Supreme Court Outlines Bounds of the Computer Fraud and Abuse Act

Skadden

06 / 07 / 21

If you have any questions regarding the matters discussed in this memorandum, please contact the following attorneys or call your regular Skadden contact.

Shay Dvoretzky
Partner / Washington, D.C.
202.371.7370
shay.dvoretzky@skadden.com

William Ridgway
Partner / Chicago
312.407.0449
william.ridgway@skadden.com

Alexander J. Kasparie
Associate / Chicago
312.407.0614
alexander.kasparie@skadden.com

One Manhattan West
New York, NY 10001
212.735.3000

In *Van Buren v. United States*, the Supreme Court's first opportunity to mark the limits of the Computer Fraud and Abuse Act (CFAA), the Supreme Court significantly curtailed the act's scope. In a decision on June 3, 2021, siding with the petitioner, ex-police officer Nathan Van Buren, the Court rejected the United States' interpretation of the CFAA, which would have opened the door for both civil and criminal liability in a wide variety of cases. Instead, the Court held that the act focuses on whether individuals have authority to access data, and not whether they had an improper purpose for accessing data that was otherwise available to them.

Background

Mr. Van Buren formerly served as a police officer in Cumming, Georgia. His service ended, however, after he accessed a police database in exchange for a bribe to retrieve certain information. Following his arrest, he was charged under 18 U.S.C. § 1030(a)(2)(C), which prohibits obtaining "information from any protected computer" by "intentionally access[ing] a computer without authorization or exceed[ing] authorized access." The statute defines exceeding authorized access as "access[ing] a computer with authorization and [ ] us[ing] such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter."[1]

The Court's Decision

The dispute raised a pure question of statutory interpretation: whether the phrase "exceed[ing] authorized access" only prohibits individuals from accessing information that they have no right to access under any circumstances, or whether it prohibits accessing information in violation of the terms governing that access. In a 6-3 decision, the Court, in an opinion authored by Justice Barrett, adopted the former reading.

Beginning with the plain text of the statute, the Court held that Mr. Van Buren's reading was more plausible than the government's was. Pointing to a host of similar statutes, the Court explained that the ordinary usage of "so" was to refer to "a stated identifiable proposition from the 'preceding' text," and not to import "*any* circumstance-based limit appearing *anywhere*." The Court likewise noted that its adoption of his reading resulted in a consistent approach to both liability prongs of § 1030(a)(2). Under that approach, to determine an individual's liability under § 1030(a)(2), a fact-finder need only determine whether the individual could or could not access a computer system or a data set within a system. Finally, the Court noted that neither its precedent nor the CFAA's legislative history supported the government's approach, and acknowledged that its reading prevented the possibility of an enormous expansion of federal liability and prosecutorial discretion.

Takeaways

- Although *Van Buren* was a criminal case, the CFAA is also a civil statute that is often used by businesses to seek redress against employees who misuse company data. The Court's decision sharply limits the ability of companies to use the CFAA against company insiders.
- Given those limits, businesses will likely turn to the trade secret laws to address employees' misuse of company information, and so should ensure that they are using "reasonable measures" to protect their company secrets, a precursor to invoking the trade secret regime.

[1] *Id.* § 1030(e)(6).

- The CFAA may still be available to companies that segment their data with passwords, so that employees are not able to access data to which they are not entitled. A banner that requires employees to certify that they are accessing data with a proper purpose will likely not be enough to invoke the CFAA.
- Finally, because action from Congress on this particular issue seems unlikely at this time, we expect state law may be used more often to address situations where employees abuse their access to sensitive information.