MUNCK WILSON MANDALA

In the News

Justices’ CFAA Ruling Shows Contract Safeguards Insufficient

June 28, 2021 | (Time to read: 6 minutes)

Justices’ CFAA Ruling Shows Contract Safeguards Insufficient

By Aaron Dilbeck
Law360 (June 25, 2021, 3:20 PM EDT) —

The Computer Fraud and Abuse Act creates both civil and criminal liability for whoever “accesses a computer without authorization or exceeds authorized access.”

On June 3, the U.S. Supreme Court held in Van Buren v. U.S. that violating contractual limitations on computer usage cannot form the basis of liability under the CFAA but expressly declined to determine whether violating contractual limitations on computer access can form the basis of liability.[1]

Because violations of contractual limitations on computer usage cannot be used to establish a CFAA claim, companies should not rely on contractual limitations on computer access either.[2]

History of the CFAA

The CFAA was originally enacted as a criminal statute “[a]fter a series of highly publicized hackings captured the public’s attention” in the 1980s to deter access to computers with certain financial information.[3] Within the CFAA’s legislative history, Congress described the CFAA “in terms of trespassing into computer systems or files.”[4]

The CFAA has since been amended to (1) allow civil claims[5] and (2) create liability for accessing any computer that connects to the internet, not just computers with certain financial information.[6]

As the CFAA made its way through the courts, the federal circuit courts disagreed over whether “exceeds authorized access” should be interpreted narrowly or broadly. The narrow interpretation was that exceeding authorized access is limited to when a person violates limits on accessing information, which does not include violating limits on the use of information.[7] As a result of the split, the Supreme Court granted certiorari in Van Buren.[8]

Supreme Court’s Ruling

Van Buren was charged, convicted and sentenced under the CFAA for exceeding authorized access because he accessed the computer while violating his departments’ computer use policy.[9] Reversing Van Buren’s conviction, the Supreme Court adopted the narrow interpretation: “Exceeds authorized access” means “the act of entering a part of the system to which a computer user lacks access privileges.”[10]

Of note, while Van Buren was a criminal case, the court also applied its interpretation to the civil context.[11] As a result, the court’s opinion will be applied in the civil context as well.

Pending Issue

Although the Supreme Court did clarify the CFAA, some ambiguity remains because the court expressly declined to resolve the issue of whether the notion that “one either can or cannot access certain areas within the system” depends on whether access is prohibited by limitations created by technological barriers, such as passwords, or contractual limitations, such as employment agreements.[12]

The court had the opportunity to address the issue again less than two weeks after issuing the Van Buren opinion, but the court again refused to address what constitutes a sufficient limitation on access in LinkedIn Corp. v. hiQ Labs Inc.[13]

The U.S. Court of Appeals for the Ninth Circuit's 2019 opinion addressed whether hiQ Labs Inc., which used bots to gather publicly available information on LinkedIn, accessed a computer without authorization and violated the CFAA by violating LinkedIn's user agreement that barred the use of bots.[14]

Instead of addressing the limitations on access issue, the court issued a cursory opinion vacating the judgment for further consideration in light of Van Buren.[15] As a result, the court likely interpreted the prohibition against bots as a limitation on use, instead of a limitation on access, issue. Although the question of what constitutes a sufficient limitation on access may seem minor or straightforward, the lower courts have not provided a uniform answer.

For example, the federal circuit courts appear to have issued conflicting opinions. The Ninth Circuit held that circumvention of technological access barriers is required to establish a person exceeds authorized access and violates the CFAA.[16]

The U.S. Court of Appeals for the Fourth Circuit, however, in the 2014 U.S. v. Steele opinion held that breaching a promise in a "resignation letter that [the defendant] would not attempt to access the system thereafter" was sufficient to establish a person acted without authorization and violates the CFAA.[17]

Although one opinion concerns "exceeds authorized access," and another concerns access "without authorization," they still offer conflicting opinions on whether a contractual limitation on access can trigger CFAA liability.

District courts outside the Fourth and Ninth Circuits have also issued conflicting opinions. The U.S. District Court for the District of Columbia held in the 2019 Psychas v. District Department of Transportation decision that a person exceeds authorized access when he had authorization to view another's account information, but was not granted permission to use that information or access that account.[18]

The U.S. District Court for the District of New Hampshire, however, held in the 2012 Wentworth-Douglass Hospital. v. Young & Novis Professional Association decision that a person only exceeds authorized access by either hacking or circumventing technological access barriers, and not by merely accessing contract restricted information.[19]

Takeaways

Because the Supreme Court found that violating contractual limitations on proper use is insufficient to trigger CFAA liability, it follows that courts can be expected to find violating contractual limitations on access is also insufficient to trigger CFAA liability.

Simply put, Van Buren will likely be applied such that violating any limitations in a contract does not constitute a violation of the CFAA. In other words, it is doubtful that a CFAA claim will stand unless a defendant circumvents technological barriers.

Despite the uncertainty as to whether access must be restricted via technological barriers for a CFAA claim, businesses should not take a wait-and-see approach.

To ensure the preservation of a potential claim under the CFAA and the remedies it affords, businesses should implement technological barriers to prevent access of their sensitive data. Technological barriers include password implementation, which restricts who can access sensitive data,[20] and network segmentation, which divides a network into subnetworks and restricts who can access certain sensitive data.[21]

Unless technological barriers are implemented, businesses will likely have to rely on other causes of action — as opposed to the CFAA — such as breach of contract, misappropriation of trade secrets, theft, common law conversion, or state statutes for computer abuse, such as the Texas Harmful Access by Computer Act,[22] when current or former employees accesses information to which they are not entitled.

Aaron Dilbeck is an associate at Munck Wilson Mandala LLP. Reprinted with permission from the Jun. 25, 2021 issue of Law360 . Further duplication without permission is prohibited. All rights reserved.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] Van Buren v. United States , No. 19-783, 2021 WL 2229206, at *5 (U.S. June 3, 2021).

[2] See id.

[3] Id. at *3-4.

[4] United States v. Valle , 807 F.3d 508, 525 (2d Cir. 2015).

[5] Violent Crime Control and Law Enforcement Act of 1994, PL 103–322, 108 Stat 1796 (Sept. 13, 1994) (amending CFAA to add subsection (g), allowing a person to "maintain a civil action" against a violator of the CFAA).

[6] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, PL 107–56, 115 Stat 272 (Oct. 26, 2001) (amending the definition of what constitutes a protected computer).

[7] United States v. Nosal , 676 F.3d 854, 864 (9th Cir. 2012); see also WEC Carolina Energy Sols. LLC v. Miller , 687 F.3d 199, 206 (4th Cir. 2012).

[8] Van Buren, 2021 WL 2229206, at *5, n.2 (noting that the narrow interpretation had been adopted by the Second, Fourth, Sixth, and Ninth Circuits and the broad interpretation had been adopted by the First, Fifth, Seventh, and Eleventh Circuits).

[9] Id. at *4; see also United States v. Van Buren , 940 F.3d 1192, 1208 (11th Cir. 2019), rev'd and remanded, No. 19-783, 2021 WL 2229206 (U.S. June 3, 2021).

[10] Van Buren, 2021 WL 2229206, at *9.

[11] Id. at *10.

[12] Id. at *9, n.8 and accompanying text.

[13] Linkedin Corp. v. hiQ Labs, Inc. , No. 19-1116, 2021 WL 2405144 (U.S. June 14, 2021).

[14] hiQ Labs, Inc. v. LinkedIn Corp. , 938 F.3d 985, 1003 (9th Cir. 2019) (The CFAA "is violated when a person circumvents a computer's generally applicable rules regarding access permissions, such as username and password requirements, to gain access to a computer.").

[15] Linkedin Corp., 2021 WL 2405144, at *1.

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

[17] United States v. Steele , 595 F. App'x 208, 211 (4th Cir. 2014).

[18] Psychas v. Dist. Dep't of Transp. , No. CV 18-0081 (ABJ), 2019 WL 4644503, at *8 (D.D.C. Sept. 24, 2019), dismissed by plaintiff sub nom. Psychas v. Marcou , No. 19-7159, 2020 WL 6600057 (D.C. Cir. Oct. 14, 2020).

[19] Wentworth-Douglass Hosp. v. Young & Novis Pro. Ass'n , No. 10-CV-120-SM, 2012 WL 2522963, at *4 (D.N.H. June 29, 2012).

[20] See Security Tips (ST04-003), Cybersecurity & Infrastructure Agency (last updated Nov. 14, 2019), https://us-cert.cisa.gov/ncas/tips/ST04-003 ("Set up individual accounts that allow onlythe access and permissions needed by each user.").

[21] See Start with Security: A Guide for Business, FTC (June 2015), https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business ("Segment your network. Not every computer in your system needs to be able to communicate with every other one. You can help protect particularly sensitive data by housing it in a separate secure place on your network."); see also Segment Networks and Deploy Application-Aware Defenses, NSA (Sept.2019), https://media.defense.gov/2019/Sep/09/2002180325/-1/-1/0/Segment%20Networks%20and%20Deploy%20Application%20Aware%20Defenses%20-%20Copy.pdf ("Generally, segmentation is done by separating access to the most sensitive and vulnerable services on the network, such as directory services, file-share services, and network management.").

[22] See Tex. Civ. Prac. & Rem. Code § 143.001, et seq.

Related People

- Aaron C. Dilbeck