Time to Re-examine Corporate Computer Access Policies

Last week the U.S. Supreme Court agreed to hear an appeal from a defendant who had been convicted of a felony charge under the Computer Fraud and Abuse Act ("CFAA"), the federal computer crime statute. Title 18, U.S.C. § 1030. The Supreme Court will resolve the issue of whether the CFAA applies to employees who use their authorized access to employers' computer systems to misuse those systems, including to steal data. The courts of appeals have been divided on this question for the past 8 years. It is an issue of high significance to business because this statute allows individuals or companies victimized by violations of the CFAA to bring a civil action against perpetrators for damages and injunctive relief. Title 18, U.S.C. § 1030(g). This alert will explain the scope of the issue before the Supreme Court and what the ultimate Supreme Court decision may mean for protecting company data.

The appeal to the Supreme Court is from the 11th Circuit in the case of *United States v. Van Buren*, 940 F.3d 1192 (11th Cir. 2019). Nathan Van Buren, a sergeant with the Cumming, Georgia Police Department was charged with violating the CFAA for exceeding authorized access to a police database. Title 18, U.S.C., § 1030(c)(2). A government informant paid Van Buren to search a police database to determine if a "woman he [the informant] liked at a strip club" was an undercover cop. Van Buren later admitted to the FBI that "he knew" conducting the search "was 'wrong'" and that his "purpose" in searching the database was not a proper police function. The evidence at trial showed that "the database is supposed to be used for law enforcement purposes only and the officers are trained on the proper and improper uses of the system." The 11th Circuit affirmed the conviction on the basis that Van Buren had exceeded his authorized access to the police database.

The crux of what the Supreme Court will decide revolves around the CFAA's language that requires the perpetrator to have accessed the computer "without authorization" or in a manner that "exceeds authorized access." The phrase "without authorization" has been uniformly interpreted by the courts to mean "without permission." "Exceeds authorized access" is defined by the CFAA to mean "to access a computer with authorization and to

Related Capabilities

- Privacy & Social Media
- Government Enforcement & Corporate Investigations
- Securities & Financial Services Litigation & Enforcement

use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." The conflict among the circuit courts centers on what it means for an employee or corporate insider to "exceed[] authorized access" to company computers. The 1st, 5th, 7th, and 11th Circuits take the view that using the computer for an improper purpose prohibited by the employer's policies exceeds authorized access and is a violation of the CFAA.

In *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577 (1st Cir. 2001), the 1st Circuit concluded that a person "exceeds authorized access" when he uses information for purposes prohibited by a confidentiality agreement. The defendant there had "authorization . . . to navigate around EF's public website," *id*. at 583, but in the First Circuit's view, he "exceeded that authorization" by his "wholesale use" of "proprietary information and know-how" to collect data from the website to aid a competitor's strategy. *Id*. at 582-83.

The 5th Circuit in *U.S. v. John*, 597 F.3d 263, 269, 272 (5th Cir. 2010), held that a Citigroup account manager, who accessed Citigroup's internal computer system to provide her brother with customer account information that he used to make fraudulent charges on those accounts, had exceeded authorized access based on "Citigroup's official policy, that . . . prohibited misuse of the company's internal computer systems and confidential customer information."

The 11th Circuit, which decided the *Van Buren* case now before the Supreme Court, also relied on internal organization rules in *U.S. v. Rodriguez*, 628 F.3d 1258, 1260, 1263-64 (11th Cir. 2010), to affirm the CFAA conviction of a Social Security Administration employee who accessed Social Security information for personal reasons in violation of the agency's policy against "obtaining information from its databases without a business reason."

The 7th Circuit's holding in *Int'l Airport Ctrs. LLC v. Citrin*, 440 F.3d 418, 420-21 (7th Cir. 2006), is even broader and does not rely exclusively on an employer's policy to define unauthorized access. *Citrin* held that "when an employee accesses a computer or information on a computer to further interests that are adverse to his employer, he violates his duty of loyalty, thereby terminating his agency relationship and losing any authority he has to access the computer or any information on it."

In contrast, the 2nd, 4th, and 9th Circuit Courts of Appeals have each held that the CFAA's "exceeds authorized access" prong does not impose criminal liability on a person with permission to access information on a computer who accesses that information for an improper purpose. A person violates the CFAA in those circuits only if he accesses data on a computer that he is prohibited from using at all, for any reason. *United States v. Nosal*, 676 F.3d 854, 862-63 (9th Cir. 2012) (*en banc*). *Nosal* reasoned that the text of Section 1030(a)(2) does not cover a person "who has unrestricted physical access to a computer but is limited in the use to which he can put the information." *Id*. at 857, 862-63. *Nosal* interpreted "exceeds authorization" to "refer to data or files on a computer that one is not authorized to access," *id*. at 857, as opposed to accessing data for an improper purpose prohibited by the employer. An example would be "an employee may be

authorized to access customer lists in order to do his job but not to send them to a competitor." *Id*. Thus, as long as an employee is permitted blanket access to a company's computers, the CFAA does not prohibit an employee from accessing any data on that computer for any purpose, even if improper or contrary to the interests of his employer.

The 4th Circuit agreed with this reasoning in *WEC Carolina Energy Sols. LLC v. Miller*, 687 F.3d 199, 202, 207 (4th Cir. 2012), and the 2nd Circuit followed suit in *United States v. Valle*, 807 F.3d 508 (2d Cir. 2015).

A major factor motivating these courts is a concern that reading the CFAA to cover "use restrictions" would reach activities "routinely prohibited by many computer-use policies" and would improperly turn "millions of ordinary citizens" into criminals, *Nosal*, 676 F.3d at 857-63, and that "such a rule would mean that any employee who checked the latest Facebook posting or sporting event scores in contravention of his employer's use policy" would be guilty of a crime. *WEC Carolina Energy Solutions, LLC*, 687 F.3d at 206.

Our best prognostication is that the Supreme Court will affirm the 11th Circuit and side with those circuits holding that "exceeds authorized access" applies to employees violating company rules and their duty of loyalty to their employers. The common sense reading of the CFAA on its face seems unambiguous — "exceeds authorized access" means that even though an employee has access to a company's computers, the employee's access can be limited by company rules and the common law governing the loyalty that an employee owes to an employer, and that when the employee violates those rules, the employee "exceeds authorized access."

The argument that the CFAA can criminalize minor violations of an employer's use policies goes to prosecutorial discretion. This is precisely the same argument that has been leveled at the federal mail and wire fraud statutes because they could be used to prosecute individuals for stealing paltry sums of money through the wires or mails under circumstances that should not be prosecuted, yet the courts have consistently upheld both statutes.

The Supreme Court's interpretation of the mail and wire fraud statutes also argues in favor of the 7th Circuit's holding that an employee's authorization terminates when the employee commits a disloyal act like stealing data for a competitor, thereby terminating his agency relationship with the employer. *Carpenter v. U.S.*, 484 U.S. 19 (1987), relied on the same state law agency principles to uphold a "scheme to defraud," the key element of the mail and wire fraud statutes. *Carpenter* affirmed the conviction of a Wall Street Journal reporter who, prior to publication, had provided his upcoming financial columns to confederates, who bought or sold stock "based on the probable impact of the column on the market." *Id*. at 23. The Supreme Court held that "an employee has a fiduciary obligation to protect confidential information obtained during the course of his employment," and intentionally exploiting that information for his own personal benefit constituted a scheme to defraud his employer of confidential information. *Id*. at 29. The same employee duty should apply to the meaning of "authorized access" under the CFAA.

Given that the Supreme Court may affirm the 11th Circuit and give renewed national breadth to the CFAA, it is an opportune time for all businesses to re-examine their computer policies to determine whether they are in a position to take full advantage of the CFAA to retrieve stolen data from disloyal employees. As the 1st Circuit explained in *EF Cultural Travel*, 318 F.3d at 63, the CFAA "is primarily a statute imposing limits on access and enhancing control by information providers." Thus, a company "can easily spell out explicitly what is forbidden" through its policies and use those policies to take action against those employees who violate those policies by stealing and/or misusing company data. And, as the FBI reminded us in an April 23, 2019 notification to private industry, all companies face a regular threat to their data from insider employees. *See* https://bit.ly/3bGD1Ux.