Cybersecurity, Privacy & Data Protection Alert

Akin Gump
STRAUSS HAUER & FELD LLP

Landmark Supreme Court Decision on Federal Anti-Hacking Law

June 8, 2021

Key Points

- The Supreme Court held that a former police officer did not violate the CFAA by "exceeding" his authorized access to a law enforcement database when he used the database to sell information because he was otherwise authorized to access the database for law enforcement purposes.
- The CFAA's "exceeds authorized access" provision covers those who obtain information from particular areas in a computer to which their computer access does not extend. It does not cover those who have improper motives for obtaining information that is otherwise available to them.
- The Court's ruling impacts what conduct is criminally enforceable under the CFAA and limits legal remedies available to employers and private parties for misuse of data or violations of use policies. Companies should analyze whether appropriate protections are in place to safeguard against conduct now decriminalized under the CFAA.

On June 3, 2021, the U.S. Supreme Court adopted a narrow interpretation of what it means to "exceed authorized access" to a computer under the Computer Fraud and Abuse Act (CFAA) in *Van Buren v. United States*, No. 19-783. In a 6-3[1] decision authored by Justice Barrett, the Court rejected a broad interpretation of the law as criminalizing common computer activity. The decision clarifies what conduct is covered under the provision: "[t]his provision 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."

Background

The CFAA provides criminal and civil remedies for whoever intentionally accesses a computer without authorization or exceeds authorized access. The 1986 anti-hacking law addresses external hacking (access without authorization) and internal hacking (exceeds authorized access). To "exceed authorized access" under the CFAA means "to access a computer with authorization and to use such access to obtain or alter

Contact Information

If you have any questions concerning this alert, please contact:

Natasha G. Kohne
Partner
nkohne@akingump.com
San Francisco
+1 415.765.9505

Michelle A. Reed
Partner
mreed@akingump.com
Dallas
+1 214.969.2713

Pratik A. Shah
Partner
pshah@akingump.com
Washington, D.C.
+1 202.887.4210

Erica E. Holland
Counsel
eholland@akingump.com
New York
+1 212.872.8126

information in the computer that the accesser is not entitled so to obtain or alter."[2] Circuit courts split on the meaning of "exceeds authorized access" resulting in different consequences for the same conduct depending on the jurisdiction.

Georgia police sergeant Nathan Van Buren was prosecuted by the U.S. Department of Justice ("DOJ") and convicted of a felony violation of the CFAA for using his access to a law enforcement database to look up a license plate number in exchange for money. Van Buren appealed his conviction to the U.S. Court of Appeals for the Eleventh Circuit, arguing he did not violate the CFAA since he accessed a database he was authorized to access. The Government argued Van Buren exceeded the scope of his authorized use of the system for personal financial gain. The Eleventh Circuit affirmed the CFAA conviction. Van Buren petitioned the Supreme Court to review; the Court granted certiorari April 20, 2021. Oral arguments were held on November 30, 2020. See our earlier post for additional background.

Ruling

The Court overturned Van Buren's conviction and reversed the Eleventh Circuit, holding:

[A]n 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. The parties agree that Van Buren accessed the law enforcement database system with authorization. The only question is whether Van Buren could use the system to retrieve license-plate information. Both sides agree that he could. Van Buren accordingly did not "excee[d] authorized access" to the database, as the CFAA defines that phrase, even though he obtained information from the database for an improper purpose.

The decision came down to competing interpretations of "**so**" in the definition of "exceeds authorized access." The Court rejected the Government's interpretation and fully adopted Van Buren's view. "Exceeds authorized access" means "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.[3]

The government argued the phrase "is not entitled **so** to obtain" referred to "information one was not allowed to obtain in the particular manner or circumstances in which he obtained it." The government added that the manner or circumstances in which one has a right to obtain information are "defined by any 'specifically and explicitly' communicated limits on one's right to access information."

Van Buren argued the phrase "is not entitled so to obtain" is "best read to refer to information that person is not entitled to obtain by using a computer that he is authorized to access." The Court agreed and laid out a grammatical analysis of the language. The Court described 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 ruling also detailed how the Government's interpretation would "attach criminal penalties to a breathtaking amount of commonplace computer activity." "If the 'exceeds authorized access' clause criminalizes every violation of a computer-use policy, then millions of otherwise law-abiding citizens are criminals." The Government argued that other provisions limit its prosecutorial power along with the DOJ's charging

policy, but the Court disagreed. “The Government’s approach would also inject arbitrariness into the assessment of criminal liability, because whether conduct like Van Buren’s violated the CFAA would depend on how an employer phrased the policy violated (as a “use” restriction or an “access” restriction).”

The opinion leaves some questions unanswered. Utilizing the gates-up-or-down inquiry, the Court does not state how a wrongdoer must circumvent the gate for liability to attach or define the gate, ultimately declining to address whether the gate inquiry turns on a technological or code based limitation on access, or instead, limits contained in contracts or policies.

Bottom Line

- The CFAA does not criminalize improper use of information on a computer the user is authorized to access. Consequently, misuse of company data or violations of terms-of-service limitations are not criminal violations of the CFAA. Companies may not completely rely on the CFAA as an enforcement tool and should revisit use policies, handbooks and contracts to police conduct and access to computers and data.
- Companies should reassess cybersecurity policies, procedures and infrastructure to better restrict access of users to only information and systems required to perform job duties, such as access controls and similar protocols. These policies, procedures and digital restrictions should draw a clear line on what a user is and is not authorized to access.
- Companies will need to utilize other legal avenues such as breach of contract, trade secret misappropriation, the Health Insurance Portability and Accountability Act (HIPAA), data breach laws and other state laws to pursue wrongdoers who misuse access to computers and information.

[1] Justice Thomas authored a dissenting opinion, joined by Chief Justice Roberts and Justice Alito.

[2] 18 U.S.C. § 1030(e)(6).

[3] 18 U.S.C. § 1030(e)(6).

akingump.com