SULLIVAN & CROMWELL LLP

S&C memo

June 4, 2021

U.S. Supreme Court Narrows the Scope of Federal Anti-Hacking Law in *Van Buren* v. *United States*

Court Holds That the Computer Fraud and Abuse Act Does Not Apply to an Individual Who Is Authorized to Access Information on a Computer but Does So for an Improper Purpose

SUMMARY

Yesterday, the U.S. Supreme Court ruled in *Van Buren* v. *United States* that Section (a)(2) of the federal Computer Fraud and Abuse Act (CFAA), which bars an individual from "exceed[ing] authorized access" to information on a computer network, does not apply to cases where an individual is generally authorized to access the information, but does so for an unauthorized or improper purpose. Instead, the Court interpreted Section (a)(2) to apply only to cases where an individual accesses information that the individual has no authority to access for any purpose. In so holding, the Court resolved a split between various federal Courts of Appeals on this issue. The decision has significant implications for law enforcement and the private sector, and particularly for employers in situations where employees access confidential or proprietary information for an unauthorized or improper purpose.

While the holding forecloses an avenue that employers and law enforcement have used to address misuse of computer systems, other statutes remain available that may address this type of harm, and there are steps that may be taken in light of the decision that may continue to allow redress under the CFAA where employees take confidential or proprietary information without authorization. These steps include revising employment policies or agreements to make clear the data or areas of a network to which an individual does not have access, and implementing electronic security tools to prohibit that access. In addition, the decision may lead to renewed advocacy for a legislative solution that would amend the CFAA to address certain types of misconduct that the Court found the statute as currently drafted does not cover.

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 [using] 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 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, and 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 authority to access it.[10] While recognizing that the Eleventh Circuit had taken a contrary position in *United States* v. *Rodriguez*, 628 F.3d 1258, 1260 (11th Cir. 2010), Van Buren cited decisions supporting his argument from other Courts of Appeal and asked the Eleventh 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 contrary rulings by other Courts of Appeal[12] nor Van Buren's disagreement with *Rodriguez* rendered *Rodriguez* inapposite.[13] The Eleventh Circuit acknowledged, however, the public policy concerns identified by the Circuits that took the contrary position.[14] The Supreme Court granted *certiorari* to resolve the Circuit split.

THE COURT'S DECISION

In a 6-3 decision authored by Justice Barrett (Justice Thomas, joined by Chief Justice Roberts and Justice Alito, dissented), the Supreme Court reversed the decision of the Eleventh Circuit and adopted the narrower interpretation of the CFAA that Van Buren advocated. In so doing, the Court held that an individual "exceeds authorized access" "when he accesses a computer with authorization but then obtains information located in particular areas of the computer . . . that are off limits to him."[15]

The majority focused on a textual analysis of the CFAA's "exceeds authorized access" definition.[16] As part of that analysis, the Court rejected the Government's argument that the plain meaning of the statutory text prohibits accessing "information one was not allowed to obtain in the particular manner or circumstances in which he obtained it."[17] The majority reasoned instead that to determine whether Van Buren was "entitled so to obtain" the information he retrieved from the law enforcement database, the only relevant question under the CFAA is whether Van Buren was authorized to access the database. In the Court's view, the text of the CFAA does not provide for an analysis of the circumstances of an individual's access if the access is authorized.[18]

The majority also rejected the Government's invitation to consider the negative policy implications of a narrower reading of the "exceeds authorized access" prong.[19] Instead, the Court noted that, under the Government's interpretation, the CFAA would "attach criminal penalties to a breathtaking amount of commonplace computer activity."[20] The Court emphasized that its textual analysis alone provided a sufficient basis for its holding, but described as "extra icing on a cake already frosted" that its ruling avoids an interpretation of the CFAA that, in the Court's view, would transform ordinary violations of computer-use policies into federal crimes.[21]

IMPLICATIONS

The Court's decision forecloses the imposition of criminal or civil liability on individuals accessing information for an improper purpose if they were otherwise authorized to access that information for proper purposes. Prior to this decision, the CFAA had been used for many years both by federal law enforcement authorities and private companies, particularly employers, to hold individuals accountable in this context. Nonetheless, there are other avenues that both law enforcement and private entities may pursue to address the improper use of information that an individual is authorized to access for certain limited purposes.

First, the decision leaves intact the CFAA's prohibition of unauthorized access to a computer network—traditional hacking by an outsider—as well as instances where an individual has permission to access a computer network, but is barred from accessing information stored in a particular location on the network for any purpose (hacking by an insider). Consequently, employers and other entities concerned with the security of sensitive information can take steps to increase the likelihood that they will have recourse under the CFAA in certain circumstances by (i) adopting company policies that narrowly limit the users who have access to that information, and (ii) employing software and other electronic barriers that prohibit employees from accessing particular data or areas of the network.

Second, following the *Van Buren* decision, there is likely to be renewed reliance on other federal and state statutory or common law provisions to establish both criminal and civil liability for improper use of information that an individual is authorized to access. Van Buren, for example, was charged with honest-services wire fraud for engaging in the same conduct underlying his conviction for violating the CFAA.[22] Other statutes like the Defend Trade Secrets Act, which provides criminal and civil liability for theft of certain

proprietary information, as well as identity theft and state privacy laws, remain available to address such conduct. Employers should consider whether the narrowing of the CFAA and the potential need to rely on other statutes to address employee misconduct—for example when an employee departs with sensitive proprietary information—warrant changes to their employment and non-disclosure agreements.

Third, the emphasis on interpretation of the statutory text, as well as certain questions posed during oral argument, signal that the fight for a more expansive CFAA statute may not end at the Supreme Court. As Van Buren argued, there are already legislative proposals for amending the CFAA to more clearly target conduct like the acts committed by Van Buren without sweeping in a broad array of more innocuous conduct by employees. For example, a revised statute could, as Justice Sotomayor suggested during oral argument, limit the coverage of the CFAA's "exceeds authorized access" prong to instances where the individual accessed information that the individual would otherwise be entitled to access, but for the purpose of personal pecuniary gain. Regardless of the particular approach to any revision, the Court's decision in *Van Buren* is likely to enhance interest in enacting such an amendment or finding a legislative solution to a common and significant problem for employers across industries.

* * *

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's 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 *Van Buren* v. *United States*, 593 U.S. ___, 20 (2021).

16 *Id.* at 5.

17 *Id.* at 6.

18 *Id.* at 8.

19 *Id.* at 5.

20 *Id.* at 17.

21 *Id.* at 17–19.

22 Van Buren's honest-services wire fraud conviction was subsequently overturned by the Eleventh Circuit for unrelated reasons. *Id.* at 4n1.

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 or to any 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.