Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

The Big CFAA Questions High Court Is Considering

By **Mark Krotoski and Jonathan Justl** (December 2, 2020, 5:27 PM EST)

Mark Krotoski

Jonathan Justl

On Monday, the U.S. Supreme Court heard oral arguments in Van Buren v. U.S., a case that will be of interest to any company that provides or limits access to data to employees or insiders.

The case raises the question about what remedy the Computer Fraud and Abuse Act provides when an insider obtains information for an unpermitted purpose and personal benefit.

The case is expected to clarify under what circumstances insiders "exceed authorized access" to a computer that may result in a federal crime. The courts have divided on this issue for over a decade.[1]

CFAA Background

Enacted in 1984,[2] the CFAA addressed the fact that no federal statute covered the area of computer crime and other statutes often did not apply.[3] In 1994, Congress added civil remedies.[4]

The CFAA prohibits an individual from "intentionally access[ing] a computer without authorization or exceed[ing] authorized access, and thereby obtain[ing] ... information" from the computer.[5] The first clause typically covers external actors who lack any authorization. The second clause generally applies to insiders who may be permitted access to a network and then exceed that authorized access.

Under the CFAA, "exceeds authorized access" refers "to access 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."[6] One U.S. Senate report notes this definition was added in 1986 to "simplify the language" and "substitute" for "the more cumbersome phrase … 'or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend.'"[7]

Facts of the Case

In Van Buren, a police sergeant with access to a restricted law enforcement database took money in

exchange for checking whether the database listed an individual as an undercover officer. At trial, a jury convicted him on two counts under the CFAA and for honest-services wire fraud. The U.S. Court of Appeals for the Eleventh Circuit affirmed the CFAA conviction and reversed and remanded the second based on instructional error.

The panel rejected Van Buren's argument that "he is innocent … because he accessed only databases that he was authorized to use, even though he did so for an inappropriate reason."[8] The conviction was supported by evidence that the database was "supposed to be used for law-enforcement purposes only and that officers are trained on the proper and improper uses of the system."[9] Van Buren also confessed "that he knew it was 'wrong' to run the [vehicle license] tag search and that he had done so for money."[10]

The sergeant had authority to access the database to perform his official duties. However, did he "exceed[] authorized access," and violate the CFAA, by searching the database outside the scope of his official duties for personal financial gain?

Briefing Arguments

Van Buren argues no. Conceding that he had "an inappropriate reason" to access the database, he contends the statute applies only if the person obtaining access had no right of access for any purpose.[11]

He argues that the phrase "not entitled so to obtain or alter" does not reach misuse or misappropriation of information.[12] He contends that employers and websites' terms of service often impose access restrictions, and that adopting a broad view of the CFAA would produce a sweeping expansion of federal criminal jurisdiction to cover common breaches on access restrictions such as checking sports scores on a work computer.[13]

He submits that the CFAA covers only "unauthorized computer hacking" and "was never meant to become a vehicle for enforcing private or public restrictions on the use of data."[14]

The U.S. argues yes. Disagreeing with Van Buren that the CFAA only reaches hackers, the U.S. contends that the statute and legislative history confirm the CFAA reaches corrupt "insiders" through the "exceeds authorized access" provision.[15]

The U.S. contends that "[a] person who 'use[s]' his authorized computer access 'to obtain or alter information in a computer' is 'entitled so to obtain or alter' that information only when he is authorized to do so under the circumstances."[16] Van Buren "indisputably was not," and his conduct falls within the "heartland" of the CFAA's prohibition on unauthorized access by insiders.[17]

The U.S. further contends that the rule of lenity does not apply because the statutory text is not ambiguous, and the hypotheticals about criminalizing trivial web surfing have no bearing.[18]

Oral Argument

Both sides received sharp questioning at Monday's argument. Justices Clarence Thomas and Amy Coney Barrett asked Jeffrey L. Fisher, counsel for Van Buren, whether "authorization" also included a scope of use component.[19] Counsel responded that the statute contains no language suggesting the scope of permitted uses or purposes for which an employee obtained information were relevant.[20]

Justice Stephen Breyer questioned Van Buren's counsel about whether the 1986 revisions to the statute, deleting the reference to "purposes," was intended to remove considerations of an insider's purposes in accessing information.[21] Counsel argued that another report suggested the 1986 amendment evidenced an intent to change the statute's reach, and the legislative history was conflicting.[22] He then stated it was dangerous to use legislative history to resolve ambiguity in a criminal statute given the rule of lenity.[23]

Justice Samuel Alito expressed concern that Van Buren's reading could exclude insiders who exploit access to highly sensitive personal information such as credit card numbers.[24] The petitioner's counsel answered that Congress' concern was hacking and Congress should decide as a matter of policy whether to expand the statute.[25] He later added that other federal statutes could reach misuse of personal information in some circumstances, such as trade secret misappropriation and the federal wire fraud statute.[26]

One line of questioning focused on whether a "parade of horribles" involving other hypothetical applications of the statue, beyond the facts, would influence the court's consideration.[27] Justice Thomas asked for some "actual examples" in the Eleventh Circuit. Counsel for Van Buren could not identify any in the Eleventh Circuit but noted two cases in the briefs.[28] Counsel warned against "constru[ing] a statute simply on the assumption the government will use it responsibly."[29]

In response to Justice Neil Gorsuch's request to the petitioner's counsel to "explain to us what the constitutional implications are of your parade," counsel referred to a First Amendment issue (concerning the right to use "fictitious online profiles for benign reasons")[30] and a vagueness issue based on the range of conduct subject to the statutory language "under the circumstances to obtain."[31] Counsel contended that the statute does not give fair notice to users that their conduct was illegal based on the statute's vagueness.[32]

Justice Elena Kagan questioned Van Buren's counsel about what the word "so" meant in the phrase, "not entitled so to obtain or alter."[33] He responded that it meant the user obtained the information via a computer as opposed to another means.[34]

Eric J. Feigin, deputy solicitor general, argued that the word "authorization" in the CFAA limited its reach and only applied when an insider received authorization through "individualized consideration."[35]

Responding to Chief Justice John Roberts' and Justice Breyer's questions, he contended that the lack of individualized permission meant that the CFAA would not reach everyone who violates a website's terms of service or a computer use policy.[36] Justice Sonia Sotomayor stated that this limitation was nowhere in the statute, and the word "so" in the statute's phrase, "entitled so to obtain or alter," does not "get around the ambiguity."[37] Disagreeing, counsel answered a later question from Justice Kagan by stating, "It would be a much tougher case for us without the word 'so'" in the statute.[38]

Justice Thomas questioned the U.S. about the impact of the 1986 amendments. Counsel responded that it simply clarified its scope without expanding it.[39] Counsel contended that the 1986 amendments deleted the 1984 reference to "purposes" merely to clarify that the reasons for an authorization (e.g., why a particular person received authorization to access information) were irrelevant.[40]

Justice Alito expressed that this case was "very difficult" and asked if additional briefing would be helpful to define the terms with greater precision.[41] Counsel for the U.S. declined the invitation noting

the meaning of the statute was "quite clear" and Van Buren offered the false choice between his interpretation and eliminating all privacy protection the statute provides.[42]

Justice Gorsuch inquired whether other statutes arguably applied to the facts and noted the "rather long line of cases in recent years in which the government has consistently sought to expand federal criminal jurisdiction."[43] Counsel answered that the government saw this case as "exactly the kind of misconduct that the statute was aimed at, because the police officer is abusing his trust."[44]

Potential Implications

The case will clarify the scope and application of the CFAA and determine whether the CFAA provides a remedy where an insider accesses a computer beyond the scope of his authority and for personal benefit. The ruling could have significant implications for organizations limiting access to data.

For instance, a recurring question confronting employers is what remedies are available for employees using their network access to obtain information for their personal benefit, to benefit new employers by accessing their prior employer's network after their departure, or to damage or harm their employers. The outcome of the case may answer whether, and to what extent, the CFAA provides a criminal or civil remedy for that recurring scenario.

Ironically, the CFAA was first enacted to address the gap in "the area of computer crime."[45] If the court decides that the CFAA does not apply to the facts of the case, then there will be no remedy under the primary federal computer statute.

The petitioner's counsel contended other statutes may apply to fill the gap. However, common statutes — such as the federal trade secret, interstate transportation of stolen property, or wire or mail fraud statutes — frequently do not apply to the facts or are an imperfect fit.

For example, for trade secret theft, the information must qualify as a trade secret.[46] Sensitive health, banking or government information, for example, typically does not qualify as a trade secret. If there is no fraud scheme or material misrepresentation, the mail and wire fraud statutes do not apply.[47] Courts are reluctant to apply the interstate transportation of stolen property statute to intangible property such as data.[48] For most factual scenarios involving insider access to data, other federal statutes typically do not apply, or if they do, are a cumbersome fit to the facts creating jury presentation issues.

Resolution of the current circuit split will provide for even application of the CFAA across the country. Under the existing circuit split, whether a remedy is available under the insider scenario depends on which jurisdiction the access to the computer occurred.

Other questions the U.S. Supreme Court may answer are who determines whether access is authorized; to what extent subjective knowledge of authorization matters; and how clear authorization must be. Those are not always easy questions as illustrated during the oral argument.

The opinion likely will address other significant questions including: Under what circumstances can companies, organizations and government agencies enforce access restrictions on information and data under the CFAA? Under the statute, when is authorized access to a computer exceeded? Do employees who intentionally violate their employers' computer policies exceed authorized access under the CFAA? What is the scope of the CFAA for criminal and civil cases?

The Supreme Court's interpretation of the CFAA will likely leave some constituencies dissatisfied and could create pressure for Congress to revise or supplement the statute.

If the court adopts Van Buren's reading, employers may pressure Congress to enact a new statute to fill the gap by providing a criminal and civil remedy against insiders who use their access for improper purposes. Conversely, the adoption of the U.S. reading could create pressure for Congress to clarify that the CFAA does not criminalize common unauthorized uses of work computers (such as web surfing, checking email, reading sports scores).

The decision also may provide impetus for a general overhaul of the CFAA to account for changes since the statute's enactment in 1984 in computer usage and interconnectivity.

Mark Krotoski is a partner and Jonathan Justl is a senior associate at at Morgan Lewis & Bockius LLP.

[1] For a discussion of the circuit split, see M. Krotoski & A. Adler, High Court May Offer Crucial Clarity On Computer Fraud Law, Law360 (May 15, 2020).

[2] See Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, Tit. II, §§ 2101-2102, 98 Stat. 2190-2192.

[3] H.R. Rep. No. 894, 98th Cong., 2d Sess. 6 (1984) [hereinafter "1984 House Report"]; see also S. Rep. No. 432, 99th Cong., 2d Sess. 2 (1986) (recounting history) [hereinafter "1986 Senate Report"].

[4] 18 U.S.C. § 1030(g); see also Pub. L. 103–322, title XXIX, § 290001(b)–(f), Sept. 13, 1994, 108 Stat. 2097– 2099 (codifying 18 U.S.C. § 1030(g) (civil private right of action).

[5] 18 U.S.C. § 1030(a)(2)(C).

[6] Id. § 1030(e)(6).

[7] 1986 Senate Report, at 9 (citation omitted).

[8] United States v. Van Buren, 940 F.3d 1192, 1208 (11th Cir. 2019).

[9] Id.

[10] Id.

[11] Br. for Petitioner 13, 17-23.

[12] Id. at 17-19.

[13] Id. at 2.

[14] Id. at 3.

[15] Br. for the United States 2-3, 12.

[16] Id. at 18.

[17] Id. at 13, 18.

[18] Id. at 15.

[19] Tr. of Oral Arg. in No. 19-783, p. 10:24-11:9; 32:6-9.

[20] Id. 11:13-19; 32:10-16.

[21] Id. 12:4-13.

[22] Id. at 12:19-13:6; see also Reply Br. for Petitioner 8 (citing S. Rep. No. 99-432, at 20-21 (1986)).

[23] Tr. of Oral Arg. in No. 19-783, p. 13:21-14:1.

[24] Id. 14:9-20.

[25] Id. 14:24-15:10.

[26] Id. 18:3-11; 26:15-27:11.

[27] Id. 8:22, 15:24, 22:4-7, 23:4-6, 24:17-19, 39:6-7, 47:11-12 48:2-3, 64:3.

[28] Id. 8:22-25-9:1-10.

[29] Id. 9:21-22.

[30] Br. for Petitioner 37.

[31] Tr. of Oral Arg. in No. 19-783, p. 23:10-25-24:1-15.

[32] Id. 24:10-15.

[33] Id. 20:18-19.

[34] Id. 20:23-25.

[35] Id. 38:12.

[36] Id. 36:24-37:10; 42:11-43:19.

[37] Id. 48:19-21; 49:17-19.

[38] Id. 52:7-9.

[39] Id. 41:3-16.

[40] Id. 41:17-25.

[41] Id. 46:12-25.

[42] Id. 47:5-17.

[43] Id. 54:6-10.

[44] Id. 55:22-56:1.

[45] 1984 House Report, at 6.

[46] 18 U.S.C. § 1839(3) (defining trade secret).

[47] Id. §§ 1341, 1343.

[48] Id. § 2314; see, e.g., United States v. Aleynikov, 676 F.3d 71, 78-79 (2nd Cir. 2012) (reversing ITSP conviction based on the theft and uploading of source code of Goldman Sachs & Co. as "purely intangible property embodied in a purely intangible format").