SMU Science and Technology Law Review

Volume 25 | Number 1 Article 4

2022

Death of The Limited License to Data: *United States v. Van Buren*

Nick Curley
Southern Methodist University, Dedman School of Law

Death of The Limited License to Data: *United States v. Van Buren.*

*Nick Curley**

ABSTRACT

The United States Supreme Court has normally viewed data as property. Yet in *United States v. Van Buren*, the Court abandoned the property law angle. *Van Buren* included examination of the Computer Fraud and Abuse Act's applicability to a police officer who accepted a bribe from undercover agents to look up a phony license plate. The Court held that under the CFAA someone only "exceeds authorized access" when they properly access a computer and then improperly access files "that are off limits to [them]."

This Case Note explores why the Supreme Court should not have abandoned the property analogy to data. The Court is wrong because it has effectively destroyed the limited license to data. Further, the Court's analysis of the underlying technology leaves several questions unanswered for companies seeking to protect their data and employees looking to comply with the CFAA. For instance, users may have different levels of authorized access such as "Read" or "Write" permissions. But the Court merely approached data with an on/off false dichotomy. *Van Buren* ignores the nuance of data authority in the modern age.

I. INTRODUCTION

Congress passed the Computer Fraud and Abuse Act ("CFAA") in 1986—the year Nintendo published Metroid, Fujifilm introduced the disposable camera, and the new Compaq Portable II Computer weighed twenty-six pounds and cost close to $5,000.[1] In 1984, Congress passed the Counterfeit Access Device and Computer Fraud and Abuse Act and soon followed the Act with a 1986 amendment to § 1030 of Title 18 of the United States Code

DOI: https://doi.org/10.25172/smustlr.25.1.4

* Nick Curley is a 2022 candidate for a Juris Doctor from SMU Dedman School of Law. He received a Bachelor of Business Administration in Finance from the University of Oklahoma in 2019.

1. Nintendo of America (@NintendoAmerica), Twitter (Jul. 10, 2021 1:00 PM), https://twitter.com/nintendoamerica/status/1417544851135115267?lang=EN [https://perma.cc/7LRU-R66T]; *The First Century of the Disposable Camera, 1886-1986*, Disposable America, https://disposableamerica.org/ course-projects/della-keyser/the-first-century-of-the-disposable-camera-1886-1986 [https://perma.cc/K4XV-LMB8]; *Compaq Portable II Computer, 1986*, The Henry Ford Museum of American Innovation, https://www.thehenryford.org/collections-and-research/digital-collections/artifact/360371 [https://perma.cc/SFY6-MDWL].

which created the CFAA.[2] Today, the CFAA criminalizes any user who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer."[3] *United States v. Van Buren* clarified that where a user has authorized access to information—such as being given the proper login credentials—a user cannot "'exceed authorized access' to [a] database . . . even though he obtained information from the database for an improper purpose."[4] Under this holding, if IBM grants an employee authorized access to data for research, and that employee then sells that data to a third party, neither the government nor IBM can hold that employee accountable under the CFAA.[5] The CFAA provides a private cause of action, but the Supreme Court's new rule has slammed the door shut on the primary tool employers and prosecutors had to combat employee hacking.[6]

II. HISTORY OF SECTION 1030(A)(2)(C)

Section 1030(a)(2)(C) casts a massive net because it "potentially regulates every use of every computer in the United States and even many millions of computers abroad."[7] Tim Wu, a law professor at Columbia University who popularized the concept of "net neutrality,"[8] called the CFAA "the worst law in technology," citing its all-encompassing scope.[9] Before the release of Matthew Broderick's hit film, *WarGames*, "the hacking community itself was small, exclusive, and rather inconspicuous."[10] These were small groups where "[t]he sharing of information became one of the central tenets of hacker ethic."[11] After the enactment of the CFAA in 1986, "[p]erceptions of who and what hackers are underwent another transforma-

2. Justin Precht, *The Computer Fraud and Abuse Act or the Modern Criminal At Work: The Dangers of Facebook from Your Cubicle*, 82 U. CIN. L. REV. 359, 360 (2014).

3. 18 U.S.C. § 1030(a)(2)(C).

4. Van Buren v. United States, 141 S. Ct. 1648, 1662 (2021).

5. *See id.*

6. § 1030(g); *see Van Buren*, 141 S. Ct. at 1662.

7. Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1561 (2010).

8. *See Timothy Wu: Faculty Bio*, COLUMBIA LAW SCHOOL, law.columbia.edu/faculty/timothy-wu [https://perma.cc/9DCA-KUEV].

9. Tim Wu, *Fixing the Worst Law in Technology*, THE NEW YORKER (Mar. 18, 2013), https://www.newyorker.com/news/news-desk/fixing-the-worst-law-in-technology [https://perma.cc/GY4M-XYHD].

10. DOUGLAS THOMAS, HACKER CULTURE 26 (2002).

11. *Id.* at 19.

tion."[12] The "day the internet shut down, November 8, 1988," Robert Morris, a Cornell graduate in computer science, launched the internet worm, which was "a computer program that transmitted itself throughout the internet, eating up an increasing number of computing cycles as it continually reproduced itself."[13] Morris brought the internet to a halt, and "[t]he only remedy was to disconnect from the network and wait for experts" to fix the problem.[14]

In 1965, Gordon Moore, the director of research and development for Fairchild Semiconductors, extrapolated the data for the number of transistors that could fit on a chip and predicted the number of components on a chip would double every other year.[15] In 1995, Moore evaluated the data and surmised "[t]he current prediction is that this is not going to stop soon."[16] By 2022, Moore's law will have cycled eighteen times since the enactment of the CFAA, and during that time, the CFAA "has since expanded to cover any information from any computer" so that "the prohibition now applies—at a minimum—to all information from all computers that connect to the internet."[17] Other than this massive increase in scope, Congress has yet to meaningfully update the language of Section 1030(a)(2)(C) since its enactment in 1986.[18]

The rapid changes in technology over the last thirty-five years will pale in comparison to the changes that artificial intelligence will bring.[19] When George Moore gave his speech in 1995, the United States had 0.49 robots per thousand workers. By 2017, that number had grown to 1.79.[20] Legal scholars have contemplated whether robots using artificial intelligence that "exceed

12. *Id.* at 27.

13. *Id.* at 27-28.

14. *Id.* at 28.

15. *1965: "Moore's Law" Predicts the Future of Integrated Circuits*, Computer History Museum, https://www.computerhistory.org/siliconengine/moores-law-predicts-the-future-of-integrated-circuits/ [https://perma.cc/PP5D-PYNR].

16. Gordon E. Moore, *Lithography and the Future of Moore's Law*, 2439 SPIE 14 (May 22, 1995).

17. Van Buren v. United States, 141 S. Ct. 1648, 1652 (2021).

18. *See id.*

19. Asha Bharadwaj & Maximiliano A. Dvorkin, *The Rise of Automation: How Robots May Impact the U.S. Labor Market*, Federal Reserve Bank of St. Louis (July 10, 2019), https://www.stlouisfed.org/publications/regional-economist/second-quarter-2019/rise-automation-robots [https://perma.cc/7KVA-6E6R].

20. *Id.*

authorized access" could be subject to criminal laws.[21] Given these extraordinary advances in technology, Congress had no way of knowing how computers would change society, and just as the Supreme Court "has no free-floating power 'to rescue Congress from its drafting errors,'" ultimately, it should be up to Congress to modernize Section 1030(a)(2)(C).[22] The world is on the frontier of technological change, and artificial intelligence may well be the catalyst to another incredible period of development.[23]

In *Van Buren*, the Court confounded its issues over the scope of the CFAA with a fight over the definition of authorized access.[24] What should have been a simple application of property law to data ended up gutting a crucial piece of cybersecurity legislation.[25] Congress passed the CFAA in a world before smartphones and the impending societal upheaval from artificial intelligence.[26] The Court has consistently applied property law to data in computers, yet refused to do so here and instead supplanted property law with a new perspective on data.[27]

III. FACTUAL BACKGROUND

The CFAA has a history of yielding absurd results.[28] Using the CFAA, the Government prosecuted twenty-four year old Aaron Swartz, "an Internet prodigy who made significant contributions to [the internet] by the age of fourteen."[29] Allegedly, Swartz attempted "to download approximately 4.8 million articles from JSTOR, [a non-profit] digital library, using the MIT network."[30] To do this, "Swartz wrote a script that instructed his computer to download JSTOR articles continuously by "trick[ing] the JSTOR servers."[31]

21. *See* Gabriel Hallevy, *The Criminal Liability of Artificial Intelligence Entities - from Science Fiction to Legal Social Control*, 4 Akron Intell. Prop. J. 171, 191 (2010).

22. King v. Burwell, 576 U.S. 473, 514 (2015) (Scalia, J., dissenting) (quoting Lamie v. United States Trustee, 540 U.S. 526, 542 (2004)).

23. *See* Bharadwaj & Dvorkin, *supra* note 19.

24. *See* Van Buren v. United States, 141 S. Ct. 1648, 1661 (2021).

25. *See id.* at 1662.

26. Rob Smith, *IBM Created the World's First Smartphone 25 Years Ago*, World Econ. F. (Mar. 13, 2018), https://www.weforum.org/agenda/2018/03/remembering-first-smartphone-simon-ibm/ [https://perma.cc/LX9A-RQKR]; Bharadwaj & Dvorkin, *supra* note 19.

27. *See Van Buren*, 141S. Ct. at 1664 (Kagan, J., dissenting).

28. Mark Murfin, *Aaron's Law: Bringing Sensibility to the Computer Fraud and Abuse Act*, 38 S. Ill. U. L. J. 469, 469 (2014).

29. *Id.*

30. *CFAA Cases*, Nat'l Ass'n of Crim. Def. Laws. (Mar. 10, 2020), https://www.nacdl.org/Content/CFAACases [https://perma.cc/7H4L-3QNU].

31. *Id.*

"Under the weight of the prosecution" and potentially facing the maximum sentence under the CFAA—thirty-five years in prison—Swartz committed suicide.[32] In response, Representative Lofgren and Senator Wyden introduced Aaron's Law to specifically address "that mere breaches of terms of service, employment agreements, or contracts are not automatic violations of the CFAA."[33] However, Congress denied to adopt Aaron's Law in 2013 and again in 2015.[34] Despite congressional reluctance, the Court reasoned that "[i]f the 'exceeds authorized access' clause encompasses violations of circumstance-based access restrictions on employers' computers," like terms of service, then the CFAA would "criminalize everything from embellishing an online-dating profile to using a pseudonym on Facebook."[35] Swartz's tragic story is a demonstration of just how outdated the CFAA is and the necessity for Congress to update cybersecurity laws.

Computer fraud and abuse is an increasing threat for the private and public sector.[36] Cybercrime "could cost the private sector $5.2 trillion" between 2019 and 2024.[37] For example, hackers held the Colonial Pipeline for almost five million dollars in ransom.[38] During this disruption, the cost of gasoline skyrocketed in the southeastern United States and did incredible damage to the economy overall when deliveries, dependent on the oil from the pipeline, stopped.[39] The Federal Bureau of Investigation ("FBI") established the Internet Crime Complaint Center ("IC3") "to provide the public with a reliable and convenient reporting mechanism to submit information to the FBI" about cybercrimes.[40] In 2020, the IC3 received 791,790 complaints

32. *Id.*

33. Ron Wyden, *Summary of Aaron's Law* https://www.wyden.senate.gov/imo/media/doc/Aaron's%20Law%20Summary.pdf [https://perma.cc/778S-S69K].

34. Aaron's Law Act of 2015, H.R. 2454, 113th Cong. (as introduced by House, July 15, 2015); Aaron's Law Act of 2015, H.R. 1918, 114th Cong. (as introduced by House, May 15, 2015).

35. Van Buren v. United States, 141 S. Ct. 1648, 1661 (2021).

36. Allison Peters & Amy Jordan, *Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime*, THIRD WAY (Oct. 2, 2019), https://www.thirdway.org/report/countering-the-cyber-enforcement-gap-strengthening-global-capacity-on-cybercrime [https://perma.cc/JR62-GFT2].

37. *Id.*

38. Michael D. Shear et al., *Colonial Pipeline Paid Roughly $5 Million in Ransom to Hackers*, N.Y. TIMES (May 13, 2021), https://www.nytimes.com/2021/05/13/us/politics/biden-colonial-pipeline-ransomware.html [https://perma.cc/78QB-X5FS].

39. *See id.*

40. *2020 Internet Crime Report*, FEDERAL BUREAU OF INVESTIGATION INTERNET CRIME COMPLAINT CTR., https://www.ic3.gov /Media/ PDF/AnnualReport/2020IC3Report.pdf [https://perma.cc/URR6-EZD2].

representing over $4.1 billion in losses.[41] During the COVID-19 pandemic, 2020 reports to the IC3 increased by sixty-nine percent.[42] The FBI admits the data is likely incomplete because this data relies on self-reporting.[43] The rapid adoption of cloud storage will further exacerbate cybercrimes because Cloud Storage "has increased the volume, velocity, and/or variety in data being generated every minute around the world."[44]

IV. DISCUSSION OF CASE

In *Van Buren*, Officer Nathan Van Buren was the subject of an FBI sting operation following a report that Van Buren had asked the deputy chief of his department for a personal loan.[45] The FBI "devised an operation" for the deputy chief to ask Van Buren to search the state license plate database to ensure an imaginary woman the deputy chief met at a strip club was not an undercover cop.[46] In exchange, the deputy chief "would pay Van Buren around $5,000."[47] Notably, "Van Buren used his patrol-car computer to access the law enforcement database with his valid credentials."[48] Following this exchange, "[t]he Federal Government then charged Van Buren with a felony violation of the CFAA" because his use of the database "violated the 'exceeds authorized access' clause of 18 U.S.C. § 1030(a)(2)."[49] In the district court, a jury convicted Van Buren of violating the CFAA and "sentenced him to 18 months in prison."[50] The Eleventh Circuit "held that Van Buren had violated the CFAA by accessing the law enforcement database for an 'inappropriate reason.'"[51]

41. *Id.* at 3.

42. *Id.*

43. Peters & Jordan, *supra* note 36; Al Baker, *An 'Iceberg' of Unseen Crimes: Many Cyber Offenses Go Unreported*, N.Y. TIMES (Feb. 5, 2018), https://www.nytimes.com/2018/02/05/nyregion/cyber-crimes-unreported.html [https://perma.cc/8DVX-NLLT].

44. Ziyad R. Alashhab et. al., *Impact of Coronavirus Pandemic Crisis on Technologies and Cloud Computing Applications*, 19 J. OF ELEC. SCI. AND TECH. 1 (Mar. 2021).

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

46. *Id.*

47. *Id.*

48. *Id.*

49. *Id.*

50. *Id.*

51. *Van Buren*, 141 S. Ct. at 1653–54 (quoting United States v. Van Buren, 940 F.3d 1192, 1208 (2019)).

Before *Van Buren*, the circuits split as to the narrow and broad views of "exceeds authorized access."[52] The Court held "an individual 'exceeds authorized access' when he accesses a computer with authorization but then obtains information located in particular areas of the computer—such as files, folders, or databases—that are off limits to him."[53] The Court focused on the definition of "exceeds authorized access," which Congress statutorily defined as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter."[54] In an examination of the text, the Court defined "'[e]ntitle' [to mean] 'to give. . .a title, right, or claim to something.'"[55] While both parties agreed that Van Buren was "entitled to obtain" the phony license-plate information, the parties disagreed whether Van Buren was "entitled *so* to obtain."[56]

The Court focused on how the "[1] text, [2] context, and [3] structure" of the law all yield support to Van Buren's position.[57] Van Buren argued that the law "refers to information one is not allowed to obtain *by using a computer that he is authorized to access*."[58] The Court crafted an example of Van Buren's reading where if a person had access to Folder Y, he could not violate the CFAA by pulling information from Folder Y for a prohibited purpose, instead a violation of the CFAA would come from an employee accessing a prohibited Folder X.[59] On the other hand, the Government read the law "to refer to information one was not allowed to obtain *in the particular manner or circumstances in which he obtained it*."[60] The Court crafted an example of the Government's reading where an employee may access Folder Y for the purposes of work, but the pulling of the same information from Folder Y to give to a competitor would result in a violation of the CFAA

52. *Id.* at 1653; *Compare* Royal Truck & Trailer Sales & Serv., Inc. v. Kraft, 974 F.3d 756, 762 (6th Cir. 2020), *and* United States v. Valle, 807 F.3d 508, 526 (2d Cir. 2015), *and* WEC Carolina Energy Sol. v. Miller, 687 F.3d 199, 207 (4th Cir. 2012), *and* United States v. Nosal, 676 F.3d 854, 864 (9th Cir. 2012), *with* United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010), *and* United States v. John, 597 F.3d 263, 273 (5th Cir. 2010), *and* Int'l Airport Ctr. v. Citrin, 440 F.3d 418, 420-21 (7th Cir. 2006), *and* EF Cultural Travel BV v. Explorica, 274 F.3d 577, 581-82 (1st Cir. 2001).

53. *Van Buren*, 141 S. Ct. at 1662.

54. *Id.* at 1653; 18 U.S.C. § 1030(e)(6).

55. *Van Buren*, 141 S. Ct. at 1654 (quoting RANDOM HOUSE DICTIONARY OF THE ENGLISH LANGUAGE 649 (2d ed. 1987)).

56. *Id.*

57. *Id.* at 1661.

58. *Id.* at 1654.

59. *Id.*

60. *Id.*

because the employee had exceeded the limits of his authority to access Folder Y.[61]

The Court acknowledges that the Government's interpretation is facially attractive, but that its reading ignores the full definition of "so."[62] Van Buren reads "so" as "a term of reference that recalls 'the same manner as has been stated' or 'the way or manner described.' "[63] The Court pointed out that the Government's reading of the law "ignores the definition's further instruction that such manner or circumstance already will " 'ha[ve] been stated,' 'asserted,' or 'described.' "[64] The Court uses this definition of "so" to hold against the Government's reading because otherwise " 'so' captures *any* circumstance-based limit appearing *anywhere*."[65] Instead, the Court agrees with Van Buren that "so" "typically represents a 'word or phrase already employed, thereby avoiding the need for repetition."[66] Ultimately, the Court agreed with Van Buren that " 'is not entitled so to obtain' is best read to refer to information that a person is not entitled to obtain by using a computer that he is authorized to access."[67]

The Government countered that Van Buren's reading rendered "so" superfluous; "so" adds nothing if it only covers situations where someone obtains information through a computer they are authorized to use, and "so" should "incorporate[ ] all of the circumstances" which might limit authorization to information.[68] However, the Court proposed a hypothetical to prove that Van Buren's "so" was not superfluous.[69] An office worker could argue he was "entitled to obtain" restricted personnel files if he could have requested hard copies from human resources, even if he accessed those files that were off limits to him through his computer.[70] The Court pointed out that Van Buren's reading of "so" "forecloses that theory of defense."[71]

Separately, the Government countered that the ordinary meaning of the phrase "exceeds authorized access" aligns with its view of the law because "any ordinary speaker of the English Language would think that Van Buren

61. *Van Buren*, 141 S. Ct. at 1654–55.

62. *Id.* at 1655.

63. *Id.* at 1654.

64. *Id.* at 1655.

65. *Id.*

66. *Id.* (quoting OXFORD UNIV. PRESS, OXFORD ENGLISH DICTIONARY 887 (John Simpson & Edmund Weiner eds., 2d ed. 1989) (internal quotations omitted).

67. *Van Buren*, 141 S. Ct. at 1655.

68. *Id.* at 1656.

69. *Id.*

70. *Id.*

71. *Id.*

exceeded his authorized access."[72] The Court found this line of reasoning unpersuasive because of how the CFAA defined authorized access, and "that an 'appropriately informed' speaker of the language would" understand the CFAA's definition.[73] The Court reasoned that because "access" means to enter a computer system itself or data within that computer, then "exceeding authorized access" would mean accessing parts of that computer that the user lacked the privileges to access.[74]

The Court provided two structural arguments in support of Van Buren's position: (1) that Van Buren's reading treats clauses in the CFAA consistently and (2) the CFAA authorizes civil liability, and the damages the CFAA provides for are "aimed at preventing the typical consequences of hacking."[75]

The first structural issue revolves around two clauses in the CFAA, the "without authorization" clause and the "exceeds authorized access" clause.[76] Van Buren's interpretation of the statute is that the "without authorization" clause "protects computers themselves by targeting so-called outside hackers."[77] An outside hacker is the traditional idea of a hacker that is attempting to access files with no authorization.[78] Additionally, "Van Buren reads the 'exceeds authorized access clause' to provide complementary protection for certain information within computers" by "targeting so-called inside hackers."[79] Inside hackers are "those who access a computer with permission but then 'exceed'" the limits of their access "by entering an area of the computer" not covered by that authorization.[80]

The second structural issue involves the remedies provided for in the civil liability portion of the CFAA.[81] The CFAA defines "[d]amage" as "any impairment to the integrity or availability of data, a program, a system or information."[82] The Court pointed out the term "loss" in the CFAA also related "to costs caused by harm to computer data, programs, system, or information services."[83] The Court reasoned that Congress limited damages to technological harm because outside hackers typically cause "loss" as defined

72. *Id.* at 1657.

73. *Van Buren*, 141 S. Ct. at 1657.

74. *Id.* at 1657–58.

75. *Id.* at 1660 (quoting Royal Truck & Trailer Sales & Serv., Inc. v. Kraft, 974 F.3d 756, 760 (6th Cir. 2020)).

76. *Van Buren*, 141 S. Ct. at 1658 (discussing 18 U.S.C. § 1030(a)(2)).

77. *Id.*

78. *Id.*

79. *Id.*

80. *Id.*

81. *Id.* at 1659.

82. 18 U.S.C. § 1030(e)(8).

83. *Van Buren*, 141 S. Ct. at 1659–60 (discussing 18 U.S.C. § 1030(e)(11)).

by the CFAA.[84] Additionally, the Court cited Van Buren as illustrative; as an inside hacker, he caused no harm to the database.[85]

In a previous case, *Musacchio v. United States*, the Supreme Court "described § 1030(a)(2) as prohibiting '(1) obtaining access without authorization; and (2) obtaining access with authorization but then using that access improperly.' "[86] The Court dispensed with this precedent by declaring it dicta, and it reasoned that even if this quote is not dicta, using authorization to obtain otherwise prohibited information is still improper.[87] The Court also found that the statutory history of the CFAA supports Van Buren's reading because the previous version of the law, the 1984 Act, expressly alluded to the purpose of an insider's access, but Congress removed that language when it implemented the CFAA.[88]

The Court then examined the policy argument that "the Government's interpretation of the statute would attach criminal penalties to a breathtaking amount of commonplace computer activity" and compared it to the "extra icing on a cake already frosted."[89] The Court lamented the possibility that if the CFAA criminalizes every violation of a computer-use policy, "then millions of otherwise law-abiding citizens are criminals."[90] Lastly, the Court said "[t]he Government's approach would inject arbitrariness into the assessment of criminal liability" because while the "exceeds authorized access" clause is a prohibition against access and not use, "the line between the two can be thin."[91]

V. ANALYSIS

In *Van Buren*, the Court created an impermeable shield for system administrators against criminal and civil liability under the CFAA.[92] Justice Thomas, dissenting, rightly points out that "the majority's reading is at odds with basic principles of property law.[93] In the modern understanding of computers, "it is well established that information contained in a computer is 'property.' "[94] The majority relies on the illustration of "entering an area of

84. *Id.* at 1659–60.

85. *Id.* at 1660.

86. *Id.* (quoting Mussachio v. United States, 577 U.S. 237, 240 (2016)).

87. *Id.*

88. *Id.* at 1660.

89. *Van Buren*, 14 S. Ct. at 1661 (discussing Yates v. United States, 574 U.S. 528, 557 (2015) (Kagan, J. dissenting)).

90. *Id.* at 1661.

91. *Id.* at 1662.

92. *Id.* at 1662.

93. *Id.* at 1664 (Thomas, J., dissenting).

94. *Id.*

the computer" as the example of exceeding authority, and this illustration is misleading.[95] Describing data as being within areas of a computer completely ignores how cloud computing works.[96] "[C]loud computing is the delivery of computing services—including servers, storage, databases, networking, software, analytics, and intelligence—over the Internet."[97] In cloud computing, data is "hosted at a remote data center managed by a cloud services provider . . . [who] makes these resources available for a monthly subscription fee or bills [the customer] according to usage."[98]

The Court's simplified view of data does not capture the sophisticated way data is stored, like in block storage.[99] In block storage, "data is organized into large volumes called 'blocks.'. . . Cloud storage providers use blocks to split large amounts of data among multiple storage nodes."[100] Not only are these nodes not contained on "areas in the computer,"[101] but providers split up the files.[102]

The tiered nature of access in computers also render the Court's "gates-up-or-down" model of access inadequate.[103] "[P]ermissions are access details given by . . . network administrators that define access rights to files on a network."[104] Permissions for a file are often stratified into different rights like writing permissions, reading permissions, and execution permissions.[105] Further, administrators can "access all files on the computer, and make changes to other user accounts."[106] Where a system administrator appropriately de-

95. *Van Buren*, 141 S. Ct. at 1658; *see Permission*, COMPUTER HOPE (Dec. 30, 2019), https://www.computerhope.com/jargon/p/permissi.htm [https://perma.cc/6WJD-WD3E].

96. *What is Cloud Computing*, MICROSOFT, https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/ [https://perma.cc/NT6Y-R78X].

97. *Id.*

98. Sai Vennam, *Cloud Computing*, IBM (Aug. 18, 2020), https://www.ibm.com/cloud/learn/cloud-computing [https://perma.cc/W5B4-35BY].

99. *See Cloud Storage*, IBM (June 24, 2019), https://www.ibm.com/cloud/learn/cloud-storage [https://perma.cc/9JZT-385X].

100. *Id.*

101. Van Buren v. United States, 141 S. Ct. 1648, 1652 (2021).

102. *See Cloud Storage*, *supra* note 99.

103. *See* COMPUTER HOPE, *supra* note 95.

104. *Id.*

105. *Id.*

106. *How Do I Log On as an Administrator*, MICROSOFT, https://support.microsoft.com/en-us/windows/how-do-i-log-on-as-an-administrator-63267a09-9926-991a-1c77-d203160c8563#:~:text=AN%20administrator%20is%20someone%20who,changes%20to%20other%20user%20accounts [https://perma.cc/7L2R-PBL2].

signs a system, they will have granted the minimum permissions available to each user without impacting the user's efficiency.[107]

Unfortunately, the Court has held that "[s]o long as a person is entitled to use a computer to obtain information in at least *one* circumstance, this statute does not apply even if the person obtains the data outside that circumstance."[108] But the tiered security system poses a significant problem to the Court's analysis.[109] Does a user with mere reading privileges on an excel file qualify as having authorized access to edit that file? Additionally, a cloud storage provider necessarily has access to all the files on a server, so an agent of the cloud storage provider, someone who a data owner never intended to grant an unlimited license, could effectively act as an outside hacker yet still be shielded from CFAA liability because they had authorized access to the file.[110]

Both the ordinary meaning and technical understanding of permissions lend themselves to the Government's reading.[111] In the previous example, a user who possesses only a permission to read a file, and surreptitiously writes false data into a file exceeds the authority of their permission on that file.[112] Justice Thomas similarly points out how "an employee who is entitled to pull the alarm in the event of a fire is not entitled to pull it for some other purpose."[113] A valet's license to park a car does not include the ability to go for a joyride.[114] Justice Thomas likened Van Buren's permission to access the database to an entitlement, and that "[e]ntitlements are necessarily circumstance dependent" because entitlements exist where there are "proper grounds."[115] Thus, "[b]ecause Van Buren lacked a law enforcement purpose, the 'proper grounds' did not exist."[116]

Curiously, the Court never addresses who gives such permissions to the employees.[117] Usually, it is the company that holds the interest in data, but it is an agent of the company, the system administrator for a network or a

107. *See The Principle of Least Privilege*, IDENTITY MGMT. INST. CTR. FOR IDENTITY GOVERNANCE, https://identitymanagementinstitute.org/the-principle-of-least-privilege/ [https://perma.cc/42D5-NSP8].

108. Van Buren v. United States, 141 S. Ct. 1648, 1663 (2021) (Thomas, J., dissenting).

109. *See* COMPUTER HOPE, *supra* note 95.

110. *See Van Buren*, 141 S. Ct. at 1662.

111. *See generally Van Buren*, 141 S. Ct. at 1662; COMPUTER HOPE, *supra* note 95.

112. *See generally Van Buren*, 141 S. Ct. at 1662; COMPUTER HOPE, *supra* note 95.

113. *Van Buren*, 141 S. Ct. at 1664.

114. *Id.*

115. *Id.*

116. *Id.* (quoting BLACK'S LAW DICTIONARY, at 477 (5th ed. 1979)).

117. *See generally Van Buren*, 141 S. Ct. 1648 (2021).

computer, who grants a user permissions on files, and thereby access to such files.[118] Social engineering also poses a unique problem to the Court's analysis of access.[119] Social engineering is where "an attacker uses human interaction . . . to obtain or compromise information about an organization or its computer systems."[120] Consider an employee with no permissions to a file who uses social engineering to convince a system administrator to email a file. Does the sending of the file by an authorized agent ratify that employee's access? The employee did not use a computer to exceed their access and does not fit the Court's Folder X/Y model.[121] In effect, the CFAA provides system administrators a safe harbor from the CFAA, and it destroys any civil liability a system administrator might have under the CFAA to the employer in the event they misuse data.[122] The Court has handed a shield to the people most capable of abusing their power.[123]

Justice Thomas appropriately analogized the situation to trespass.[124] A real property owner grants a license to enter onto their land because they know the license necessarily hinges upon the existence of an approved purpose.[125] Purpose is at the heart of conditional licenses, and "[a] conditional license or restricted consent to enter land creates a privilege to do so only in so far as the condition or restriction is complied with."[126] Thus, "[w]hat is true for land is also true in the computer context."[127]

The dangerous implication of the majority's holding is that low-level employees with any quantum of access to data can now access that data for illicit purposes and still be shielded from CFAA liability.[128] Unfortunately, this outcome is predicated on a fundamental misconception of how permissions work in computers.[129] Following *Van Buren*, employers must now

118. *See* MICROSOFT, *supra* note 105.

119. *Avoiding Social Engineering and Phishing Attacks*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (last updated Aug. 25, 2020), https://us-cert.cisa.gov/ncas/tips/ST04-014 [https://perma.cc/E629-JMK9].

120. *Id.*

121. *See* Van Buren v. United States, 141 S. Ct. 1648, 1654 (2021).

122. *See id.* at 1662.

123. *See Network and Computer Systems Administrators*, U.S. BUREAU OF LAB. STAT. (Sept. 8, 2021), https://www.bls.gov/ooh/computer-and-information-technology/mobile/network-and-computer-systems-administrators.htm [https://perma.cc/P4J3-PKF7].

124. *Van Buren*, 141 S. Ct. at 1664 (Thomas, J., dissenting).

125. *Id.*

126. *Id.* at 1664–65.

127. *Id.* at 1665.

128. *See id.* at 1662.

129. *See* COMPUTER HOPE, *supra* note 95.

closely police and narrow access to information knowing that even a peppercorn of authority is enough to shield a hacker from the CFAA.[130] A limited license is a concept taught to first-year law school students in their basic property law course, and even though data is considered property, the Court has effectively ruled that there are no limited licenses for data.[131] Further, the Court has taken away a vital prosecutorial tool which fought an increasingly complex cybersecurity war against insider criminals.[132]

While the Court's concern about the scope of the CFAA is well-founded, insider hacking is an innocent casualty to a blunt solution.[133] The Electronic Frontier Foundation's ("EFF") amici brief argued that the Government's reading of the CFAA would create "an all-purpose Internet policing statute."[134] However, both the EFF and the Court confound their fears of an overbroad scope with the real issue of licenses in *Van Buren*.[135] While the scope of the CFAA is a problem, the issue in *Van Buren* is not that it applies "to all information from all computers that connect to the internet,"[136] but that *Van Buren* exceeded the authority of his license as both a computer programmer and a layman would understand it.[137]

The CFAA was never an all-purpose internet policing statue; by applying the principles of property law to the CFAA, the Court could have imposed property law as a bandage until Congress addressed the scope of the statute.[138] The Court even defined "[e]ntitle" as "to give . . . a title, right, or

130. *See U.S. Supreme Court Narrows the Scope of Federal Anti-Hacking Law in Van Buren v. United States*, SULLIVAN & CROMWELL LLP at 3 (Jun. 4, 2021), *https://www.sullcrom.com/files/upload/sc-publication-supreme-court-narrows-scope-federal-anti-hacking-law-van-buren-united-states.pdf* [https://perma.cc/B2B6-HWVT].

131. *See Van Buren*, 141 S. Ct. at 1662.

132. Leslie R. Caldwell, *Prosecuting Privacy Abuses by Corporate and Government Insiders*, U.S. DEP'T OF JUST. (last updated Mar. 3, 2017), https://www.justice.gov/archives/opa/blog/prosecuting-privacy-abuses-corporate-and-government-insiders [https://perma.cc/S33Q-24UF]; *Data Security: Top Threats to Data Protection*, U.S. DEP'T OF EDUC., at 4 (last updated June 2015), https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Issue%20Brief%20Data%20Security%20Top%20Threats%20to%20Data%20Protection_0.pdf (The DOE recognizes insiders as the first non-technical cyber security threat to information systems) [https://perma.cc/3MMA-29KG].

133. Caldwell, *supra* note 132.

134. Brief of Amici Curiae Electronic Frontier Foundation Supporting Petitioner at 9, Van Buren v. United States, 141 S. Ct. 1648 (2021) (No. 19-783), (Bloomberg Law).

135. *See id.*; *See Van Buren*, 141 S. Ct. at 1661.

136. *Van Buren*, 141 S. Ct. at 1652.

137. *See id.*

138. *See id.* at 1664-65 (Thomas, J., dissenting).

claim to something."[139] Yet it refused to use that property law context to inform its definition of "so" in the "entitled so to obtain" clause.[140] In doing so, the Supreme Court has made the CFAA a toothless tiger to fight insider computer fraud. This decision does not eliminate the problem of insider computer fraud, it merely declaws its remedies in the civil and criminal contexts. The Court may be signaling to Congress that it is time to act, but in doing so, the Court has created an unworkable solution for data owners.

139. *Id.* at 1654.

140. *See id.* at 1655.