# Supreme Court Clarifies 'Exceeding Authorized Access' Under CFAA: So Much Depends on 'So'

by Steve Kramarsky & John R. Millson

Cybercrime and hacking are much in the news recently, and the recent wave of ransomware attacks reminds us of how our dependence on heavily networked and interconnected systems can leave even our most critical infrastructure vulnerable to attack. Numerous federal and state statutes seek to provide protection against this kind of activity, but even leaving aside enforcement issues (which can be substantial, particularly for conduct that originates outside the United States) courts have struggled to interpret the precise scope of these laws. While most people have some idea of what "computer hacking" is, defining it with the specificity necessary to impose criminal liability has sometimes turned out to be a challenge.

For example, most federal criminal prosecutions for "hacking" (as that term is generally understood) are brought under the Computer Fraud and Abuse Act (the CFAA), 18 U.S.C. §1030, which covers a broad range of misconduct relating to networked computer systems. Violations of the CFAA can lead to both civil and criminal liability, so the statute attempts to draw bright lines defining its scope. Nonetheless, the courts within the Federal Circuit have disagreed substantially about what conduct the statute actually prohibits—at least at the margins.

Broadly speaking, the CFAA prohibits online misconduct in several categories: obtaining unauthorized access to a system (or exceeding authorized access to a system) and thereby improperly gaining access to protected information, damaging computer systems (either by unauthorized access or by transmitting malicious code), trafficking in passwords and code used for unauthorized access, and extortion or threats related to the prohibited conduct. Although the prohibited conduct is broadly defined, the "access" prohibitions are aimed at a person who "intentionally accesses a computer without authorization or exceeds authorized access." The issue, for many courts, has been the meaning of "exceeding authorized access." If a Netflix subscriber shares their password with a roommate in violation of Netflix's terms of service, is the roommate subject to federal criminal prosecution under the CFAA? The access is "authorized" in the sense that the password is valid and the roommate has the subscriber's permission, but it "exceeds" the authorization set out in the terms of service. Is that contract violation also a federal crime?

That specific question is currently unresolved, and the Supreme Court has declined to address it directly. But recently the Supreme Court addressed a related question regarding the scope of authorized access under the CFAA which may provide some useful guidance: What happens when an *authorized* user accesses a system for an explicitly *unauthorized* purpose? The Circuits had split on whether such conduct

would trigger the "exceeding authorized access" clause, and the Supreme Court ruled that it did not, siding with the Second Circuit (among others) in construing the CFAA narrowly. The opinion, *Van Buren v. United States*, 141 S.Ct. 1648 (2021), is worth a closer read.

# Background and Procedural History

While working as a police sergeant in Georgia, Nathan Van Buren "developed a friendly relationship" with Andrew Albo, an individual Van Buren's supervisor described as "very volatile." Van Buren approached Albo and asked for a personal loan, but Alpo recorded their conversation and "took it to the local sheriff's office," alleging that Van Buren had tried to "shake him down." That tape was given to the FBI, which set up a sting operation to trap Van Buren: at the FBI's behest, Albo asked Van Burde to run a search through a law enforcement database for a woman's license plate, to confirm she was not an undercover officer. Albo offered Van Buren $5,000 for conducting the search.

Van Buren used his valid law enforcement credentials to log in to a law enforcement database and run the license-plate search. Van Buren's search violated department policy, which permitted him "to obtain database information only for law enforcement purposes." Shortly thereafter, Van Buren shared the results of his search with Albo and was arrested for violation of the CFAA.

After a trial, Van Buren was found to have violated CFAA §1030(a)(2), which prohibits intentionally accessing a computer without authorization, or exceeding authorized access, and thereby obtaining information from any protected computer. (In the context of the CFAA a "protected computer" has been held to include any computer connected to the Internet.) Van Buren's conviction relied on the finding that he knew he was "exceed[ing] authorized access" when he ran the search because he had been trained that department policy prohibited conducting a search through any law enforcement database for personal purposes. Van Buren was sentenced to 18 months in prison. On appeal, the Eleventh Circuit upheld the conviction, finding that "Van Buren had violated the CFAA by accessing the law enforcement for an 'inappropriate reason.'" See *United States v. Van Buren*, 940 F.3d 1192, 1208 (2019).

# The Supreme Court Ruling

Van Buren appealed his conviction to the Supreme Court. In 2020, the court granted certiorari to resolve a circuit split "regarding the scope of liability under the CFAA's 'exceeds authorized access' clause." Several circuits, including the Eleventh, Fifth, Seventh, and First had taken an expansive view of that clause, holding that an authorized user who accesses a system for an unauthorized purpose—or in a manner that violates the underlying rules of the system's operator—also violates the CFAA. Others, including the Second, Sixth, Fourth, and Ninth had taken a narrower one.

The central question before the court was whether individuals who "have improper motives for obtaining information that is otherwise available to them," violate the CFAA's prohibition against exceeding

"authorized access" to obtain that information. The court answered that question in the negative, holding that the plain language of the CFAA called for narrower reading of the statute than the Eleventh Circuit employed. The court held that the plain meaning of "exceeds authorized access," as defined in the CFAA, applies only to computer uses through which an individual gains access to "information that [they are] not entitled to obtain." In other words, if a user is entitled to access the specific information at issue, what they do with that information is beyond the scope of the CFAA.

The court first considered the text of the statute. The CFAA defines "exceeds authorized access" to mean "to access a computer with authorization and use such access to obtain … information in the computer that the accesser is not entitled so to obtain." The question before the court was whether Van Buren was "entitled so to obtain" the information in his license-plate search. The court's textual analysis centered primarily on the word "so." Van Buren argued that "so" "serves as a term of reference that recalls 'the same manner as has been stated.'" And therefore that "[t]he disputed phrase, 'entitled so to obtain'" "asks whether one has the right, in 'the same manner as has been stated,' [in the CFAA, by using a computer that he is authorized to access] to obtain the relevant information."

Put more simply, Van Buren argued that the word "so" is intended to *narrow* the scope of prohibited conduct, so that it includes only using authorized access to obtain information that is beyond the scope of that authorization—for example, using a valid login to gain access to material in a folder or database that the user is not authorized to access.

The government argued that "so" modifies "entitled" to "refer to information one was not allowed to obtain *in the particular manner or circumstances in which he obtained it.*" The court rejected that interpretation, finding that it would write into the statute "any circumstance-based limit appearing anywhere—in the United States Code, a state statute, a private agreement, or anywhere else." In other words, the court held that, under the government's reading, that CFAA would potentially criminalize any violation of any restriction on use, public or private.

The court thus accepted Van Buren's position and held that CFAA §1030(a)(2)'s prohibition on "exceed[ing] authorized access" applies only to individuals who use a computer to access files they are not allowed to have, not individuals who access files they are allowed to have, but use them for an impermissible purpose.

The court found support for this interpretation in the structure of the statute, as well as in its text. The court considered the interplay "between the 'without authorization' and "exceeds authorized access' clauses." Under Van Buren's reading, the "without authorization" clause targets "outside hackers" who access a computer without permission, while the "exceeds authorized access" clause provides "complementary protection" by targeting "inside hackers" who '"exceed' the parameters of authorized access by entering an area of the computer to which [that] authorization does not extend." T he court found that Van Buren's reading caused the clauses to function consistently with 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."

The court observed that the government's position would create an inconsistency "with the design and structure" of subsection (a)(2) by incorporating purpose-based limits into the "exceeds authorized access" clause, but not the "without authorization" clause.

Finally, the court considered the legislative history and practical impact of the government's position, noting that an amendment to the CFAA "*to remove* the statute's reference to purpose" cut against the government's purpose-based reading. As to practical impact, Justice Barrett wrote—in perhaps the driving force behind the opinion—that the government's interpretation would criminalize the actions of "millions of otherwise law-abiding citizens" who engaged in acts as innocuous as checking their personal e-mail at work in violation of their employer's policies. The court appeared to express the view (consistent with that expressed by the Second Circuit) that the CFAA, as a criminal statute, must be interpreted narrowly, rather than expansively, to avoid such an outcome.

## Dissenting Opinions and Practical Effects

The court's opinion in *Van Buren* establishes a bright line rule: the CFAA's prohibition against exceeding authorized access only criminalizes use of a computer to access information to which the user is not entitled access under any circumstances. The analysis focuses entirely on the user's right to access the system—not the purpose of that access or the subsequent use of the material accessed.

While that ruling will certainly make for more consistent enforcement, a dissenting opinion signed by Justices Thomas, Roberts, and Alito discusses the limitations inherent in that approach, which had led the Eleventh Circuit and several other Circuit courts to a different view. A natural reading of the phrase "exceeds authorized access" could well include using a computer system to which one has legitimate, authorized access for some unauthorized purpose, because the "precondition that permitted [the user] to use that data was absent" and therefore the use "exceed[ed] authorized access."

The majority opinion parses the definition of "exceeds authorized access" differently and holds that the statute explicitly limits its reach to access of information the user was not entitled to access. But even for the majority, this a close call, coming down to the interpretation of the word "so." Perhaps the most obvious driver for the majority's interpretation was a practical one, which came in a whisper at the end of its opinion: "[T]he government's interpretation of the statute would attach criminal penalties to a breathtaking amount of commonplace computer activity." Everyone checks their email at work and an interpretation of the CFAA that might make doing so a federal crime would be hard to swallow.

Which brings us back to Netflix. The court does not answer the question of whether the Netflix subscriber's roommate violates the CFAA by logging in with borrowed credentials. *Van Buren* focuses on whether the access was authorized, but does not analyze what happens if an individual uses valid credentials, with the consent of their "owner," to access a service in violation of its terms of use. However, the decision in *Van Buren* makes it clear that the court will not automatically import the violation of private policies

or contracts into a criminal statute to criminalize a broad range of "ordinary" conduct. It looks like the roommate is safe for now.

This article first appeared in the *New York Law Journal* on July 26, 2021. Stephen M. Kramarsky, a member of Dewey Pegno & Kramarsky, focuses on complex commercial and intellectual property litigation. Jack Millson is an associate at the firm.