Crowell

Client Alert

"Authorized Access": The Supreme Court's First Foray Into The Computer Fraud And Abuse Act

April 22, 2020

On April 20, 2020, the Supreme Court granted cert in *Van Buren v. United States*, to resolve an important circuit split over the meaning of "authorized access" under the Computer Fraud and Abuse Act (CFAA). This is the Court's first foray into analyzing the precise contours of CFAA liability. *Van Buren* may have far-reaching implications for any individual or business operating in the digital domain, as the scope of civil and criminal liability under the CFAA can impact just about any sort of relationship involving access to computer systems, whether it be employer-employee relationships or third-party relationships.

The CFAA was enacted in 1986 as a first-of-its-kind statute designed to combat computer-related crimes, and has become an important and powerful tool for not only for the government but any business seeking to protect its intellectual property and computer systems. The CFAA imposes criminal liability on any person who "intentionally accesses a computer without authorization" or "exceeds authorized access" and, in doing so, obtains information from any protected computer. The CFAA also provides a civil cause of action for similar conduct. See 18 U.S.C. §§ 1030(a)(2), 1030(a)(4), 1030(a)(5)(B)-(C).

The term "without authorization" is undefined, but the CFAA 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 accessor is not entitled to obtain or alter." 18 U.S.C. § 1030(e)(6). As can be expected, there has been extensive litigation over the interpretation of "without authorization" and "exceeds authorized access." This has led to a circuit split on what type of conduct actually constitutes a CFAA violation. In particular, courts have grappled with whether the language of the CFAA places the focus on how the individual *accessed* the information, rather than how or under what circumstances the individual *used* the information.

For example, the First, Fifth, Seventh, and Eleventh Circuits broadly interpret "exceeding authorized access" to include using information on a computer in violation of a confidentiality agreement, or accessing information on a computer for a purpose prohibited by an employer. Specifically, the Eleventh Circuit has held that a defendant "exceeded his authorized access" under the CFAA by improperly using information that he was authorized to access. *U.S. v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010). In *Rodriguez*, a former employee of the Social Security Administration accessed the personal records of 17 different individuals for nonbusiness reasons while employed by the SSA. *Id*. There is no dispute that he was authorized to access those personal records. *Id*. However, the Eleventh Circuit held that the defendant "exceeded his authorized access and violated the [CFAA] when he obtained personal information for a nonbusiness reason" in violation of an established SSA policy. *Id; see also Int'l Airport Ctrs., LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006) (holding that when an employee of a real estate business deleted data regarding potential acquisition properties from his company laptop, the destruction of information breached the defendant's duty of loyalty and therefore terminated the employee's authorization to access the computer).

In contrast, the Second, Fourth, and Ninth Circuits have adopted a narrower interpretation of "exceeding authorized access": liability cannot be imposed on a person with permission to access information on a

computer who then uses that information for an improper purpose. In the seminal case *U.S. v. Nosal*, the Ninth Circuit held that subsequent improper use of information that was acquired by individuals with authorization to access such information is not a CFAA violation. 676 F.3d 854 (9th Cir. 2012). In *Nosal*, an ex-employee was charged with violating the CFAA on a theory that he induced former colleagues to use legitimate credentials—i.e., authorized credentials—to access the company's infrastructure and provide the former employee with information. *Id*. While the ex-employees' use of the information was clearly improper, the Ninth Circuit refused to extend the CFAA to this conduct because the accomplices were authorized to access the information, regardless of the subsequent use of that information. *See also WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199 (4th Cir. 2012) (holding that improper use of information validly accessed did not qualify as "unauthorized access" or "exceeding authorized access" within the meaning of the statute).

This brings us back to the case pending before the Supreme Court. Mr. Van Buren was a state police officer in Georgia. As part of a sting operation, the FBI used a third-party informant to ask Mr. Van Buren to obtain information from the Georgia Crime Information Center database. Mr. Van Buren had authorization to access this database for "law enforcement purposes" and, accordingly, accessed the database and provided the information to the third-party informant. The FBI arrested him for a CFAA violation (among other offenses) the next day. Though Mr. Van Buren had authorized access to the database, he had exceeded that authorization when he accessed the database to provide information to the third-party informant (i.e., not for law enforcement purposes). The Eleventh Circuit affirmed Van Buren's CFAA conviction, rejecting his argument that he was "innocent of computer fraud because he accessed only databases that he was authorized" to access.

The Eleventh Circuit's decision recognized that "other courts have rejected *Rodriguez's* interpretation of 'exceeds authorized access'" and invited the Supreme Court to resolve this split. The Supreme Court's decision will reverberate in the digital domain, in both the context of criminal enforcement of the CFAA and civil liability under that statute. If the Supreme Court adopts the narrower view, then businesses seeking to curb unauthorized use of information by employees and others will have a narrower set of legal tools and must rely on theories apart from the access itself. For example, the federal Defend Trade Secrets Act (DTSA) and state trade secret, tort, trespass and contract law will take on more significance in holding individuals liable for access to and use of the information. If the broader view prevails, then more expansive theories of CFAA enforcement and liability will be available.

In addition to *Van Buren*, a second CFAA case, *HiQ v. LinkedIn*, is pending before the Supreme Court. That case involves a business using automated bots to scrape information from public LinkedIn profiles including name, work history, job titles and skills, and using the information to yield "people analytics" in order to sell such information to its clients. LinkedIn is asking the Supreme Court to consider whether the use of automated bots to harvest personal data from public-facing websites—even after the computer servers' owners have expressly denied permission to access the data—constitutes "intentionally access[ing] a computer without authorization" in violation of the CFAA. Like *Van Buren*, a decision in *HiQ* could have far-reaching implications for companies relying on, or opposing, data scraping (or other technical measures to obtain information) to support a business.

Crowell & Moring's technology practice is devoted to litigating highly complex and ground-breaking technology issues in a variety of domains, including the CFAA. We will continue to monitor developments in *Van Buren* and *HiQ* and provide updates that will position businesses to adequately protect their systems and information in the rapidly changing legal technological landscape, and also avoid running afoul of the CFAA.For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Stephen M. Byers
Partner – Washington, D.C.
Phone: +1.202.624.2878
Email: sbyers@crowell.com

Jeffrey L. Poston
Partner – Washington, D.C.
Phone: +1.202.624.2775
Email: jposton@crowell.com

Gabriel M. Ramsey
Partner – San Francisco
Phone: +1.415.365.7207
Email: gramsey@crowell.com