SCOTUS RESOLVES CIRCUIT SPLIT, LIMITS THE SCOPE OF THE COMPUTER FRAUD AND ABUSE ACT

Date: 7 June 2021

U.S. Labor, Employment, and Workplace Safety and Litigation and Dispute Resolution Alert

By: April Boyer, Jonathan B. Morton, Rio J. Gonzalez

On 3 June 2021, the Supreme Court of the United States (SCOTUS) issued a 6-3 decision in *Van Buren v. United States*, resolving a circuit split on the meaning of "exceeds authorized access" and limiting the scope of the Computer Fraud and Abuse Act (CFAA).

Specifically, SCOTUS decided the issue of whether it is a violation of the CFAA to use a computer system for an improper purpose where the user otherwise has access to the computer system for legitimate purposes. In *Van Buren*, SCOTUS ruled that a police officer did not violate the CFAA when taking a cash payment in exchange for searching the Georgia Crime Information Center database because the police officer already had access to the database for work purposes. Specifically, the Court held that "an individual exceeds authorized access 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."

The decision limits the ability to prosecute individuals, government officials, or employees who might overreach their access to company data or digital information. The opinion has broad reach as civil and criminal liability under the CFAA impacts a broad scope of relationships involving access to computer systems—including employment relationships, third-party business relationships, and individual access to web-based platforms. Previously, a broad interpretation of the CFAA meant that a website's (or similar virtual platform's) terms of service could likely define the scope of use by a user and, thereby, criminalize activity beyond that scope. Now, the decision likely protects individuals from criminal or civil liability for breaking a website's online terms of service. Similarly, a broad interpretation of the CFAA meant that an employer could bring a claim against dishonest employees who accessed employer computer systems for improper purposes. Following the decision, SCOTUS has adopted a "gates up" approach whereby an employee's mere right to access an employer's computer system may shield the employee from civil or criminal liability under the CFAA despite improper use of the computer system. For example, employers who discover that an employee has wrongfully taken employer information can no longer use the CFAA as a tool to impose civil liability on the employee if the employee had access to that information as part of that employee's employment duties and responsibilities. Instead, to bring a claim under the CFAA, the employer will need to show that the employee obtained the information from a file, folder, or database to which the employee's computer access did not extend.

THE COMPUTER FRAUD AND ABUSE ACT

The CFAA, enacted in 1986 during the early stages of the Internet, imposes criminal or civil liability on any person who "intentionally accesses a computer without authorization" or "exceeds authorized access"[1] and, in doing so, obtains information from any protected computer.[2] The CFAA generally covers many types of computer fraud, including trade secret theft, hacking, data breaches, and anticompetitive behavior. Specifically, in order to plead a claim under the CFAA, a plaintiff must allege that a defendant (i) intentionally accessed a computer, (ii) lacked authority to access the computer or exceeded granted authority to access the computer, (iii) obtained data from the computer, and (iv) caused a loss of $5,000 or more during a one-year period.[3]

Prior to *Van Buren*, there existed a circuit split on the interpretation of "exceeds authorized access." Specifically, the First, Fifth, Seventh, and Eleventh Circuits interpreted the phrase broadly while the Second, Fourth, and Ninth Circuits adopted a narrow interpretation. The First,[4] Fifth,[5] Seventh,[6] and Eleventh[7] Circuits generally found that an employee's or corporate insider's use of a computer for an improper purpose prohibited by employment policies exceeded authorized access and violated the CFAA. Comparatively, the Second,[8] Fourth,[9] and Ninth[10] Circuits adopted a narrow "gates up" approach and generally held that "exceeds authorized access" does not impose liability on a person who accesses information for an improper purpose if the individual has access to the computer. In other words, the courts split as to whether the CFAA covered an employee who took or misused employer information for his own purposes to which the employee had access as part of that employee's employment duties and responsibilities.

FACTUAL AND PROCEDURAL HISTORY

In *Van Buren*, the FBI used a third-party informant to ask a Georgia state police officer to obtain information from the Georgia Crime Information Center database. Specifically, an undercover informant asked the police officer to perform a license plate search in order to determine whether a woman the informant had met at strip club was in fact an undercover police officer. In return, the informant offered the police officer $6,000 in order to run the search. After accessing the database and providing the information to the third-party informant, the FBI arrested the police officer for violating the CFAA. While the police officer had authorization to access the database for "law enforcement purposes," the FBI determined that by accessing the database to provide information to the informant, the police officer exceeded his authorization to access the database for such purposes.

Although the police officer had authority to access the database, the legal question concerned whether or not the police officer *exceeded* his authorization. The jury convicted the police officer, and the Northern District of Georgia sentenced him to eighteen months in prison for violating the CFAA. The police officer then appealed the decision to the Eleventh Circuit. The Eleventh Circuit affirmed[11] the police officer's conviction, finding that the police officer had violated the CFAA by accessing the law enforcement database for an "inappropriate reason." The Eleventh Circuit also invited SCOTUS to resolve the growing circuit split on the issue. On 20 April 2020, SCOTUS granted certiorari in order to decide the meaning of "authorized access" under the CFAA.

THE SUPREME COURT'S OPINION

The Court's decision, written by Justice Barrett and joined by Justices Breyer, Sotomayor, Kagan, Gorsuch, and Kavanagh, reversed the Eleventh Circuit's broad reading of the CFAA. The decision notes that the CFAA protects against those "who obtain information from particular areas in the computer—such as files, folders, or

databases—to which their computer access does not extend" but does not protect against those who "have improper motives for obtaining information that is otherwise available to them." Because the police officer had access to the police database to retrieve the license plate information, the Court found that the police officer did not exceed his access in using the database for an improper purpose.

While the opinion was based upon the majority's reading of the relevant text of the CFAA, it is important to note that the Court relied, in part, on the fact that the Government's interpretation of the CFAA "would attach criminal penalties to a breathtaking amount of commonplace computer activity." Specifically, the decision references how the Government's interpretation would criminalize an employee who sends a personal e-mail, an employee who reads the news using a work computer, or an individual who embellishes an online dating profile. Chief Justice Roberts, Justice Alito, and Justice Thomas dissented from the majority view, finding the majority's decision contrary to the plain meaning of the text and relying on principles of property law to reject a "gates open" approach to the meaning of "authorized access." Specifically, the dissent found that "without valid law enforcement purposes, he was forbidden to use the computer to obtain that information."

KEY TAKEAWAYS

- Businesses should consider heightened screening measures to protect sensitive data and to prevent employees or third-party users from accessing data to which they are not otherwise entitled or otherwise need not access. Be clear on what is and is not accessible by employees.
- Employers should update their workplace policies concerning limiting employee access to sensitive information on employer computers.
- Where trade secrets theft claims are at issue, employers may need to rely more heavily on the Defend Trade Secrets Act of 2016 (or comparable state laws) to pursue the misappropriation—even where the files were removed from a computer system—if the employee had access to the database where the data was stored.

FOOTNOTES

[1] "Exceeds authorized access" is defined as accessing "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." 18 U.S.C. § 1030(e)(6).

[2] 18 U.S.C. §§ 1030(a)(2), 1030(a)(4), 1030(a)(5)(B)-(C).

[3] 18 U.S.C. §§ 1030.

[4] EF Cultural Travel BV v. Explorica, Inc., 274 F. 3d 577 (1st Cir. 2001).

[5] United States v. John, 597 F.3d 263 (5th Cir. 2010).

[6] Int'l Airport Ctrs. LLC v. Citrin, 440 F. 3d. 418, 420-21 (7th Cir. 2006).

[7] United States v. Rodriguez, 682 F. 3d 1258 (11th Cir. 2010).

[8] United States v. Valle, 807 F.3d 508 (2d Cir. 2015).

[9] WEC Carolina Energy Sols. LLC v. Miller, 687 F.3d 199 (4th Cir. 2012).

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

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

KEY CONTACTS

APRIL BOYER
PARTNER

MIAMI
+1.305.539.3380
APRIL.BOYER@KLGATES.COM

JONATHAN B. MORTON
PARTNER

MIAMI
+1.305.539.3357
JONATHAN.MORTON@KLGATES.COM

