SULLIVAN & CROMWELL LLP

April 21, 2020

United States Supreme Court Grants *Certiorari* in *Van Buren* v. *United States*

Court Will Review Whether the Computer Fraud and Abuse Act Prohibits an Individual Who Is Authorized to Access Information on a Computer for Specific Purposes from Accessing that Information for an Improper Purpose

SUMMARY

Yesterday, the U.S. Supreme Court agreed to hear argument in the closely watched case of *Van Buren* v. *United States*, No. 19-783, which will have significant implications for employers protecting sensitive data and information. The appeal, which likely will not be decided until 2021, presents the question of whether Section (a)(2) of the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, which bars individuals from "exceed[ing] authorized access" to a computer, prohibits an individual who is authorized to access information on a computer for specific purposes from accessing that information for an improper purpose. This case will allow the Supreme Court to address an issue of law that has caused a significant split between the First, Fifth, Seventh, and Eleventh Circuits, which interpret Section 1030(a)(2)'s prohibition to apply to individuals who exceed their authorized access by obtaining information on a computer for an improper purpose, and the Second, Fourth, and Ninth Circuits, which interpret Section 1030(a)(2) to cover only cases where individuals access information on a computer which they had no right to access for any purpose.

BACKGROUND

Section (a)(2) of the CFAA proscribes "intentionally access[ing] a computer without authorization or exceed[ing] authorized access, and thereby obtain[ing] . . . information from any protected computer."[1] The CFAA further defines "exceeds authorized access" as "access[ing] 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."[2] The CFAA provides for both criminal and civil liability for a violation of the statute.[3]

In 2015, an FBI sting operation targeted Georgia police sergeant Nathan Van Buren after he solicited a loan from an individual (the Informant) that Van Buren had met in his capacity as a police officer.[4] As part of the sting, the Informant offered Van Buren money in exchange for Van Buren undertaking a computer search to determine whether a purported female acquaintance of the Informant was an undercover officer.[5] Van Buren agreed to conduct the search and ran what he believed to be the woman's license plate number through the Georgia Crime Information Center (GCIC) database, a government database maintained by the Georgia Bureau of Investigation (GBI).[6] The following day, the FBI and GBI interviewed Van Buren, at which time he confessed both to conducting the search and to knowing that its purpose was to learn whether the woman was an undercover officer.[7] Ultimately, Van Buren was tried and convicted of violating the CFAA and honest-services wire fraud in the United States District Court for the Northern District of Georgia.[8]

On appeal, Van Buren argued that he did not "exceed[] authorized access," within the meaning of Section 1030(a)(2), because he was authorized as a police officer to access the GCIC database.[9] Van Buren distinguished his improper *use* of the GCIC database from his legitimate right to access it.[10] While recognizing that the Eleventh Circuit had taken the contrary position in *United States* v. *Rodriguez*, 628 F.3d 1258, 1260 (11th Cir. 2010), Van Buren emphasized the Circuit split on the issue and asked the Circuit to revisit its earlier decision.[11]

In affirming Van Buren's CFAA conviction, the Eleventh Circuit relied upon *Rodriguez* as binding precedent and explained that neither the Circuit split[12] nor Van Buren's disagreement with *Rodriguez* rendered the decision inapposite.[13] The court acknowledged, however, the public policy concerns identified by the Circuits that have taken the contrary position.[14] These Circuits have reasoned that interpreting Section 1030(a)(2) to apply more broadly to include situations where an individual *uses* information for an improper purpose that he is otherwise entitled to access (such as in *Van Buren*) could transform ordinary violations of an employer's computer-use policy, such as an employee utilizing his or her work computer for personal use, into federal crimes.[15] As a result, these Circuits have interpreted Section 1030(a)(2) more narrowly to apply only where an individual *accesses* information that he has no authorization to access under any circumstances – for example, by hacking into a computer.

IMPLICATIONS

The U.S. Supreme Court's eventual decision may resolve the deep Circuit split on this issue, with significant implications for federal law enforcement and employers around the country. The ultimate decision may impact law enforcement's ability to prosecute individuals who access confidential, sensitive, and proprietary information for an improper purpose, as well as companies' efforts to vindicate their rights in civil litigation as a result of that conduct.

If the U.S. Supreme Court upholds the Eleventh Circuit's decision in *Van Buren*, federal law enforcement can criminally prosecute and employers can pursue civil claims under the CFAA against individuals and entities that misuse their authorized access to confidential and proprietary information for a purpose that

violates the terms or scope of their authorization. While Van Buren and those who have filed *amicus* briefs on his behalf claim that such a result would expand the CFAA from a tool to combat hacking into a mechanism for overbroad policing of computer usage,[16] the Justice Department has argued that such fears are unfounded given that the CFAA has not been used in the First, Fifth, Seventh, or Eleventh Circuits to prosecute "commonplace activities" that violate "private computer-use policies."[17] The Justice Department maintains that affirming *Van Buren* would allow law enforcement to punish, and private employees to seek redress for, the misappropriation of "proprietary or confidential information for forbidden uses,"[18] as well as the exploitation of security flaws and vulnerabilities in company computer systems.

For law enforcement and private entities operating in the Second, Fourth, or Ninth Circuits, a decision by the Supreme Court to affirm Van Buren's conviction may open a previously unavailable avenue for holding individuals accountable for their misuse of others' computer systems, which may be significant in certain contexts. For example, it may enable an employer to seek redress where it may otherwise have been difficult to prove that an employee has violated other applicable statutes, such as misappropriation of trade secrets, by accessing or stealing confidential, proprietary information. Should the Supreme Court interpret § 1030(a)(2) of the CFAA as the Justice Department suggests, an employee that accesses such information—even if permitted to do so by his or her employment policy—with the intent to misappropriate it or utilize it outside of the ambit of his or her employment, could be criminally or civilly liable. The Supreme Court's decision can be expected to bring much-needed clarity to this particularly important and heavily litigated provision of the CFAA.

* * *

ENDNOTES

1 18 U.S.C. § 1030(a)(2). The CFAA's "without authorization" prong penalizes the invasion of computer systems to which an individual has no right of access, which often includes "hacking" committed by unknown third parties.

2 18 U.S.C. § 1030(e)(6).

3 18 U.S.C. § 1030(c).

4 *United States* v. *Van Buren*, 940 F.3d 1192, 1197 (11th Cir. 2019).

5 *Id.*

6 *Id.* at 1198.

7 *Id.*

8 *Id.*

9 Reply Brief at 12, *Van Buren*, 940 F.3d 1192 (11th Cir. 2019) (No. 18-12024).

10 *Id.*

11 *Id.* at 12–13.

12 *See, e.g.*, *United States* v. *Valle*, 807 F.3d 508, 523 (2d Cir. 2015) (concluding that the government and defendant's interpretations of the CFAA were each plausible and applying the rule of lenity to resolve doubts in favor of the defendant); *United States* v. *Nosal*, 676 F.3d 854, 862–63 (9th Cir. 2012) (holding that § 1030(a)(2) does not cover a person "who has unrestricted physical access to a computer, but is limited in the use to which he can put the information"); *WEC Carolina Energy Sols. LLC* v. *Miller*, 687 F.3d 199, 204 (distinguishing "improper *use*" from obtaining or altering information "that falls outside the bounds of [an individual's] approved access" to a computer) (emphasis in the original).

13 *Van Buren*, 940 F.3d at 1208.

14 *Id.*

15 *See, e.g.*, *Valle*, 807 F.3d at 528 ("While the Government might promise that it would not prosecute an individual for checking Facebook at work, we are not at liberty to take prosecutors at their word in such matters."); *see also Nosal*, 676 F.3d at 860 ("[U]nder the broad interpretation of the CFAA, such minor dalliances" as "[Google]-chatting with friends, playing games, shopping or watching sports highlights," "would become federal crimes" if done on a work computer.").

16 *See* Brief for Electronic Frontier Foundation, Center for Democracy & Technology, and New America's Open Technology Institute, as Amici Curiae Supporting Petitioner, at 14, *Van Buren* v. *United States*, No. 19-783; *see also* Petition for Writ of Certiorari at 12–13, *Van Buren*, No. 19-783.

17 Brief in Opp. to Writ of Certiorari at 15–16, *Van Buren*, No. 19-783. The Justice Department also argued that private civil suits for "trivial" conduct were unlikely given that § 1030(g) prohibits private civil suits unless damages exceed $5,000. *Id.* at 18.

18 *Id.*

ABOUT SULLIVAN & CROMWELL LLP

Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 875 lawyers on four continents, with four offices in the United States, including its headquarters in New York, four offices in Europe, two in Australia and three in Asia.

CONTACTING SULLIVAN & CROMWELL LLP

This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers listed below, or to any other Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future publications by sending an e-mail to SCPublications@sullcrom.com.

CONTACTS

New York		
H. Rodgin Cohen	+1-212-558-3534	cohenhr@sullcrom.com
Mitchell S. Eitel	+1-212-558-4960	eitelm@sullcrom.com
John Evangelakos	+1-212-558-4260	evangelakosj@sullcrom.com
Jared M. Fishman	+1-212-558-1689	fishmanj@sullcrom.com
Nicole Friedlander	+1-212-558-4332	friedlandern@sullcrom.com
Scott D. Miller	+1-212-558-3109	millersc@sullcrom.com
Sharon L. Nelles	+1-212-558-4976	nelless@sullcrom.com
Matthew A. Schwartz	+1-212-558-4197	schwartzmatthew@sullcrom.com
Alexander J. Willscher	+1-212-558-4104	willschera@sullcrom.com
Michael M. Wiseman	+1-212-558-3846	wisemanm@sullcrom.com
Washington, D.C.		
Julia M. Jordan	+1-202-956-7535	jordanjm@sullcrom.com
Aisling O'Shea	+1-202-956-7595	osheaa@sullcrom.com
Los Angeles		
Anthony J. Lewis	+1-310-712-6615	lewisan@sullcrom.com
Robert A. Sacks	+1-310-712-6640	sacksr@sullcrom.com
Palo Alto		
Nader A. Mousavi	+1-650-461-5660	mousavin@sullcrom.com
Sarah P. Payne	+1-650-461-5669	paynesa@sullcrom.com