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

CFAA And The High Court's Fight Against Overcriminalization

By **Harry Sandick and Jacob Chefitz** (June 6, 2021, 11:58 AM EDT)

Harry Sandick

Jacob Chefitz

On June 3, the U.S. Supreme Court decided Van Buren v. United States, holding that the Computer Fraud and Abuse Act, or CFAA, only reaches computer users "who obtain information from particular areas in the computer ... to which their computer access does not extend."[1]

The court rejected the government's more expansive interpretation, which would have punished people who "have improper motives for obtaining information that is otherwise available to them."[2] The court ruled in the defendant's favor by a 6-3 vote, in an opinion by Justice Amy Coney Barrett.

In Van Buren, the court confronted a notoriously broad and somewhat out-of-date 1986 statute.

When confronted with a statute like this, one that is ambiguously worded and not tailored to the realities of the present day, it is important for the judiciary to read the statute in a manner that advances sound policy and does not provide prosecutors with the discretion to prosecute ordinary, innocent conduct.

The Van Buren majority agreed and declined the government's offer to "attach criminal penalties to a breathtaking amount of commonplace computer activity."[3]

In so ruling, the court continued a recent trend of limiting the reach of the criminal law and not "constru[ing] a criminal statute on the assumption that the Government will 'use it responsibly.'"[4]

Background

The government charged Nathan Van Buren, a police sergeant in Georgia, with violating the CFAA, which imposes criminal liability on anyone who "intentionally accesses a computer without authorization or exceeds authorized access."[5]

Van Buren had asked an acquaintance, Andrew Albo, for a personal loan. Albo, however, secretly recorded his conversation with Van Buren, and brought it to the attention of the local sheriff's office.

The matter eventually found its way to the FBI, which devised a sting operation: Albo would ask Van

Buren to search the state law enforcement computer database — to which Van Buren had access as a police sergeant — for a license plate purportedly belonging to a woman whom Albo had met at a local strip club. Albo would tell Van Buren that he wanted to ensure that the woman was not an undercover cop, and he would offer to pay Van Buren $5,000 for the search. Van Buren agreed, entered the database, searched for the license plate, and reported back to Albo.

After a jury trial, Van Buren was convicted and sentenced to 18 months in prison.

Van Buren appealed to the U.S. Court of Appeals for the Eleventh Circuit, arguing that he had not violated the CFAA because a computer user "exceeds authorized access" only by accessing information beyond the scope of the user's access rights, not by misusing information to which the user otherwise has access. Because he did have a right to access the law enforcement computer database — he just used that access for a prohibited purpose — Van Buren argued that the CFAA did not apply to him.

The government disagreed. The Eleventh Circuit affirmed the conviction[6] but acknowledged that a circuit split existed as to the meaning of the CFAA's "exceeds authorized access" clause. The Supreme Court granted certiorari to resolve the circuit split.

The Supreme Court's Opinion

In an opinion by Justice Barrett, the court adopted Van Buren's interpretation, holding that one "exceeds authorized access" under the CFAA "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."[7]

Justice Clarence Thomas dissented, joined by Chief Justice Roberts and Justice Samuel Alito.

The majority, unsurprisingly, began with the plain text of the statute. The CFAA defines the phrase "exceeds authorized access" as "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."[8]

The key word, the majority explained, is "so." That word, the majority reasoned, is "a term of reference," and thus the phrase "so to obtain" means to obtain in "the same manner as has been stated."[9] That manner is "via a computer one is otherwise authorized to access," and therefore the phrase "is not entitled so to obtain" must be read as "not allowed to obtain by using a computer that he is authorized to access."[10]

But while grounding its ruling in the statute's plain language, the majority refused to ignore the consequences of the government's preferred reading, explaining that those consequences are "extra icing on a cake already frosted."[11] Under the government's preferred interpretation, the CFAA would "criminalize everything from embellishing an online-dating profile to using a pseudonym on Facebook,"[12] or even just checking sports scores on a work computer without an employer's permission.

The majority was unwilling to accept that "millions of otherwise law-abiding citizens are criminals,"[13] noting that the government's current CFAA charging policy gives federal prosecutors the discretion to prosecute any CFAA violation, no matter how small.

In dissent, Justice Thomas rejected the majority's plain meaning analysis, arguing that the statutory text

supported the government and that basic principles of property law indicate that one is not entitled to obtain information for an unauthorized purpose. Justice Thomas criticized the majority's concern that the government's interpretation would criminalize a broad swath of commonplace activity. On Justice Thomas's reading, many provisions of the CFAA, such as its intent requirement, limit its scope. Discomfort with the expansive scope of federal criminal law, Justice Thomas chided, is not a ground for altering statutes.

Takeaways

There are several big-picture takeaways from the court's decision.

The reach of the CFAA has been curtailed.

After Van Buren, the government will not be able to use the CFAA to prosecute some of the types of cases that it has prosecuted in the past. The CFAA still can be used by prosecutors to punish those who hack into computers or those who use their permitted access to get information from other parts of the computer system to which their access does not extend. But it will no longer be able to prosecute people like Van Buren who use their authorized access to the computer system for a malign purpose — such as the selling of law enforcement data. In several circuits, this means that some people who could have been prosecuted now will not.

Immediate impact on active cases.

Ongoing investigations that go beyond what Van Buren permits will be terminated without charges, and convictions that have not reached a final, unappealable judgment will be reversed and dismissed. It is not clear whether this decision will help those previously convicted of CFAA violations. In the time since Van Buren was handed down, commentators have pointed to prior cases in which the CFAA was used by prosecutors in an unfair manner, most notably the tragic case of Aaron Swartz, who was unjustly prosecuted by the District of Massachusetts.[14]

The Supreme Court continues to protect defendants from prosecutors' tortured or extreme readings of federal criminal statutes.

Beyond the CFAA itself, Van Buren continues a recent trend of Supreme Court decisions limiting the scope of broadly written criminal statutes and reining in the vast prosecutorial discretion that comes with them. While these decisions generally begin with the plain meaning of the text, they do not shy away from their real-world consequences and in fact take them quite seriously.

This trend can be traced at least as far back as the court's 2014 decision in Bond v. United States, in which the court refused to interpret the Chemical Weapons Convention Implementation Act of 1998 to cover "a jilted wife's [attempt] to injure her husband's lover" by putting lab chemicals on a doorknob.[15]

The following year, in Yates v. United States, the court again struck back at what Justice Elena Kagan, dissenting, described as the "overcriminalization and excessive punishment in the U.S. Code," holding that throwing a fish off a boat does not count as destroying a "record, document, or tangible object" under the Sarbanes-Oxley Act.[16]

More recent cases have brought this trend into sharper focus. In its 2018 decision in Marinello v. United

States, the court limited the reach of the tax obstruction statute by requiring the government to prove that the defendant was aware of a pending tax-related proceeding, like an audit, or could reasonably foresee such a proceeding, at the time when he engaged in the obstructive conduct.

And last term, in Kelly v. United States, the court unanimously reversed the wire fraud convictions in the Bridgegate scandal, with Justice Kagan writing that to hold otherwise would be "a sweeping expansion of federal criminal jurisdiction."[17]

Van Buren is the latest iteration of this trend. It is a continuation of the court's ongoing project of narrowing the scope of broad criminal statutes and wresting discretion from the hands of overzealous prosecutors.

Defense counsel should challenge how prosecutors apply federal criminal law.

Van Buren likely won't be the last time that the Supreme Court is called upon to narrow the reach of the federal criminal code. As Justice Thomas noted in his Van Buren dissent, "[m]uch of the Federal Code criminalizes common activity."

Congress itself has generally shown little appetite or ability to address the issue. Indeed, the CFAA has long been criticized as an ambiguous and outdated statute, yet it took a case like Van Buren to remedy it. Congress can always amend statutes like the CFAA, but recent history suggests that's a long shot, and more cases like Bond, Yates, Marinello, Kelly and Van Buren can be expected.

Another possible target is the so-called right-to-control theory of mail and wire fraud prosecution, which allows the conviction of someone for property fraud even where the object of the crime only is to deprive the victim of his right to control property — a theory with no grounding in the text or structure of the statute and which allows commonplace conduct to lead to criminal prosecution.[18]

Conclusion

As Justice Kagan recognized in her dissent in Yates and her majority opinion in Kelly, we have seen rampant overcriminalization in recent decades, with prosecutors taking advantage of broadly written statutes that are only rarely revisited by Congress, and using them to prosecute people whose conduct is at the outer bound of what the text of the criminal law prohibits.

Van Buren is a continuation of the court's ongoing project of drawing certain lines:

- Not all bad conduct is criminal — there are other remedies for someone like Van Buren who abuses their power;

- Don't depend on the wise discretion of prosecutors when a statute could be used to criminalize innocent conduct — that's a dangerous guiding principle in a free country; and

- Don't lose sight of a decision's practical impact, even in an era of textualism.

Harry Sandick is a partner and former federal prosecutor, and Jacob Chefitz is an associate, at Patterson Belknap Webb & Tyler LLP.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] Van Buren v. United States, No. 19-783 (U.S. June 3, 2021) ("Van Buren"), slip op. at 1.

[2] Id.

[3] Id. at 17.

[4] Marinello v. United States, 138 S. Ct. 1101, 1109 (2018) (quoting McDonnell v. United States, 136 S. Ct. 2355, 2372-73 (2015)).

[5] 18 U.S.C. § 1030(a)(2).

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

[7] Van Buren, slip op. at 20.

[8] 18 U.S.C. § 1030(e)(6).

[9] Van Buren, slip op. at 5-6.

[10] Id. at 6 (brackets and italics removed).

[11] Id. at 17 (quoting Yates v. United States, 574 U.S. 528, 557 (2015) (Kagan, J., dissenting)).

[12] Id. at 18.

[13] Id. at 17-18.

[14] Andrew Crocker & Kurt Opsahl, "Supreme Court Overturns Overbroad Interpretation of CFAA, Protecting Security Researchers and Everyday Users," Electronic Frontier Foundation (June 3, 2021) ("We remember the tragic and unjust results of the CFAA's misuse, such as the death of Aaron Swartz[.]"), found at https://www.eff.org/deeplinks/2021/06/supreme-court-overturns-overbroad-interpretation-cfaa-protecting-security

[15] Bond v. United States, 572 U.S. 844, 848 (2014).

[16] Yates v. United States, 574 U.S. at 569 (Kagan, J., dissenting).

[17] Kelly v. United States, 140 S. Ct. 1565, 1574 (2020) (citing Cleveland, 531 U.S. 12, 24 (2000)).

[18] Harry Sandick and Jared Buszin, "Justices Should Revisit 2nd Circuit Theory in NCAA Bribe Case," Law 360 (Feb. 3, 2021).