Alert
Intellectual Property/Media

Weil

June 7, 2021

Supreme Court Narrows Scope of Liability under the Computer Fraud and Abuse Act

*By Jessica Lynn Falk**

On June 3, 2021, the U.S. Supreme Court issued its opinion in *Van Buren v. United States*. At issue was whether the Computer Fraud and Abuse Act of 1986 ("CFAA"), which was aimed at targeting computer fraud and hacking, makes it illegal for an authorized user of a computer system to use their access to obtain information with an improper motive or for an improper purpose. No. 19-783, at 1 (June 3, 2021). Specifically, petitioner Nathan Van Buren, a former police sergeant, used his computer to access a government database to retrieve information about a particular license plate number in exchange for money. *Id.* at 3. Despite using his valid credentials to access the database, Van Buren violated his department's policy, which "authorized him to obtain database information only for law enforcement purposes." *Id.* at 1. Van Buren was charged with a felony violation of the CFAA on the ground that running the license plate number violated the CFAA's "exceeds authorized access" clause at 18 U.S.C. § 1030(a)(2). *Id.* at 3-4. The jury convicted Van Buren and the U.S. District Court for the Northern District of Georgia sentenced him to 18 months imprisonment. *Id.* A panel of the U.S. Court of Appeals for the Eleventh Circuit affirmed Van Buren's conviction in accordance with Eleventh Circuit precedent. *Id.* The Eleventh Circuit was joined by the First, Fifth and Seventh Circuits in taking a broader view of the "exceeds authorized access" clause whereas the Second, Fourth, Sixth and Ninth Circuits all held a narrower view. *Id.* at 4. The Supreme Court granted Van Buren's petition for a writ of certiorari to resolve the circuit split "regarding the scope of liability under the CFAA's 'exceeds authorized access' clause." *Id.* at 5.

Writing for the 6-3 majority, Justice Amy Coney Barrett reversed the judgment of the Eleventh Circuit, holding that "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." *Id.* at 20. The majority conceded that Van Buren obtained the license plate information for an improper purpose, but ultimately concluded that he did not "exceed authorized access" as the CFAA defines that phrase. *Id.*

The CFAA defines "exceeds authorized access" as "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." 18 U.S.C. §1030(e)(6). The majority interpreted this last phrase, "is not entitled so to obtain" as referring "to information one is not allowed to obtain *by using a computer that he is authorized to access*." No. 19-783, at 6 (emphasis in

** Associate Anna A. Iskikian assisted in the preparation of this article*

original). Because Van Buren was *authorized* to access the information he obtained from the database, he did not violate the CFAA by obtaining this information, even though he did so with an improper motive. *Id.* at 1. The Government had argued that the phrase "is not entitled so to obtain" pertained to "information one was not allowed to obtain *in the particular manner or circumstances in which he obtained it*." *Id.* at 6 (emphasis in original). According to the Government's interpretation, the circumstance of Van Buren's improper purpose in obtaining the information violated the CFAA. The majority rejected this reading, noting that the Government did "not identify any textual basis for" its reading of circumstance-based limits into the CFAA. *Id.* at 7. The Court also rejected the Government's "common parlance" reading of the phrase "exceeds authorized access," and focused instead on the CFAA's explicit definition of the phrase as well as the overall technical and "computational" nature of the statute. *Id.* at 11.

Additionally, the Court noted that "the Government's interpretation of the statute would attach criminal penalties to a breathtaking amount of commonplace computer activity." *Id.* at 17. The Court remarked that "[i]f the 'exceeds authorized access' clause criminalizes every violation of a computer-use policy, then millions of otherwise law-abiding citizens are criminals." *Id.* at 17-18. As the Court explained, employers commonly have computer access policies that state that the computers or electronic devices "can be used only for business purposes," therefore, under the Government's interpretation, "an employee who sends a personal e-mail or reads the news using her work computer has violated the CFAA." *Id.* at 18. The Court also expressed concern over applying the Government's interpretation to internet access given that websites and other online services typically only grant a user access if the user abides by the entity's terms of service. *Id.* Citing several *amici*, the Court echoed their concerns that a broad interpretation of the CFAA could result in "criminaliz[ing] everything from embellishing an online-dating profile to using a pseudonym on Facebook." *Id.*

Justice Clarence Thomas wrote a dissenting opinion, stating that under the majority's narrow reading, the CFAA will "apply only when a person is 'not entitled [*under any possible circumstances*] so to obtain' information." *Van Buren*, No. 19-783, dissenting slip op. at 3 (emphasis in original). The dissent also criticized the majority's conclusion at the outset that Van Buren was entitled to obtain the particular license plate information at issue, noting that "the plain meaning of 'entitled' compel[led] the opposite conclusion." *Id.* Accordingly, because Van Buren lacked a law enforcement purpose, he was "not entitled to obtain the data when he did so," in violation of the CFAA's "exceeds authorized access" clause. *Id.*

The Court's decision significantly reduces the range of conduct that can violate the "exceeds authorized access" clause of the CFAA. As a result, companies will not be able to invoke the CFAA's private action right against employees and other individuals that are authorized to access company systems but use that access improperly, and will be forced to rely on claims such as misappropriation of trade secrets or breach of contract to protect against such conduct. Of note, this decision also limits the ability of website owners to claim CFAA violations where a third party undertakes web-scraping of their site in violation of the site's terms of service. As a result, companies should consider evaluating their current data systems and how they restrict access to sensitive or confidential materials from users who are otherwise authorized to access those data systems.

If you have questions concerning the contents of this issue, or would like more information about Weil's IP/Media practice group, please speak to your regular contact at Weil, or to the editors or practice group members listed below:

Editor:

Randi Singer (NY)	View Bio	randi.singer@weil.com	+1 212 310 8152

Contributing Authors:

Jessica Lynn Falk (NY)	View Bio	jessica.falk@weil.com	+1 212 310 8511
Anna A. Iskikian (NY)		anna.iskikian@weil.com	+1 212 310 8272