Cybersecurity, Privacy & Data Protection Alert

Akin Gump
STRAUSS HAUER & FELD LLP

Supreme Court to Consider Scope of CFAA

April 24, 2020

Key Points

- The U.S. Supreme Court will review whether a person who is authorized to access information on a computer for certain purposes violates the CFAA if he accesses the same information for an improper purpose.[1]
- The Court's decision will likely resolve a circuit split on how broadly to interpret the CFAA. Courts of Appeals across the country vary in their interpretation on what it means to exceed authorized access to a computer under the CFAA.
- The Court's ruling will impact what common computer activities may carry criminal and civil liability under the CFAA and the future of computer fraud and hacking cases.

On Monday, April 20, 2020, the Supreme Court of the United States granted a certiorari petition in *Van Buren v. United States* (No. 19-783) to consider the scope of the Computer Fraud and Abuse Act (CFAA), specifically whether a user's authorized access to information for an unauthorized purpose violates the CFAA. Under the CFAA, it is a federal crime to access a computer system and obtain information without authorization or to exceed authorized access.[2] The statute 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."[3] Circuit courts are split on their interpretation of this language.

Appeals courts for the First, Fifth, Seventh and Eleventh Circuits have interpreted this provision broadly, finding potential liability under the CFAA for **unauthorized use** of information even where there was **authorized access** to the same information. However, the Second, Fourth and Ninth Circuits have taken a narrow approach, finding potential liability for exceeding **authorized access** not simply exceeding **authorized use**.

In *United States v. Van Buren*, a sergeant with the Cumming, Georgia Police Department was convicted of violating the CFAA when he used his authorized access to a government database to search for a license plate number for an improper purpose. Van Buren was authorized to use the database for law enforcement purposes and had been trained on the proper and improper use of the system. In a sting operation, the Federal Bureau of Investigation (FBI) found that Van Buren used

Contact Information

If you have questions about 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

Diana E. Schaffner
Counsel
dschaffner@akingump.com
San Francisco
+1 415.765.9507

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

the database for an illicit purpose, namely, to search the license plate number of a woman to determine if she was an undercover police offer, in exchange for money. The government argued Van Buren exceeded the scope of his authorized use of the system.

Van Buren appealed his conviction and argued that he was innocent of computer fraud since he only accessed databases that he was authorized to access.[4] On October 10, 2019, the U.S. Court of Appeals for the Eleventh Circuit affirmed the CFAA conviction. The Eleventh Circuit acknowledged that other courts have rejected the Eleventh Circuit's interpretation but held it was bound by its own precedent, finding that even a person with authority to access a computer can be guilty of computer fraud under the CFAA if that person misuses the computer.[5] On December 18, 2019, Van Buren petitioned the high court to consider the matter.

In the petition for certiorari, Van Buren argued the Eleventh Circuit's decision went far beyond the CFAA's objective, which he states is to forbid computer hacking, and could criminalize whole categories of innocuous behavior by most everyone who uses a computer. The petition states the broad reading of the statute would criminalize behavior like employees using company computers to generate March Madness brackets or law students using a legal research database, meant for educational use only, to look up housing laws to negotiate rent or a security deposit refund. Both uses could violate computer or system terms of use policies.

The Supreme Court will now have a chance to determine whether to interpret the CFAA broadly or narrowly and finally bring clarity to law. The Court's ruling will be consequential for cybersecurity strategies, company computer-use policies and ordinary internet, computer and smartphone users.

We will continue to monitor this case and provide updates of any significant developments.

[1] *Van Buren v. United States*, 940 F.3d 1192 (11th Cir. 2019) *petition for cert. granted*, No. 19-783 (U.S. Apr. 20, 2020).

[2] 18 U.S.C. §1030(a)(2)(C).

[3] 18 U.S.C. §1030(e)(6).

[4] *United States v. Van Buren*, 940 F.3d 1192, 1207 (11th Cir. 2019).

[5] *Id*. at 1208.

akingump.com