Tech & Telecom Law News

INSIGHT: High Court's First Foray Into Computer Fraud Act Could Upend Liability

By Gabriel Ramsey, Jeffrey Poston, Stephen Byers, and Kayvan Ghaffari

May 11, 2020, 4:00 AM

The U.S. Supreme Court will venture into a circuit split on interpretation of the Computer Fraud and Abuse Act. Crowell & Moring attorneys say it 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.

On April 20, the U.S. 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. 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, including employee 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 the government but any business seeking to protect its intellectual property and computer systems.

The CFAA imposes criminal and civil 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. *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).

Circuit Splits Over Interpretations

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 as courts grapple with whether the CFAA focuses on how the individual *accessed* information, rather than how or under what circumstances the individual *used* information.

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.

For example, 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. *United States 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. There was no dispute he was authorized to access those personal records. However, the court held 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.

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 *United States v. Nosal*, the Ninth Circuit held 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 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.

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 improper use of information validly accessed did not qualify as "unauthorized access" or "exceeding authorized access").

This brings us back to *Van Buren*. Van Buren was charged with violating the CFAA by accessing Georgia's Crime Information Center database for an improper purpose. As a police officer, Van Buren was authorized to access this database for "law-enforcement purposes."

During an FBI sting operation, however, Van Buren provided information from the database to a third-party informant unrelated to any criminal investigation. Van Buren was arrested and convicted of violating the CFAA.

The government claimed Van Buren exceeded the scope of his authorized access when he provided information for a non-law enforcement purpose (i.e., provided information to the informant). Bound by *Rodriguez*, the Eleventh Circuit affirmed the conviction and focused on whether Van Buren had authority to *use* the information the way he did rather than authority to *access* the information from the database.

The Eleventh Circuit's decision recognized "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

If the broader view prevails, more expansive theories of CFAA enforcement and liability will be available. Employees will have to pay close attention to employment agreements, computer-use policies and other rules defining unauthorized use of data.

Such policies often prohibit sharing of information more broadly within the company than needed, forwarding documents to personal email to work at home, or accessing folders not strictly necessary for an individual's role.

Such activities may suddenly take on greater significance and companies could wield the increased risk of CFAA liability to broadly prevent unauthorized dissemination or use of information.

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 and state trade secret, tort, trespass and contract law will take on more significance in holding individuals liable for improper access to and use of the information.

Businesses would need revisit their corporate policies, appropriately delineate levels of access to the system, implement consistent computer access revocation procedures, and include provisions explicitly governing the use and dissemination of information.

This column does not necessarily reflect the opinion of The Bureau of National Affairs, Inc. or its owners.

Author Information

Gabriel Ramsey is a litigation partner at Crowell & Moring handling a broad range of technology-related litigation matters regarding computing environments, platforms, data access and usage, Internet law, intellectual property, cybersecurity and regulatory issues. He has twice been named one of the top 75 IP litigators in California and a top cyber lawyer by the Daily Journal.

Jeffrey Poston is a litigation partner and co-chair of Crowell & Moring's Privacy & Cybersecurity Group. He counsels and defends clients in complex data protection matters involving class-actions and regulatory enforcement actions, as well as commercial disputes.

Stephen Byers is a partner in Crowell & Moring's White Collar & Regulatory Enforcement Group who focuses on matters involving procurement fraud, health care fraud and abuse, trade secrets theft, foreign bribery, computer crimes and cybersecurity.

Kayvan Ghaffari is a Bay Area-based technology litigator who regularly litigates high-stakes cases under the DMCA and CFAA, including Facebook v. Power Ventures. Ghaffari also operates in the cyber domain, handling numerous disputes involving cybersecurity technologies, cybercrime, fraud and hacking.