King & Spalding
Client Alert

JUNE 24, 2021

For more information, contact:

Zack Harmon
+1 202 626 5594
zharmon@kslaw.com

Sumon Dantiki
+1 202 626 5591
sdantiki@kslaw.com

Scott Ferber
+1 202 626 8974
sferber@kslaw.com

Bethany Rupert
+1 404 572 3525
brupert@kslaw.com

King & Spalding

Washington, DC
1700 Pennsylvania Avenue
2nd Floor
Washington, DC 20006-4707
Tel: +1 202 737 0500

Supreme Court Decision on Computer Fraud and Abuse Act: Implications for Cybersecurity and Insider Threat Programs

Earlier this month, the Supreme Court issued its first major decision on the Computer Fraud and Abuse Act ("CFAA") in *Van Buren v. United States*.[1] The decision has significant implications for how organizations protect confidential and sensitive information from insider threats or other individuals legitimately on their systems. In light of the decision, organizations should assess: (1) whether they have an updated data map of where they store particularly sensitive information and critical intellectual property on their networks; (2) whether they have clear technical controls and policies governing which employees, contractors, vendors, or others may access such information that are still enforceable following the decision; and (3) whether their current terms of service or use agreements on public-facing websites and consumer applications are still fully enforceable following the decision.

The Supreme Court in *Van Buren* reviewed the CFAA conviction of a police officer who used a law enforcement license plate database, to which he had authorized access for his official duties, to retrieve information unrelated to his job in exchange for money. The scheme—part of an undercover sting operation by the FBI—contravened police department policy which prohibited using the database for a non-law enforcement purpose such as personal use. The officer was subsequently charged and convicted for violating the CFAA by "exceed[ing] [his] authorized access" to access a computer.[2]

Prior to *Van Buren*, federal circuits were divided over the question of whether a person violates the CFAA when accessing information via a valid login or other legitimate authorization *for an improper purpose*. In its analysis, the Supreme Court applied a "gates-up-or-down" inquiry, holding that, for the purposes of the CFAA, "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." (emphasis supplied).[3] If an individual actually has authority to access files/folders in the computer (i.e. the gates are "up"), he cannot "exceed" authorized access by accessing those files/folders, *even if he accesses them for an improper purpose*, such as one that would violate an organization's explicit policies. The Court explained that both parties agreed that Van Buren actually had access to the police computer system, as well as the specific files/folders in question - i.e., the gates were up. According to the Court's interpretation:

> If 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.[4]

Overall, the Court's interpretation may limit the CFAA's application to those who gain access to computer systems or folders without permission, such as external or internal "hackers." Notably, the Court reserved the question of "whether this [gates-up-or-down] inquiry turns only on technological (or 'code-based') limitations on access, or instead also looks to limits contained in contracts or policies."[5] Still, individuals with permission to access data for a specific purpose, who then use their access to the information for a different, unauthorized purpose - like company employees obtaining and disclosing confidential and sensitive data to a competitor - may no longer be prosecuted under the CFAA and be the subject of related civil suits under the CFAA.

In today's technological age, most corporations – from large to small businesses – maintain network and platform access and use policies. These policies are meant to protect an organization's most valuable "crown jewels" – whether trade secrets, sensitive data, important IP, or other corporate assets. To date, corporations also generally have relied on broad policies governing permissible access and use by employees, contractors, and other legitimate "insiders" to such items on company networks. Prior to *Van Buren*, if such an insider violated an organization's use policy, he may have been subject to criminal prosecution and civil suit under the CFAA. *Van Buren* narrows the grounds on which an organization may civilly or criminally enforce its data access and use policies.

Without the threat of CFAA civil or criminal actions, companies who deal in sensitive or confidential data should take adequate steps to ensure they are protected under the new legal regime. This might include:

- Map and document where sensitive data, IP, and trade secrets reside on the network and review access restrictions surrounding them.
- Consider and document access restrictions to sensitive data from a technological ("code-based") perspective, as well as a contractual and written policy perspective.
- Review data use policies and contractual agreements for different categories of "insiders" who may have access to corporate networks, including employees, contractors, vendors, or others.
- Review the terms of service for public-facing websites or other external entry points to a company's digital infrastructure and consider whether additional measures are necessary, such as switching to gated access or monitoring the efforts of data scrapers to revoke their authorization.
- Review the terms of service or use agreements for electronic platforms or consumer applications.

ABOUT KING & SPALDING

Celebrating more than 130 years of service, King & Spalding is an international law firm that represents a broad array of clients, including half of the Fortune Global 100, with 1,200 lawyers in 22 offices in the United States, Europe, the Middle East and Asia. The firm has handled matters in over 160 countries on six continents and is consistently recognized for the results it obtains, uncompromising commitment to quality, and dedication to understanding the business and culture of its clients.

ABU DHABI	CHARLOTTE	FRANKFURT	LOS ANGELES	PARIS	SINGAPORE
ATLANTA	CHICAGO	GENEVA	MOSCOW	RIYADH	TOKYO
AUSTIN	DENVER	HOUSTON	NEW YORK	SAN FRANCISCO	WASHINGTON, D.C.
BRUSSELS	DUBAI	LONDON	NORTHERN VIRGINIA	SILICON VALLEY	

[1] *Van Buren v. United States*, No. 19-783 (U.S. June 3, 2021).
[2] 18 U.S.C. § 1030(a)(2).
[3] *See* https://www.supremecourt.gov/opinions/20pdf/19-783_k53l.pdf, at 20.
[4] *Van Buren*, No. 19-783 at 6.
[5] *Id*. at 13 n.8.