New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 264—NO. 92
TUESDAY, NOVEMBER 10, 2020

WHITE-COLLAR CRIME

Expert Analysis

The Supreme Court Will Interpret Another White-Collar Criminal Statute

By **Elkan Abramowitz**

And **Jonathan S. Sack**

The Computer Fraud and Abuse Act (CFAA) is the sort of broadly worded criminal statute which gives white-collar prosecutors considerable power—and makes defense counsel and judges uneasy. The law prohibits obtaining information by "access[ing] a computer without authorization or exceed[ing] authorized access." Computer hacking—"access[ing] a computer without authorization"—clearly violates the law. But the meaning of the other operative words, "or exceed[ing] authorized access," is not so clear.

The different ways of interpreting the statute have led to a split in the Courts of Appeals. Four Circuits have read the statute broadly: An individual "exceeds authorized access" when she accesses a computer and obtains information for an improper purpose, even if the person's access to the information is authorized. Four other circuits have read the statute narrowly: An individual "exceeds authorized access" only if she obtains information that she is not allowed to access, even if the purpose is improper. In practical terms, if a company Human Resources officer peeks at sensitive information out of idle curiosity, not because of work, would that be a crime because of the improper purpose, or would it not be a crime because the HR officer had the authority to review personnel files?

The first four circuits to address the meaning of "exceeds authorized access" read the words expansively.

The meaning of "exceeds authorized access" will soon be taken up by the Supreme Court in *United States v. Van Buren*, 940 F.3d 1192 (11th Cir. 2019), cert. granted, 2020 WL 190655 (Mem.) (U.S. April 20, 2020). Oral argument is scheduled for Nov. 30, 2020. In this article, we describe the Circuit split and explore different methods used by appellate courts to interpret the operative words of the CFAA. In *Van Buren*, the Supreme Court will have the opportunity once more to articulate its approach to interpreting white-collar criminal statutes.

Statutory Background

The statutory provision at issue originated in the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, see Pub.L. No. 98-473, §2102(a), 98 Stat. 1837, 2190, now codified as 18 U.S.C. §1030. Congress made it a crime to "access[ ] a computer without authorization, *or having accessed a computer with authorization, use[ ] the opportunity such access provides for purposes to which such authorization does not extend*." Id. (emphasis added).

In 1986, Congress enacted the CFAA as an amendment to the 1984 law. The CFAA reformulated the prohibition, adopting the present language. Congress replaced the italicized words with the "exceeds authorized access" phrase, so that the language now reads as follows: An individual violates the law when she "intentionally accesses a computer without authorization *or exceeds authorized access*, and thereby obtains … information" from the computer. 18 U.S.C. §1030(a)(2) (emphasis added). Congress went on to define "exceeds authorized access" to mean

ELKAN ABRAMOWITZ *and* JONATHAN SACK *are members of Morvillo Abramowitz Grand Iason & Anello. Mr. Abramowitz is a former chief of the criminal division in the U.S. Attorney's Office for the Southern District of New York. Mr. Sack is a former chief of the criminal division in the U.S. Attorney's Office for the Eastern District of New York.* DANI KIRSZTAJN, *an associate of the firm, contributed to this article.*

"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 to so obtain or alter." 18 U.S.C. §1030(e)(6).

The Broad Construction

The first four circuits to address the meaning of "exceeds authorized access" read the words expansively. See *EF Cultural Travel BV v. Explorica*, 274 F.3d 577 (1st Cir. 2001); *Int'l Airport Ctrs. v. Citrin*, 440 F.3d 418 (7th Cir. 2006); *United States v. John*, 597 F.3d 263 (5th Cir. 2010); *United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010). These courts held that a person "exceeds authorized access" if she accesses information for an unauthorized or improper purpose. See, e.g., *John*, 597 F.3d at 272-73 (affirming conviction of bank employee found guilty of using information to which she had authorized access to perpetrate a fraud). In this reading, the core issue is the defendant's purpose for obtaining the information, regardless of the defendant's authorized access.

The Eleventh Circuit's reasoning in *United States v. Rodriguez* is illustrative. The defendant, an employee of the Social Security Administration, used his access to agency databases to obtain personal information about several women for non-business purposes (e.g., to send them gifts). Obtaining information for these purposes violated agency policy. 628 F.3d at 1260. The defendant was convicted of violating the CFAA.

On appeal, the Eleventh Circuit affirmed the conviction. Relying on the statute's definition of "exceeds authorized access," the court held that the evidence at trial—chiefly, the defendant's testimony that he had purposely obtained personal information in violation of agency policy—demonstrated that "the plain language of the Act foreclose[d] any argument that [the defendant] did not exceed his authorized access." Id. at 1263. The court did not consider a narrower reading of the statute.

The Narrow Construction

Since 2010, four Circuits, including the Second Circuit, have rejected the broad interpretation of "exceeds authorized access." See *Royal Truck & Trailer Sales & Servs. v. Kraft*, 974 F.3d 756 (6th Cir. 2020); *United States v. Valle*, 807 F.3d 508 (2d Cir. 2015); *WEC Carolina Energy Sols. v. Miller*, 687 F.3d 199 (4th Cir. 2012); *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (en banc). These courts have held that "exceeds authorized access" means obtaining information that someone is prohibited from accessing in the first place. The core issue is the authority to access information, regardless of the purpose for obtaining the information.

Courts have taken two different paths to reach this conclusion. Three Circuits have found ambiguity in the statutory text and looked to policy considerations and legislative history to give specific meaning to "exceeds authorized access." See *Valle*, 807 F.3d at 526-28; *Miller*, 687 F.3d at 205-06; *Nosal*, 676 F.3d at 865-66.

The Second Circuit's reasoning in *United States v. Valle* illustrates this interpretive method. The defendant was New York City Police Department officer who had access to a computer program, Omnixx Force Mobile (OFM), which allowed officers to search databases of sensitive information. Accessing OFM for personal reasons, unrelated to official duties, violated NYPD policy. Valle accessed OFM to search for information about a woman and share the information with someone on the dark web (the two men discussed a possible kidnapping). Following a jury trial, Valle was convicted of "exceed[ing] authorized access," in violation of §1030(a)(2), and other offenses.

On appeal, Valle conceded that he lacked a legitimate purpose for querying the database, but argued that he did not "exceed authorized access" because he was authorized, as a police officer, to access the database, and therefore his purpose was irrelevant. The government argued that Valle "exceed[ed] authorized access" because his authorized access was limited to a law enforcement purpose, and his search lacked that purpose.

The Second Circuit reversed Valle's CFAA conviction. The court looked to the text of the statute and found that the word "authorization" could refer to either the purpose for which a person accesses a computer or the particular files and databases to which one's authorization extends. Because both readings were reasonable in the court's view, it found the statute to be ambiguous and turned to legislative history, but here too the court found support for different interpretations. The defendant argued that in 1986, when Congress inserted "exceeds authorized access" and removed the predecessor statutory language focusing on "purpose," Congress "intended to abrogate any purpose-based inquiry." The government argued that the substituted language, along with the specific definition of "exceeds authorized access," was intended just "to simplify the language." *Valle,* 807 F.3d at 525-26 (citing S. Rep. No. 99-432, at 2486, 2494).

Finding both the text and the legislative history inconclusive, the Second Circuit adopted a narrow interpretation under the principle of lenity. Holding that it was "required by the rule of lenity to adopt the interpretation that favor[ed] the defendant," id. at 526, the court emphasized that interpreting the statute as the government requested could transform ordinary violations of an employer's computer-use policy into federal crimes. See id. at 528. While the government "might [have] promise[d] that it would not prosecute an individual for checking Facebook at work," the court was "not at liberty to take prosecutors' word in such matters." Id. ("A court should not uphold a highly problematic interpretation of a statute merely because the Government promises to use it responsibly.").

The Sixth Circuit earlier this year construed the statute narrowly, but reached different conclusions along the way: It relied strictly on a reading of the statutory text without considering legislative history at all. See *Royal Truck*, 974 F.3d at 760-61. In a civil case, which alleged misappropriation of confidential company information by two former employees, the court found that "exceeds authorized access" has a clear meaning. Focusing on the statutory definition of "exceeds authorized access," the court looked to the dictionary definitions of the terms "access," "authorization," and "obtain or alter"—and Congress's use of the word "so" in the phrase "not entitled *so* to obtain or alter" (emphasis added)—and held that the provision applied to obtaining information a person was not entitled to access, regardless of purpose. Id.

The court also looked to other provisions which "appear aimed at preventing the typical consequences of hacking, rather than the misuse of corporate information in the manner alleged" by the plaintiff. Id. The court also cited the rule of statutory construction that "where Congress knows how to say something but chooses not to, its silence is controlling," referring to the fact that Congress knew how to say "exceeds authorized *use*," as it had done in other statutes. Id. (citing 6 U.S.C. §482(b)(1), (b)(3)) (emphasis added).

The Sixth Circuit earlier this year construed the statute narrowly, but reached different conclusions along the way: It relied strictly on a reading of the statutory text without considering legislative history at all.

Interestingly, the Sixth Circuit did not invoke the rule of lenity. But that was very likely because the Sixth Circuit, unlike the Second Circuit, addressed an alleged civil violation of the CFAA to which the rule of lenity would not apply. The Sixth Circuit's method of interpretation differed in another respect: It did not look to legislative history because it did not find ambiguity in the statutory text.

'United States v. Van Buren'

Like *Valle*, *Van Buren* concerns a police officer who had authorization to access a crime database but used that access for an improper purpose. Affirming the defendant's conviction, the Eleventh Circuit stated that it was bound by Eleventh Circuit precedent (*Rodriguez*). Under *Rodriguez*, "the record contained enough evidence for a jury to convict Van Buren of computer fraud" because he had searched the crime information database for a private purpose in violation of department policy.

Conclusion

In *Yates v. United States*, 135 S. Ct. 1074 (2015), the Supreme Court followed the textualist approach to reading statutes championed by the late Justice Antonin Scalia. See Elkan Abramowitz and Jonathan Sack, *Justice Scalia's Approach to Textualism in White-Collar Law*, N.Y.L.J. (March 1, 2016). But, as suggested by the majority and dissenting opinions in *Yates*, a close reading of statutory text does not always yield the same result. Faced with different results and interpretive methods in the Circuits, the Supreme Court in *Van Buren* may take the opportunity to clarify further how to read white-collar criminal statutes.