HINSHAW

# U.S. Supreme Court Limits Reach of Computer Fraud and Abuse Act

**Privacy, Cyber & AI Decoded Alert | 4 min read**
Jun 9, 2021

Enacted in 1986, the Computer Fraud and Abuse Act (CFAA) provides businesses with a private right of action against an individual who "exceeds authorized access" of their computers. Violators are subject to criminal liability as well, punishable by fines and imprisonment. On June 3, 2021, the Supreme Court of the United States resolved a circuit court split over the scope of activity that constitutes "exceed[ing] authorized access."

In *Van Buren v. United States*, 593 U.S. ___ (2021), the Supreme Court held that an individual "exceeds authorized access" under the CFAA when they access a computer with authorization, but then obtain or alter information within the system that the individual was unauthorized to access for any purpose. The High Court declined to apply the CFAA to individuals who are authorized to access information within the system, but do so for an *improper* purpose. Whether an individual's authority to access the information within the system may be governed by policy as well as technology, however, remains unclear.

Van Buren, a former police sergeant, used a department-issued device to access a law enforcement database to retrieve a license plate number in exchange for money, in direct violation of department policy. Van Buren was subsequently charged with a felony under the CFAA for "exceed[ing] authorized access." The clause "exceeds authorized access" is defined in the statute as accessing "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."

There was no dispute that Van Buren had authority to access the department-issued device and had authority to access the database while performing law enforcement functions. The sole question before the Supreme Court was whether Van Buren violated the CFAA because he accessed the database for personal reasons. The Eleventh Circuit had answered this question affirmatively and held that Van Buren violated the CFAA by accessing the database for an "inappropriate reason."

The Supreme Court rejected the Eleventh Circuit's broad interpretation, finding instead, that the word "so" in the final clause of the CFAA definition for "exceeds authorized access" limited the scope of activity that constitutes a violation. The final clause refers to information "that the accessor is not entitled *so* to obtain." Because the word "so" means "the same manner as has been stated," the Supreme Court reasoned, the "phrase 'is 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." The Supreme Court held that an individual "exceeds authorized access" under CFAA when they "access 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." The Supreme Court declined to address whether the scope of the information that is "off-limits" may be governed by contract (*e.g.*, department policy, human resource manuals, etc.) as well as technology (*e.g.*, passwords, administrator rights, encryption, etc.).

# Significance of Decision

*For CIOs and Security Officers:* The CFAA does not apply to individuals who use their access to databases and files for an improper purpose. While the CFAA remains a valid weapon against insiders that have no authority at all to access a specific digital storage location, **the CFAA can no longer be used to prosecute insiders that download work files**—or any other information the insider has authority to access—before leaving to work for a competitor or for other personal reasons. Given that the Supreme Court declined to address whether a policy manual or employment contract can govern the scope of information that is "off-limits," businesses should expand their efforts to deploy strict technological access controls over sensitive information.

*For GCs and Insurers:* The Supreme Court's decision is based on CFAA's explicit definition for the phrase "exceed authorized access" and not the plain meaning of those words. Most statutes dealing with digital storage and handling of information use some combination of the terms "authorize" and "access" to define what constitutes a violation, but do not further define the terms beyond their ordinary meaning. The data breach notification laws in Connecticut and Florida, for example, define a "Breach of Security" as "unauthorized access" to personal information. Historically, unauthorized access to electronic information is deemed to occur both when an unauthorized individual gains access to information as well as when an authorized individual gains access to information for an improper purpose or for a purpose beyond which they were granted authority. The Supreme Court's decision in *Van Buren* may not change how lower courts interpret statutes using the plain meaning of terms "authorized" and "access," but **the decision is likely to create some confusion regarding the property rights associated with electronic information**.

Employers looking for additional insight on the impact of *Van Buren* should read Ambrose McCall's piece in the *Employment Law Observer*.

## Related Capabilities

Data Privacy, AI & Cybersecurity