 1663.

[88] Caroline Simons & Roland Chang, *Supreme Court Narrows Scope of the Computer Fraud and Abuse Act*, ORRICK TRADE SECRETS WATCH (July 22, 2021), https://blogs.orrick.com/trade-secrets-watch/2021/07/22/supreme-court-narrows-scope-of-the-computer-fraud-and-abuse-act/ [https://perma.cc/V8BK-2VJC].

[89] Orin Kerr, *The Supreme Court Reins in the CFAA in Van Buren*, LAWFARE (June 9, 2021), https://www.lawfareblog.com/supreme-court-reins-cfaa-van-buren [https://perma.cc/ECC3-E6S7].

[90] *Id.*

[91] Fisher Phillips News Podcast, *The Post-Van Buren Workplace and the Computer Fraud and Abuse Act, Part I*, FISHER PHILLIPS, (July 26, 2021), https://www.fisherphillips.com/news-insights/post-van-buren-workplace-computer-fraud-part-1.html.

[92] *Id.*

[93] *Id.*

to advise companies to review or add internal technological restrictions within computer systems, files, and databases to limit access to confidential information. [94] Companies should also review and refresh contracts and policies for employees regarding confidentiality, data security, and terms of use.[95] Ultimately, however, *Van Buren* was not the conclusive interpretation of the "exceeds authorized access" provision that the legal community hoped it would be, because of the potential for footnote eight to undermine the narrow view approach.

C. *VAN BUREN*'S CONTRIBUTION TO THE PROBLEM

While much concern exists about footnote eight's apparent contradiction of the Court's "gates-up-or-down" inquiry, legal scholarship has failed to recognize that the inquiry itself is impracticable because of its ambiguity. The Court's language in the opinion describes the "gates-up-or-down" inquiry as asking whether one "can or cannot access a computer system," and "can or cannot access certain areas within the system."[96] Furthermore, the Court stated that a user violates the CFAA when they enter areas of a computer that are "off limits," a vague rule that is impossible to apply.[97] The Court is unclear as to whether a user's status—for example, as an ex-employee or a recipient of a cease-and-desist letter—can bar them from accessing information, or whether a technological gate must exist to prevent them from entering.

Despite the seeming simplicity of a gates-up-or-down inquiry, fundamental questions arise when applied to real-world scenarios and caselaw: does the gate move up and down based on technology, and if so, does blocking a user's IP address close the gates of access to them, or are the gates a code-based restrictions like a password portal? Or in an entirely different interpretation, is the gate based on the user's identity, where it opens for current employees but closes for former ones? The opinion in *Van Buren* stops short of establishing a clear and useful "gates" test for courts to apply to CFAA claims.

In some cases, the gate is clear. For example, the court in *US v. Morris* partially adopted a code-based approach when it held that Morris violated the CFAA because a computer virus he made, known as the "worm," exploited vulnerabilities in the source code of various computers programs, known as "bug[s]," and guessed passwords.[98] The "worm" first infected a computer at MIT and then, at a much faster rate than he anticipated, spread to machines

[94] Fisher Phillips News Podcast, *supra* note 91.

[95] *Id.*

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

[97] *Id.* at 1662.

[98] United States v. Morris, 928 F.2d 504, 505–06 (2d Cir. 1991).

across the country at leading universities, military sites, and medical research facilities.[99] By exploiting vulnerabilities and guessing passwords, Morris circumvented technical gates that were down for him.

However, in many if not most other cases, the gate is harder to articulate. Recall *US v. Auernheimer*, where the defendant wrote a script to automatically display email addresses in AT&T's website login portal by manipulating the website's URL strings.[100] The iPad users' unique identifying number at the end of the URL and email addresses were confidential to AT&T, and therefore Auernheimer's access was unauthorized and violated the CFAA.[101] But applying the "gates-up-or-down" inquiry from *Van Buren* makes it unclear whether Auernheimer violated the CFAA. What the gate is and whether Auernheimer trespassed are difficult to articulate. Anyone can type in URL strings, and a code-based gate blocking access to the URL landing pages did not seem to exist. But an argument for a gate existing could be that AT&T intended the information to be confidential and did not intend for anyone but the account holder to see the auto-filled page. Yet, what the gate is in this scenario is still in question. *Auernheimer* becomes impossible to resolve under the Court's "gates-up-or-down" inquiry.

Footnotes eight and nine only exacerbate the test's ambiguity. Footnote eight's refusal to adopt a strictly technological-based gate may undermine *Van Buren's* holding. The dicta allows lower courts to look at contract and purpose-based restrictions as closed gates that trigger liability instead of "speed bumps" that would not.[102] Further, although footnote nine offers a potential interpretation of authorization as "user authentication," the opinion does not explicitly endorse this interpretation, and thus leaves the lower courts guessing as to whether user authentication is the proper test to apply.[103] The Court's reluctance to endorse a specific definition of the "gates" in the "gates-up-or-down" inquiry undermines the test's strength and exposes its underlying fragility.

Under the Courts' unclear holding, the lower courts could move the goalposts of the "gates-up-or-down" inquiry at whim to fit different interpretive paradigms in a manner as inconsistent as before *Van Buren.* And just as before, prosecutors and private actors will abuse the ambiguity of the "gates," threatening the legality of ordinary computer usage.

[99] *Id.* at 506.

[100] U.S. v. Auernheimer, 748 F.3d 525, 530–31 (2014).

[101] Superseding Indictment, U.S. v. Auernheimer, 748 F.3d 525, 530–31 (2014).

[102] *See* Kerr, *supra* note 48, at 1147 (describing types of systems of internet access known as "virtual speed bumps").

[103] *See Van Buren,* 141 S. Ct. at n.9.

An example of how the courts could shift the goalposts is in treating cease-and-desist letters as gates rather than speed-bumps. For example, in *Facebook v. Power Ventures,* Facebook sent a cease and desist letter to Power Ventures for accessing and using Facebook user accounts to send automated messages.[104] Power Ventures enabled social media users to view their accounts across numerous platforms in one place, by soliciting user data through automated scripts. [105] Users gave their consent to Power Ventures to access their Facebook accounts and send emails to Facebook friends to promote its platform.[106] The Ninth Circuit held that Facebook's cease and desist letter revoked Power Venture's access to the platform, using the analogy of a person wanting to borrow a friend's jewelry held in a bank safe deposit box.[107] If the bank did not allow the borrower onto its premises for any reason, then the person's access has been denied. The court held that Power Ventures acted "without authorization" in violation of the CFAA.[108]

Here, when applying the ambiguous "gates-up-or-down" inquiry from *Van Buren,* the gates could shift from technological barriers that prevent access, to cease-and-desist letters sent to specific undesirable users. Because the gates lack a clear definition, they grant the courts capacious interpretive grounds to modify the gates at the court's discretion.

The code-based and authentication-based paradigms can help define the "gates" in *Van Buren's* "gates-up-or-down" inquiry in part, but also create several problems. The following section evaluates the strengths and weaknesses of using the code-based paradigm and the authentication-based paradigm to define "gates." Part IV then lays out a normative solution to define the "gates" in a way that resolves weaknesses in both the paradigms and *Van Buren*'s narrow view holding.

D. PROBLEMS WITH APPLYING THE CODE-BASED PARADIGM TO *VAN BUREN*

The code-based paradigm could define the "gates" as code-based restrictions, like a password portal. However, the formulation of a "code-based" restriction is vague, and even more vague is what it means to breach a code-based barrier so as to trigger liability.[109] The most obvious breach is using sophisticated web tools and manipulating native code to surpass a code-based restriction. For example, any act that fits within the common conception of

[104] Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1062 (9th Cir. 2016).

[105] *Id.*

[106] *Id.* at 1065.

[107] *Id.* at 1068.

[108] *Id.* at 1069.

[109] *Kerr, supra* note 48 at 1164.

"hacking" to bypass a password portal will trigger liability if there is a code-based gate. But does an employee who shares a password with an ex-employee breach the code-based paradigm, and trigger liability? In other words, is password sharing a computer crime? The code-based paradigm was meant to extract a clearly defined rule of the narrow view interpretation of the "exceeds authorized access" provision. However, its vague formulation fails to establish a standard of what it means to breach a password portal, and essentially is an unproductive restatement of the narrow view of exceeds authorized access. A stricter standard of circumvention is needed.

Secondly, defining the "gates" under the code-based paradigm is ineffective at protecting ethical hackers and bug bounty program participants. It would create a chilling effect on ethical, or "white-hat," hackers and cybersecurity researchers whose work often requires circumventing code-based barriers.[110] External computer and website users who report bugs and security vulnerabilities are essential to a company's network infrastructure, just like motorists who report potholes are to a city's road infrastructure.[111]

Participants in rewards programs for identifying software vulnerabilities, known as "bug bounty" programs, are especially vulnerable to committing CFAA violations if the "gates" are based on code barriers.[112] In a bug bounty program, companies offer rewards for computer users who can find loopholes in their website or software code. Companies such as Shopify, Mozilla, and Atlassian have contractual safe harbors for bug bounty participants, which a strictly code-based definition of "gates" in the "gates-up-or-down" inquiry would fail to consider.[113] For example, Mozilla promises that "as long as you comply with this policy, [w]e consider your security research to be 'authorized' under the Computer Fraud and Abuse Act."[114]

[110] *See Computer Fraud and Abuse Act Hampers Security Research*, ELEC. FRONTIER FOUND., https://www.eff.org/document/cfaa-and-security-researchers [https://perma.cc/KQ85-GQ2G] (last visited Oct 4, 2021) (listing other examples of public interest computer hackers include car safety system hackers, electronic voting system security hackers, and medical device hackers who identify security flaws in implantable medical devices such as insulin pumps and pacemakers, which put patients' privacy and safety at risk); *see also* Mark A. Lemley et al., Brief of Technology Companies as Amici Curiae in Support of Petitioner at 4, Van Buren v. United States, 141 S. Ct. 1648 (2021) (No. 19-783) (July 8, 2020).

[111] *Id.* at 5.

[112] *See id.*

[113] *Id.* at 8.

[114] *Security Bug Bounty Program*, MOZILLA https://www.mozilla.org/en-US/security/bug-bounty/ [https://perma.cc/ND4X-J4H6] (last visited Dec 8, 2021).

Despite these contractual safe harbors, the risk for bug bounty participants and the larger ethical hacking community is still widely perceived.[115] While the Department of Justice's Computer Crime and Intellectual Property Section states that safe harbors for bug bounty programs will "substantially reduc[e] . . . the likelihood" of CFAA prosecution, prosecutors are not barred from pursuing cases against ethical hackers if they so desire.[116]

For example, a student at the University of Michigan faced an FBI investigation and potential CFAA charges for attempting to hack into an app, despite the app's participation in a bug bounty program.[117] As part of an election security course, the student identified security weaknesses in Voatz's app, an app that enables people overseas to vote in U.S. elections. Prosecutors argued that Voatz's bug bounty contract terms went into effect only after the student had hacked into the app, and that the student hacked into the "live election" part of the app, which was excluded from the bug bounty terms.[118] Yet Voatz only updated its terms to exclude the "live election" part after the investigation was underway.[119]

The prosecutorial discretion used to criminalize a legitimate bug bounty participant in *Voatz* is the latest part of a chronic history of CFAA abuses. From contract-protected hacking to trivial violations of contracts and policies, nearly any type of computer usage could become a target for the ever-expanding scope of the CFAA. Bug bounty programs highlight the importance of incorporating alternative measures such as user authentication into the "gates" in the "gates-up-or-down" inquiry, and show why the gates cannot be solely based on code restrictions.

E. PROBLEMS WITH THE AUTHENTICATION-BASED PARADIGM TO *VAN BUREN*

The "authentication-based" paradigm, alluded to in footnote nine and proposed by scholars such as Professor Kerr, is necessary to adopt, but must also resolve three main concerns. First, authentication should be more clearly

[115] *See* Brief of Technology Companies, *supra* note 111, at 10 (stating that the risk of criminal liability for security researchers is not a hypothetical threat, and that the government "can and will bring criminal cases based on a mere terms of service violation, even if the company didn't ask it to."

[116] *See* Brief of Technology Companies, *supra* note 111, at 11 (stating that "what companies think is ordinary testing behavior may well look like malicious hacking to a prosecutor unversed in computer security.").

[117] Kevin Collier, *FBI Investigating if Attempted 2018 Voting App Hack Was Linked to Michigan College Course*, CNN (Oct. 5, 2019) https://www.cnn.com/2019/10/04/politics/fbi-voting-app-hack-investigation/index.html [https://perma.cc/CV5S-26RE].

[118] *Id.*

[119] *Id.*

defined. Secondly, safeguards must be in place to prevent the paradigm from emboldening private actors to co-opt prosecutorial power and prosecutorial discretion. And relatedly, it must not be abused in a way that deputizes the CFAA to go after minor employment quarrels and intellectual property disputes unrelated to cybercrime.

The definition of authentication in an "authentication-based" restriction must be clarified. In footnote nine, the Court suggested that the "gates" adopt the CFAA password trafficking provision's definition of authorization as "'authentication,' which turns on whether a user's credentials allow him to proceed past a computer's access gate."[120] But neither the Court nor the password trafficking provision defines "user credentials," which could refer to a passcode, a job position, both at once, or something else altogether.

Additionally, recall Professor Kerr's definition of the authentication as "verifying that the user is the person who has the access rights to the information accessed."[121] The definition of "access rights" should have a clearer definition than "user credentials." Additionally, if the authentication gate becomes a "matter of social understanding rather than technology" as Professor Kerr suggests, changing norms about what constitutes authentication may incentivize liberal prosecutions under numerous interpretations of authentication and create mass confusion among the courts.[122] The result could be déjà vu of the CFAA's overexpansion from when prosecutors and broad view advocates attempted to expand the CFAA's unauthorized access provision to include violations of employment contracts and social media terms of use.

Secondly, an authentication-based definition of the "gates" in the "gates-up-or-down" inquiry could enable companies and civil litigants to confer and revoke user credentials on a whim, enabling them to bring CFAA claims at their discretion. Under an authentication-based paradigm, the computer owner has the sole power to raise and lower the gates of federal criminal liability depending on whether it verifies the user. This seems especially harsh given that civil penalties for contract and state law violations already provide adequate remedies for unverified computer usage. Additional safeguards to the authentication-based paradigm are necessary to protect computer users who violate contract and state laws from federal criminal liability under the CFAA.

For example, applying the authentication-based paradigm in instances where companies issue cease-and-desist letters to data scrapers or revoke

[120] *Van Buren,* 141 S. Ct. 1648, n.9 (2021).

[121] Kerr, *supra* note 48, at 1147.

[122] *Id.* at 1173.

access for ex-employees will empower private companies to weaponize the CFAA for their own private gain. If the recipient of a cease-and-desist letter ignores the letter, or the ex-employee continues to access the employer's computer, then they could face federal criminal charges under statute meant to deter sophisticated computer hacking. The CFAA already provides a private right of action, so formalizing the authentication paradigm can further explode these kinds of claims.[123] For example, in *Swartz*, the grand jury found that Aaron Swartz "exceeded authorized access" because he ignored JSTOR's numerous IP blocking protocols; the protocols indicated that JSTOR had revoked Swartz's authorization to use their service.[124] Handing to private companies the lever that opens and closes the "gates" that trigger a federal crime would create a significant chilling effect on employees and computer users.

An authentication-based approach taken alone will affirm and reinforce the deputization of the CFAA for corporate employment quarrels, which are far from the sophisticated cyber hacking the CFAA was meant to pursue. For example, in *Nosal II*, a former employee whose access to the company's database was revoked, borrowed a valid password from a current employee to access the database.[125] The court held that Nosal violated the CFAA because accessing a computer once one's access has been revoked constitutes unauthorized entry, and that the "unequivocal revocation of computer access closes both the front door and the back door."[126] Violating revoked access rules, like in *Nosal II,* should not have the same cause of action as computer hackers who use sophisticated technological skills to commit "breaking and entering" into computers. Further, other federal, state, and contract laws are sufficient to deter such bad inside actors. For example, 18 U.S.C. § 1832 is a criminal law that already prohibits the theft of trade secrets.[127] Escalating commercial intellectual property quarrels to the level of federal criminal liability is superfluous and reductive to Congress's goals for the CFAA.

[123] 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/U5DC-ZNWC].

[124] Indictment, United States v. Swartz, Defendant., 2012 WL 4341933 ¶ 38–39.

[125] United States v. Nosal, 844 F.3d 1024 (9th Cir. 2016*), cert. denied*, 138 S. Ct. 314 (2017).

[126] *Id.* at 1028.

[127] 18 U.S.C. § 1832.

IV. NORMATIVE SOLUTION

A. THE DOUBLE-DOOR INQUIRY

To narrow and clarify the Court's definitions of "without authorized access" and "exceeds authorized access, the "gates" in *Van Buren's* "gates-up-or-down" inquiry should consist of a code-based prong and an authentication-based prong. In reference to the two-part vestibule entryways found in colder climates, a "double-door" inquiry requires that a hacker first pass the code-based door, and then, pass the authentication-based door, to face CFAA liability.

For the first prong or "gate," a computer user must circumvent a clearly defined code-based barrier to fall within the CFAA's scope. A code-based barrier is one that protects information using one of the following: an alphanumeric passcode, a code-based identifier like an IP address or a web cookie, encryption token, or source code. Circumvention occurs when a person attempts to bypass a code-based barrier using technical tools or manipulating native code. It can involve trial-and-error password cracking known as a "brute force attack," in which hackers use automated systems to enter different passwords until one works.[128] Circumvention can also include decoding scrambled messages or possessing the translation "key" that can decode messages; these are tactics that fall under a coding technique known as decryption. Another common circumvention tactic is manipulating the source code of a computer program or website, either by inputting new malicious code or changing the code in vulnerable areas.[129]

This definition of "circumventing a code-based barrier" uses a heightened and stricter standard than that of previous scholarship. It narrows the definition to specific categories of computer code that can be circumvented, while requiring a heightened standard of "circumvention" or "manipulation" as opposed to mere entry through a coded gate. Ordering the doors by starting with the strict standard of circumvention to the broader standard of authorization, rather than the reverse, is the most effective structure to eliminate many cases from being improperly criminalized under a CFAA analysis. For example, access violations relating to trade secrets, or contract and use-based restrictions, like in *Van Buren,* will be tossed out at the first door under the heightened circumvention analysis.

[128] *What is a brute force attack?,* CLOUDFLARE, https://www.cloudflare.com/learning/bots/brute-force-attack/ [https://perma.cc/82QR-TJNW] (last visited Dec 8, 2021).

[129] Sharma9955, *5 Common Hacking Techniques Used by Hackers,* GEEKS FOR GEEKS (Feb. 19, 2020), https://www.geeksforgeeks.org/5-common-hacking-techniques-used-by-hackers/?ref=rp [https://perma.cc/RA35-FDV3].

Once the court determines a user circumvented a code-based restriction, the user may pass through the first set of doors and advance to the second set. Under the second set of doors, there is an "authentication-based" gate where the computer has the ability to verify users based on any aspect of their identity, which could include job position, age, relation to the user, or other means that the owner chooses. For example, the computer could recognize an employee based on their company-issued key fob, and grant them access. In this case, the second gate is "lifted" and no trespass or CFAA violation occurs. If the computer is unable to authenticate the user's identity, then the second gate is down for the user and they have committed trespass in violation of the CFAA.

B. Why the Double-Door Inquiry Resolves the Aforementioned Problems

1. *It resolves the problems with a strictly code-based approach.*

The double-door inquiry resolves the outstanding problems with a strictly code-based approach, because it weighs both the legitimacy of the user's technical actions and their identity, whereas the code-based paradigm only focuses on the former. Further, it clarifies the definition of a code-based gate as referring specifically to passcodes, code-based identifiers, encryption tokens, and source code. It eliminates the vagueness of the term as previous scholars have mentioned. The two-gates test sets forth a clearly defined technical gate and requires verification of a user's identity, narrowing the scope of the CFAA to filter out most user activity that violates existing law based on contracts, trade secrets, or other intellectual property issues.[130] This section evaluates its effectiveness when applied to trade secret disputes that have been wrongly criminalized under the CFAA, as well as addressing potential cases involving ethical hackers and bug bounty program participants.

First, the two-gates test is a solution to situations where a strictly code-based test could find CFAA liability for mere entry through, rather than circumvention or manipulation, of a code-based barrier. In the past, trade secret cases that companies pursued under the guise of the CFAA argued a code-based approach, especially where they revoked a computer user's access, but the user still acquired a password. For example, in *United States v. Rich,* a man paid an employee at Lending Tree to give him account access so he could

[130] *See* Kerr, *supra* note 48, at 1170 (arguing that civil contract law such as terms and conditions or terms of use on websites already set legal limits on how people can use websites); Lee, *supra* note 47, at 1340 (arguing that other laws already create a catch-all for computer crimes such as trade secret theft).

use the company's paid services.[131] And in *Nosal II,* an ex-employee borrowed valid credentials from a current employee to access the firm's database.[132] Under a code-based gate test, because the users crossed through the code-based gate of the password portal, they could be liable under the CFAA.[133] Such an outcome has the potential to escalate account password sharing to the level of a federal crime.

However, under the two-gates test, neither case would be a CFAA violation, because the first gate has a heightened standard for trespassing through a code-based barrier that requires circumvention or manipulation of the barrier. Because both actors in *Rich* and *Nosal II* obtained the proper passwords without manipulating the code or circumventing the portal by potentially attacking the source code, or intercepting a web cookie that stored the login information, they fail the first part of the inquiry. Without even broaching the second part about user authentication, no possible CFAA violation results. Contract law, state law, and trade secret law are sufficient avenues to pursue remedies, thus maintaining the limited scope of the CFAA.

Second, the double-door test protects bug bounty program participants and "white hat" hackers, whom companies protect through contract and policy terms. A common example is a hacker who finds errors in a program's source code, known as "bugs." These bugs can often make the system vulnerable to third party access and data breaches. Under the double-door paradigm, these hackers often circumvent technological barriers to protected information and therefore trespass through the first "gate," which triggers potential CFAA liability. Yet then under the paradigm, these white hackers then move on to the "authentication-based" gate of the test. Because contract and policy terms explicitly lift the gate for them, they do not trespass under a double-door inquiry and therefore do not violate the CFAA.

Adopting this test for ethical hackers and bug bounty programs incentivizes companies to create safe harbors for computer users who can identify and report security vulnerabilities. It strengthens network infrastructure overall and eliminates the chilling effect on security research due to the uncertainty of prosecution. Further, First Amendment protections are likely available even for those white hat hackers and algorithmic auditors who are not explicitly protected by contracts.[134] White hat hackers shed light on

[131] United States v. Rich, 610 F. App'x 334, 334 (4th Cir. 2015).

[132] United States v. Nosal, 844 F.3d 1024, 1024 (9th Cir. 2016*), cert. denied*, 138 S. Ct. 314 (2017).

[133] *See id.*

[134] Jacquellena Carrero, *Access Granted: A First Amendment Theory of Reform of the CFAA Access Provision*, 120 COLUM. L. REV. 131, 135 (2020).

vulnerabilities for the public interest, distinguishing them from unprotected hackers such as those who act for ransom or other commercial aims.

2. It resolves the problems with a strictly authentication-based approach.

The two-gates test resolves the problems with a solely authentication-based approach, which would dangerously overexpand criminally liable acts under the CFAA. For example, companies who issue cease-and-desist letters could pursue CFAA charges under an authentication-based paradigm, because revoking access to a website closes the authentication-based gate. However, under a two-gates test, alleged hackers must first trespass through a clearly defined code-based gate to be within the scope of a CFAA violation. Therefore, any cease-and-desist case in which computer users accessed publicly available information does not pass the first gate and is sealed off from triggering liability under the CFAA.

The manipulation of publicly available URL strings in *Auernheimer* is an example of where the two-gates test can eliminate confusion regarding whether a computer user "exceeds authorized access" under the CFAA.[135] Because Auernheimer did not circumvent any code-based restrictions, the gate was not down and he did not attempt to trespass through it.[136] *Auernheimer* would be sealed off from triggering liability under the CFAA.[137]

Similarly, in *HiQ Labs v. LinkedIn,* the defendants did not circumvent any code-based restrictions when they data scraped LinkedIn's web pages.[138] In that case, the company HiQ used an automated system to scan and collect data from across LinkedIn en masse, a technique known as data scraping.[139] Because LinkedIn's web pages were available to the public, HiQ would not have committed any form of code-based trespass.[140] Therefore, the case would be sealed off from a valid CFAA claim.

Requiring first a code-based gate and then an authentication-based gate ultimately eliminates the Court's ambiguity regarding whether violations of purpose or used-based restrictions found in contracts and policy can trigger CFAA liability. By requiring first that a computer user circumvent or manipulate a code-based restriction, and secondly that they lack authentication, the user has committed trespass through a "gates-down" situation. The double-door inquiry adequately narrows the "narrow view" of

[135] *See* U.S. v. Auernheimer, 748 F.3d 525 (2014).
[136] *See id.*
[137] *See id.*
[138] HiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985, 1004–05 (9th Cir. 2019)
[139] *See id.* at 1004.
[140] *See id.*

the CFAA to reign in the overexpansion of CFAA prosecution that criminalizes relatively trivial computer activity. It redirects the statute to fulfill its original purpose and best aligns with legislative intent.

C. IMPLEMENTING THE DOUBLE-DOOR INQUIRY

While the CFAA may have originally intended to criminalize acts of code-based or technological circumvention on computers, the everchanging landscape of technology and cybersecurity demand a wholly new interpretation of unauthorized computer access. Therefore, the gates must not only refer to code-based trespass, but must refer to user verification and authentication. This double-door inquiry with an updated and clearer definition of a code-based gate and an authentication gate is necessary to modernize the CFAA so that it keeps up with innovations in cyber hacking.

Two possible ways to implement this test exist: one is through the courts, the other through legislation. First, courts should adopt the two-part test I have proposed for interpreting the definition of authorized access in the CFAA.[141] However, we cannot leave the work of line-drawing entirely to the lower courts. Given that a CFAA case failed to reach Supreme Court for almost forty years despite the severity of inconsistent CFAA rulings in the lower courts, a legislative solution is necessary to prevent further criminalization of innocent computer users. Legislation should amend the CFAA to define "without authorization" as a two-gates test that involves both code-based access and also user authentication. The appendix of this note includes a legislative proposal to adopt the double-door inquiry into the statute.

V. CONCLUSION

The Supreme Court codified the narrow view of the CFAA's "exceeds authorized access" provision, in hopes of ending the decades-long interpretive juggling act among the lower courts. Yet, *Van Buren* failed to establish the clarity needed of the provision. While computer crime experts see the narrow view outcome as desirable because it puts officer Van Buren and other purpose-based cases out of the CFAA's scope, the Courts resulting "gates-up-or-down" inquiry has evaded important scrutiny. This Note is the first to challenge it for being too ambiguous and therefore impracticable. A normative solution to defining the "gates" of the "gates-up-or-down" inquiry is necessary

[141] Kerr, *supra* note 89 (arguing that *Van Buren* leaves the interstitial work of defining a "closed gate" to the lower courts).

to ensure effective, lasting reform of the CFAA's "exceeds authorized access" provision.

The "double-door" inquiry requires bypassing two gates instead of one to trigger a CFAA violation. The first gate asks whether a user has used sophisticated technical skills to circumvent a code-based restriction such as a password portal, while the second gate asks whether a user has authentication, meaning the owner has verified the user's access based on their identity or employment status. Only this "double-door" test of both a technology-based gate and an authentication-based gate is rigorous enough to apply the "gates-up-or-down" inquiry to past and future cybercrime cases, while also reigning in the overexpansion of the CFAA's prosecutorial domain. *Van Buren* was not the end to the interpretive woes of the CFAA's "exceeds authorized access" provision many hoped it would be. Rather, it began the Sisyphean challenge of combatting the most sophisticated technical computer hackers with a few ambiguously written words. The Computer Fraud and Abuse Act must evolve to narrow and clarify its language. Only then will its meaning have enough substance to deter and punish the real bad actors of the age of information.

VI. APPENDIX

18 U.S.C. §1030. Fraud and related activity in connection with computers

(a) Whoever—

  (2) Intentionally access a computer without authorization or exceeds authorized access, and thereby obtains—

    (C) Information from any protected computer; . . .

The term "without authorization" means to (1) manipulate or circumvent a code-based barrier to a computer or information on a computer and (2) lack authentication.

A code-based barrier is an account or information protected by one of the following: an alphanumeric passcode, a code-based identifier like an IP address or a web cookie, encryption token, or source code.

Authentication refers to when the computer owner has verified the user and thus granted authentication. The owner can verify the user based on any aspect of their identity, such as job position, age, relation to the user, or other means that the owner chooses.