Intellectual Property & Technology Law Journal

Edited by the Technology and Proprietary Rights Group of Weil, Gotshal & Manges LLP

VOLUME 33 • NUMBER 7 • JULY-AUGUST 2021

U.S. Supreme Court Favors Narrower Reading of Computer Fraud and Abuse Act "So" It Does Not Cover Misuse of Authorized Access

Aime Dempsey

A significant opinion concerning computer security was one of those the U.S. Supreme Court issued during its end-of-term flurry this year. Employers and others who permit computer access to sensitive information for business or other defined purposes may want to take note of the ruling, *Van Buren v. United States*.[1]

Spoiler alert: The opinion undercuts use of the Computer Fraud and Abuse Act of 1986 ("CFAA")[2] to obtain federal jurisdiction in employer-employee disputes. (As a practical matter, however, the Defend Trade Secrets Act of 2016 had already filled the gap for many circumstances).

THE RULING

Last December, the Supreme Court accepted certiorari for *Van Buren v. United States*,[3] a case from the U.S. Court of Appeals for the Eleventh Circuit requiring interpretation of a specific part of the CFAA, a federal anti-hacking statute that generally prohibits obtaining or altering computer information without authorization, or by exceeding authorized access.

The Supreme Court has now reversed the Eleventh Circuit judgment, holding that the CFAA "covers those who obtain information from particular areas in the computer – such as files, folders, or databases – to which their computer access does not extend. It does not cover those who, like Van Buren, have improper motives for obtaining information that is otherwise available to them."

In other words, the Supreme Court settled upon the narrower of the proffered readings of the CFAA, such that a smaller sphere of behaviors will be found to violate the statute. The decision suggests that, in order to maintain the possibility of a CFAA action, which confers federal jurisdiction, as part of its available arsenal to protect confidential information, a wise employer will review its computer use policies with special attention to which computer databases, files, and folders employees and other users are entitled, or permitted, to access for any purpose.

Aime Dempsey is a member of the Litigation and Employment, Labor & Workforce Management practices at Epstein Becker & Green, P.C. She handles a broad range of commercial and employment-related matters, including those involving employee mobility and confidential information, across tribunals. Resident in the firm's New York office, Ms. Dempsey may be contacted at *adempsey@ebglaw.com*.

THE ISSUE

The critical question before the Supreme Court in *Van Buren* was how to interpret the phrase "exceeds authorized access" in the statute, which provides for criminal penalties and/or a private right of action against someone who "intentionally accesses a computer without authorization or exceeds authorized access" and thereby causes damage.

Petitioner Nathan Van Buren was a police sergeant in Cumming, Georgia, who used his valid credentials to access the patrol car computer, and, from that computer, the law enforcement database maintained by the Georgia Crime Information Center ("GCIC"), in order to obtain information about a license plate. Van Buren was led to believe that the license plate belonged to a woman in whom an acquaintance of his was romantically interested, and that the acquaintance would pay him about $5,000 to check the license plate information.

There was no dispute that Van Buren was authorized to access both the computer and the database involved, and there was also no dispute that he sought the license plate information for an improper purpose, outside his job duties; that is, to find out, on behalf of another individual and for his own personal gain, whether the owner of the license plate was an undercover police officer.

Van Buren was charged with and convicted of various offenses, including violation of the CFAA, and sentenced to 18 months in prison.

THE CIRCUIT COURT DECISION

Van Buren appealed the CFAA conviction, arguing, *inter alia*, that he did not "exceed [] authorized access" because he was authorized to access the GCIC database, even if he violated department and other policies by searching the database for personal gain rather than police business. The Eleventh Circuit affirmed the conviction, based on its precedent adhering to the broader interpretation of "exceeds authorized access" – that is, as prohibiting an individual from using his or her authorized access to databases or computer folders for purposes that are not authorized.

The circuits had split on whether that interpretation or the narrower view, whereby the CFAA is only violated if the user is not authorized to access the database or computer folder in the first place, was right.

THE SUPREME COURT'S ANALYSIS

The Supreme Court agreed to resolve the split. The Supreme Court decided, in a 6-3 decision authored by Justice Barrett and joined by Justices Breyer, Sotomayor, Kagan, Gorsuch, and Kavanaugh, that the narrower reading is the correct one.

The term "exceeds authorized access" is defined in the CFAA to mean "to access a computer with authorization and to use such access to obtain or alter information in the computer that the assessor is not entitled *so* to obtain or alter."[4] Because there is no dispute that Van Buren was "authorized" to "access [the] computer" he used, or that he "obtain[ed] information," the decision turned on whether he was "entitled so to obtain" the information. As foreshadowed by the oral argument, the analysis turns on the meaning of the word "so" in the phrase "entitled so to obtain."

The opinion undertook a painstaking analysis, beginning with a text-based approach. The Supreme Court addressed the text of the statute from several angles. It determined that "so," using the dictionary definition of "the same manner as has been stated" or "the way or manner described" must have its reference within the text of the statute, rather than outside of it. The majority found that the proper antecedent to "not entitled so to obtain," then, is via a computer the user is authorized to access.

The Supreme Court explained that, once having legitimately accessed a computer, the user may then go on to access areas of the computer where information is stored, such as databases, files, or folders. The user may have permission, whether by password, policy, or otherwise, to access some areas of the computer, but not others. The word "so" in the phrase "entitled so to obtain" accordingly refers to which of those areas the individual accesses from that authorized computer.

Thus, if the user only accesses files the user is legitimately permitted to access, the user does not violate the statute, even if the user then uses that information for an improper purpose, but if the user accesses, and obtains or alters information from, unauthorized databases, files or folders, the user runs afoul of the CFAA.

For example, an employer's computer network may have numerous databases, and may assign its employees a desktop or laptop computer from which the employees are authorized to access the network to perform their job functions.

If the employees are permitted to access databases in their own departments, and are prohibited from accessing, for example, a human resources database, they violate the CFAA if they obtain or alter any information from the human resources database.

If, on the other hand, there are no policies or passwords limiting the databases the employees can access, they will not violate the CFAA by accessing the human resources database, even if they use it to view other employees' personnel files, or other information that may be considered confidential. (To be clear, this interpretation of the CFAA would not prevent termination of the employee for violating company policy by viewing confidential files.)

The Supreme Court thus adopted Van Buren's interpretation of the statute and rejected the Government's reading, which would interpret "is not entitled so to obtain" to "refer to information one was not allowed to obtain *in the particular manner or circumstances in which he obtained it*."[5] That is the understanding that Van Buren was subject to at trial: because he was only permitted by policy to use the license plate database for police business, his use of it for an unauthorized purpose was found to be a violation. The Supreme Court's decision adopting the narrower view thus overturned his conviction.

After examining the text and the arguments of the government and of the dissent from several angles to support its reading, the Supreme Court proceeded to also analyze the structure of the statute. The Supreme Court decided that the structure, as well as the purposes of the statute, like the textual analysis, also supported the narrow view. The Supreme Court explained that the phrases "without authorization" and "exceeds authorized access" are best balanced when both are evaluated using a "gates up or down" approach. That is, the user either does, or does not, have authorization to access a particular computer, and the user does, or does not, have permissible access to a particular database, file, or folder. Finding a CFAA violation when a person misuses data or information from a database that the user did have permission to access, according to the Supreme Court, would not afford the structure of the statute that same balance.

In addition, the Supreme Court found its interpretation of the CFAA best suited the anti-hacking purposes of the statute in that accessing prohibited computer files or folders is akin to internal hacking, whereas misusing information the user is authorized to access is not.

Finally, the majority discussed some of the "parade of horribles" that had been described at oral argument. Though not finding the issue determinative, calling it "extra icing on a cake already frosted," the Supreme Court noted that the government's reading "would attach criminal penalties to a breathtaking amount of commonplace computer activity." The Supreme Court cited sending a personal email or reading the newspaper from a work computer that is designated to be used for work purposes only, as examples of activities that could be criminalized if the broader view prevailed.

CONCLUSION

There are some key takeaways from the decision for employers and others with computer information to protect.

Given the narrow reading of "exceeds authorized access," the CFAA will not be available as a cause of action when an employee or other invited computer user misuses computer information the user is legitimately authorized to access (as has been true in the U.S. Courts of Appeals for the Second, Fourth, and Ninth Circuits for some time, though not in the U.S. Courts of Appeals for the First, Fifth, Seventh, or Eleventh Circuits). Accordingly, companies will have to rely on common law and contractual protections for confidential information, the Defense of Trade Secrets Act, if applicable, company policy, and similar tools, which are not diminished by this decision, to handle employees who, for example, download files they have worked on to take to a competitor.

However, owners of sensitive and confidential information may still be guided by the decision and its reasoning to take steps that could increase options for invoking the CFAA and could better protect their computer information more generally.

For example, employers will be well-advised to carefully evaluate the permissions granted to employees, customers, or other users, for the files, folders, and databases that make up the areas of their computers or computer networks. Perhaps not all employees need access to all databases, and if they

do not "so" need access, perhaps it should be formally restricted, via explicit policy or even by password or other barrier.

Although the meaning of the word "so" in the CFAA has now been settled, protection of confidential information remains an ongoing process, requiring constant vigilance.

Notes

1. *Van Buren v. United States*, No. 19-783 (U.S. June 3, 2021).
2. 18 U.S.C. §1030 *et seq*.
3. No. 19-783.
4. Section 1030(e)(6). (Emphasis added).
5. Emphasis in original.