GIBSON DUNN

Supreme Court Narrows Scope Of Computer Fraud and Abuse Act, Holding It Does Not Prohibit Accessing Otherwise Available Information For An Improper Purpose

Client Alert | June 3, 2021

Decided June 3, 2021

***Van Buren v. United States,* No. 19-783**

Today, the Supreme Court held 6-3 that the Computer Fraud and Abuse Act does not cover obtaining information for an improper purpose if the user is otherwise authorized to access that information.

Background:
The Computer Fraud and Abuse Act of 1986 (CFAA) creates criminal and civil liability for "[w]hoever . . . intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information." 18 U.S.C. § 1030(a)(2). The phrase "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." *Id.* § 1030(e)(6).

Van Buren, a police officer, used his access to a law-enforcement database to run an unauthorized license-plate search in exchange for money, and was charged under the CFAA. The Eleventh Circuit, applying a broad view of the CFAA, held that Van Buren had exceeded his authorized access because he accessed the database for an improper purpose, in violation of his department's policies.

The Supreme Court granted certiorari to resolve the split between the narrow approach of the Second, Fourth, and Ninth Circuits, which hold that a person "exceeds authorized access" only if he accesses information on a computer that he is prohibited from accessing, and the broader approach of the First, Fifth, Seventh, and Eleventh Circuits, which hold that a person "exceeds authorized access" if he accesses otherwise available information for an unauthorized purpose.

Issue:
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 unauthorized purpose.

Court's Holding:
No. The CFAA proscribes only obtaining information from computers, files, folders, or

Related People

Lucas C. Townsend

Bradley J. Hamburger

Matt Benjamin

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

databases that a person is not authorized to access. It does not create liability for those who, like Van Buren, obtain information otherwise available to them for an unauthorized purpose.

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 . . . have improper motives for obtaining information that is otherwise available to them."

Justice Barrett, writing for the Court

What It Means:

- By holding that the CFAA does not prohibit accessing otherwise-available information for an improper purpose, today's decision clarifies that day-to-day violations of computer-use policies, such as using an employer-provided electronic device for a non-business purpose in violation of workplace rules, or using a pseudonym on a social media website in violation of the site's terms and conditions, do not in and of themselves give rise to liability under the CFAA.
- The Court explained that section 1030(a)(2)'s "exceeds authorized access" clause targets "inside hackers"—"those who access a computer with permission, but then exceed the parameters of authorized access by entering an area of the computer to which that authorization does not extend," whereas the "without authorization" clause targets "outside hackers"—those who "access a computer without any permission at all." The Court held that liability under both clauses turns on "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"—rejecting the Government's view that the "exceeds authorized access" inquiry depends on the facts and circumstances.
- The Court specifically left open the question of whether the scope of authorization turns only on technological or code-based restrictions on access or violations of contractual terms alone may give rise to liability under the CFAA. Nonetheless, the Court's reasoning suggests that a user violating terms-of-service or other policy restrictions alone likely does not exceed authorized access under the CFAA.

The Court's opinion is available here.

Gibson Dunn's lawyers are available to assist in addressing any questions you may have regarding developments at the Supreme Court. Please feel free to contact the following practice leaders:

Appellate and Constitutional Law Practice

Allyson N. Ho
+1 214.698.3233
aho@gibsondunn.com

Mark A. Perry
+1 202.887.3667
mperry@gibsondunn.com

Lucas C. Townsend
+1 202.887.3731
ltownsend@gibsondunn.com

Bradley J. Hamburger
+1 213.229.7658
bhamburger@gibsondunn.com

Related Practice: Privacy, Cybersecurity and Data Innovation

Alexander H. Southwell
+1 212.351.3981
asouthwell@gibsondunn.com

S. Ashlie Beringer
+1 650.849.5327
aberinger@gibsondunn.com

Ahmed Baladi
+33 (0)1 56 43 13 50
abaladi@gibsondunn.com

Matthew Benjamin
+1 212.351.4079

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

mbenjamin@gibsondunn.com
Related Practice: White Collar Defense and Investigations

Stephanie Brooker
+1 201.887.3502
sbrooker@gibsondunn.com
Joel M. Cohen
+1 212.351.2664
jcohen@gibsondunn.com
Nicola T. Hanna
+1 213.229.7269
nhanna@gibsondunn.com
Chuck Stevens
+1 415.393.8391
cstevens@gibsondunn.com
F. Joseph Warin
+1 202.887.3609
fwarin@gibsondunn.com
Reed Brodsky
+1 212.351.5334
rbrodsky@gibsondunn.com

Related Capabilities

Appellate and Constitutional Law

Privacy, Cybersecurity, and Data Innovation

White Collar Defense and Investigations

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**