PAUL HASTINGS

Stay Current

June 2021

Follow @Paul_Hastings

U.S. Supreme Court Narrows the Scope of Liability under the Computer Fraud and Abuse Act

By Kimia Favagehi & Aaron Charfoos

Introduction

The Supreme Court's ruling in *Van Buren v. United States*[1] has changed what was arguably once a punishable computer crime into just a violation of corporate policy.

On June 3rd, the Court's ruling in *Van Buren* narrowed the scope of liability under the Computer Fraud and Abuse Act ("CFAA"). The high court reversed an Eleventh Circuit decision to convict an ex-police sergeant who conducted a non-law enforcement search in the police department's database, finding that the sergeant had not "exceed[ed] authorized access."[2]

The Supreme Court stated that an individual does not exceed authorized access when they access a part of a computer to which they have access, even if they do so with an improper motive. Rather, "an 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."[3]

This major case appears to narrow the scope of liability under the CFAA's "exceeds authorized access"[4] clause and informs companies on what can be punishable in cybersecurity and computer crime.

Computer Fraud and Abuse Act

Congress originally enacted the CFAA in 1986 as an anti-hacking statute. The CFAA's primary purpose is to prevent unauthorized access to computers. The statute applies to any "protected computer,"[5] which until *Van Buren*, has prompted broad interpretations generally applicable to any computer connected to the internet.

Among its various criminal offenses, the CFAA imposes criminal liability when a person or entity "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer."[6] Punishments consist of monetary fines or imprisonment.

Courts have differed in their interpretations of the CFAA, with some adopting a narrow construction, while others have opted for a broader interpretation.

Van Buren v. United States

Nathan Van Buren conducted a license plate search in the police department's database in exchange for money. At the time he conducted the search, Van Buren had been given access to the database as part of his job duties. Federal prosecutors charged Van Buren for violating the CFAA by exceeding his authorized access when he conducted the search for a non-law enforcement purpose.

The Supreme Court was asked whether, under the CFAA, Van Buren exceeded his authorized access when he conducted the search for an improper purpose even though he was authorized to access the database? According to the Supreme Court, he did not.

Writing for the majority in a 6-3 split decision, Justice Barrett, joined by Justices Breyer, Sotomayor, Kagan, Gorsuch, and Kavanaugh, held that Van Buren did not violate the CFAA because exceeding authorized access "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."[7]

Because Van Buren's access did extend to the database, he did not exceed his authorized access as defined by the CFAA. The Court acknowledged that Van Buren's search clearly violated department policy, and he could be separately held responsible under different theories for that, but this was not enough to hold him criminally liable under the CFAA.

Rejecting the Government's broad view, the majority favored the narrower interpretation that one either possesses access to a computer—in Van Buren's case, the police department's database—or lacks access. Therefore, when an individual like Van Buren enters a part of a computer system to which they have access privileges, they are not violating the CFAA even if they violate corporate policies.

Justice Barrett's example is instructive—

> *"[I]f a person has access to information stored in a computer— e.g., in 'Folder Y,' from which the person could permissibly pull information—then he does not violate the CFAA by obtaining such information, regardless of whether he pulled the information for a prohibited purpose. But if the information is instead located in prohibited 'Folder X,' to which the person lacks access, he violates the CFAA by obtaining such information."*[8]

Looking Ahead

Companies should also be aware of another CFAA focused litigation, hiQ Labs v. LinkedIn.[9] In that case, the Ninth Circuit upheld a ruling by the district court that the CFAA did not prevent companies from scraping, or collecting, data on publicly available websites. On the other hand, if the data collector circumvents a technological barrier to gain access to the information they may violate the CFAA. LinkedIn has asked the Supreme Court to review the ruling, but the Court has not ruled on LinkedIn's petition.

Key Takeaways

The Supreme Court appears to have significantly narrowed the scope of liability in the CFAA. In light of *Van Buren* and other developments, going forward, companies should take several steps to help protect their data:

- Companies should review their policies and procedures to ensure that "exceeding authorization" is a clear violation of their own policies, even if the CFAA is unavailable;

- Companies should review internal controls and ensure that users are given the least privileged access to company systems and regularly audit those rights as employees move from role to role; and
- Companies should consider adding additional technical and contractual safeguards to prevent third parties from misusing information to which they gain access.

With the legal landscape shifting, companies should take affirmative steps to protect data that the CFAA may have once protected.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

Chicago

Aaron Charfoos
1.312.499.6016
aaroncharfoos@paulhastings.com

Washington, D.C.

Benham Dayanim
1.202.551.1737
bdayanim@paulhastings.com

Sherrese Smith
1.202.551.1965
sherresesmith@paulhastings.com

[1] *Van Buren v. United States*, No. 19-783, slip op. (U.S. June 3, 2021).

[2] 18 U.S.C. § 1030(e)(6).

[3] *Van Buren*, slip op. at 20.

[4] § 1030(e)(6).

[5] *Id.* § 1030(a)(2)(c).

[6] *Id.*

[7] *Van Buren*, slip op. at 1.

[8] *Id.* at 6.

[9] *hiQ Labs, Inc. v. LinkedIn Corporation*, 938 F.3d 985 (9th Cir. 2019).