High Court Is Likely To Adopt 6th Circ.'s Narrow View Of CFAA

By **Jay Bogan** (October 1, 2020)


Jay Bogan

Loose language in a criminal statute conferring a private cause of action — such as the Computer Fraud and Abuse Act — presents an interpretative dilemma for courts.

The CFAA furthers the legitimate public interest in preventing and punishing computer fraud and abuse. But there is currently a circuit split as to what constitutes computer fraud and abuse under the CFAA, and the U.S. Court of Appeals for the Sixth Circuit recently deepened that split.

The concept of a scheme or artifice to defraud into the federal mail, wire and bank fraud statutes has been broadly interpreted to reach all sorts of dishonest conduct intended to separate a victim from his money or property.[1]

Based on the text of the CFAA, courts have articulated a number of plausible reasons to take an expansive view of computer fraud and abuse, so as to punish and provide civil remedies for the misuse of confidential information.[2]

But such an expansive view creates tension in the digital context addressed by the CFAA. An overly broad view of CFAA liability expands criminal liability and potentially criminalizes a wide range of conduct, such as using a work computer to participate in a National Collegiate Athletic Association March Madness pool.

In Royal Truck & Trailer Sales and Service Inc. v. Kraft, the Sixth Circuit added to the circuit split that has existed for roughly eight years by taking a narrow view of CFAA liability in a civil case.[3] That decision came on the heels of the U.S. Supreme Court's grant of certiorari in a criminal case, U.S. v. Van Buren, in which the U.S. Court of Appeals for the Eleventh Circuit reaffirmed the broad view of CFAA liability.[4]

The Sixth Circuit's Decision in Royal Truck

After discovering that two former sales employees had accessed its computer network and transferred confidential company information to their personal email accounts, Royal Truck brought suit against them, asserting claims under the CFAA. The U.S. District Court for the Eastern District of Michigan dismissed the CFAA claims. Royal Truck appealed, but the Sixth Circuit affirmed the dismissal.

Under the CFAA, a person who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains ... information from any protected computer ... shall be punished."[5] Although a violation gives rise to criminal liability, the CFAA also provides a private right of action, including in instances where a person suffers a "loss" over the course of a year "aggregating at least $5,000 in value."[6]

On appeal, Royal Truck conceded the former employees had authorization to access company data through their company email accounts, because they accessed the system while still employed. The question on appeal therefore focused on whether the two defendants exceeded authorized access by later misusing the data, in violation of Royal Truck's internal policies.

The CFAA defines "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."[7]

Construing this language and analyzing dictionary definitions of the terms "access," "authorization," and "obtain or alter," the Sixth Circuit concluded that the CFAA's plain language does not reach the misuse of data obtained through authorized access. According to the Sixth Circuit, "Section 1030(a)(2)'s aim, in other words, is penalizing those who breach cyber barriers without permission, rather than policing those who misuse the data they are authorized to obtain."[8]

The Sixth Circuit relied in part on the rule of statutory construction that "where Congress knows how to say something but chooses not to, its silence is controlling."[9] Congress knew how to say "exceeds unauthorized use" but chose not to do so when enacting the CFAA. As an example, the panel cited the statute requiring that federal agencies share homeland security information in a way that "ensure[s] that such information is not used for an unauthorized purpose."[10]

In the panel's view, the interpretation of the relevant statutory language led to a plain understanding of its terms, precluding liability in that case.[11] The Sixth Circuit also questioned whether there should be criminal liability under the CFAA "for conduct as pedestrian as checking one's private social media account on a work phone."[12]

The Eleventh Circuit's Decision in Van Buren

As a police officer in Georgia, Nathan Van Buren had access to an official government database maintained by the Georgia Bureau of Investigation — the Georgia Crime Information Center database.

While Van Buren was authorized to access the Georgia Crime Information Center database for legitimate law enforcement purposes, he accepted $6,000 from an individual to obtain information from the Georgia Crime Information Center for an illegitimate purpose — to look up information about someone Van Buren thought was a dancer the individual had met at a strip club. In fact, Van Buren had been caught in a sting operation set up by the Federal Bureau of Investigation.

Van Buren was indicted, tried and convicted by a jury of computer fraud under the CFAA. On appeal, he challenged the sufficiency of the evidence supporting his conviction. The panel determined, however, that his appeal essentially sought to overrule the Eleventh Circuit's decision in a prior case, U.S. v. Rodriguez.[13]

In Rodriguez, an employee of the Social Security Administration, in violation of SSA policy, accessed the SSA database for personal reasons to obtain information about seventeen different people. After being convicted of computer fraud under the CFAA, Rodriguez appealed, arguing the conviction should be reversed because he had authority to access the SSA database, even though he did so for an illegitimate purpose.

The Eleventh Circuit rejected the argument and affirmed the conviction, ruling Rodriguez had exceeded authorized access by obtaining personal information for a nonbusiness reason.[14]

While acknowledging the circuit split on the exceeds authorized access issue, the panel in Van Buren followed Rodriguez and affirmed Van Buren's conviction.

Supreme Court Grants Certiorari in Van Buren

Van Buren petitioned for a writ of certiorari, presenting the following question:

> Whether a person who is authorized to access information on a computer for certain purposes violates Section 1030(a)(2) of the Computer Fraud and Abuse Act if he accesses the same information for an improper purpose.

The Supreme Court granted the petition on April 20, thereafter setting the case for argument on Nov. 30.

I predict that the narrow view of CFAA liability will prevail.

Both the Eleventh Circuit (broad view) and the Sixth Circuit (narrow view) concluded that the plain language of the CFAA supported their respective positions.[15]

In my view, the only plain language argument that is persuasive supports the narrow view. A person authorized to access information is authorized to obtain that information, if only by reading the information. A person who simply accessed a computer system and memorized a phone number stored on the system — even if the person did so for a personal reason — cannot fairly be said to have exceeded authorized access.

A plain language interpretation leading to the narrow view, such as the Sixth Circuit's, more plausibly tracks the language and purpose of the statute than the Eleventh Circuit's interpretation, especially when viewed through the prism of the "where Congress knows how to say something but chooses not to" rule of statutory construction. Congress knows how to penalize the misuse of information. The fact that it did not employ "exceeds authorized use" language in the CFAA is significant.

And this is further supported by the fact that the CFAA's damages and loss provisions do not permit monetary relief for the misuse of information, as do trade secret misappropriation statutes.[16]

The en banc U.S. Court of Appeals for the Ninth Circuit in U.S. v. Nosal made a persuasive case that the CFAA is a hacking statute focused on computer trespass, rather than a statute dealing with the misuse of information obtained in the absence of a computer trespass.[17]

Section 1030(a)(2)(C) of the CFAA deals with two situations: where a person accesses a computer (1) without authorization or (2) exceeds authorized access.

The first situation is an outside hack, whereby a person breaks into another's computer system and accesses information the person had no right to access or obtain to begin with.

It is more plausible to interpret exceeds authorized access as an inside hack, thus treating without authorization and exceeds authorized access in a corresponding way. Otherwise, an exceeds authorized access case moves into a broader dimension of criminal, and civil, liability than a without authorization case.

And to the extent the CFAA's plain language does not support the narrow view, then it is ambiguous. Accordingly, the language should be narrowly construed under the rule of lenity, given that the CFAA is a criminal statute, even though it also provides a private right of action.[18]

Applying the rule of lenity makes particular sense given the legitimate concerns about basing criminal liability on internal company rules and policies, which often address innocuous misconduct, such as using employer-issued devices to surf the Internet for personal reasons, viewing personal email accounts while at work, or using a work computer to fill out a March Madness bracket.

Finally, the fact that the Supreme Court granted certiorari in a criminal case, which brings the rule of lenity into sharper focus, is another indicator the narrow view will prevail.

Jay F. Bogan III is a partner at Kilpatrick Townsend & Stockton LLP.

[1] See 18 U.S.C. §§ 1341, 1343, and 1344.

[2] See, e.g., United States v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010).

[3] Royal Truck & Trailer Sales and Service, Inc. v. Kraft, --- F.3d ---, No. 19-1235, 2020 WL 5406118 (6th Cir. Sept. 9, 2020).

[4] United States v. Van Buren, 940 F.3d 1192 (11th Cir. 2019), cert. granted, 206 L. Ed. 2d 822 (2020).

[5] 18 U.S.C. § 1030(a)(2)–(a)(2)(C).

[6] 18 U.S.C. § 1030(c)(4)(A)(i)(I).

[7] 18 U.S.C. § 1030(e)(6).

[8] 2020 WL 5406118, at *3.

[9] 2020 WL 5406118, at *3 (citations omitted).

[10] Id. (citing 6 U.S.C. § 482(b)(1), (b)(3)).

[11] Id. at *4.

[12] Id.

[13] Van Buren, 940 F.3d at 1207 (discussing United States v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010)).

[14] Rodriguez, 628 F.3d at 1263.

[15] Rodriguez, 628 F.3d at 1263; Kraft, 2020 WL 5406118, at *4.

[16] See 18 U.S.C. § 1030(e)(8), (11)).

[17] United States v. Nosal, 676 F.3d 854 (9th Cir. 2012) (en banc).

[18] See United States v. Valle, 807 F.3d 508 (2d Cir. 2015) (applying the rule of lenity in adopting the narrow view of CFAA liability).