U.S. Supreme Court Will Finally Weigh In on Scope of Computer Fraud and Abuse Act

By Clifford R. Atlas, Jason C. Gavejian, Joseph J. Lazzarotti, Ravindra K. Shaw and Erik J. Winton

April 27, 2020

The U.S. Supreme Court has agreed to decide whether it is a violation of the Computer Fraud and Abuse Act (CFAA) when an individual who is authorized to access information on a computer accesses the same information for an improper purpose. *Van Buren v. United States*, No. 19-783.

CFAA

The CFAA imposes both criminal and civil liability on an individual who intentionally accesses a computer "without authorization" or "exceeds authorized access" and, thereby, obtains information from the computer.

"Without authorization" is not defined in the statute.

The statute defines "exceeds authorized access" to mean accessing a computer with authorization and using the access to obtain or alter information in the computer that the person accessing it is not entitled to obtain or alter.

Eleventh Circuit Decision

The U.S. Court of Appeals for the Eleventh Circuit held that Nathan Van Buren, a police sergeant permitted to search a license plate database for law enforcement purposes, "exceeded his authorized access and violated the [CFAA] when he obtained [the victim's] personal information *for a nonbusiness reason."*

Van Buren conducted the search at the request of an acquaintance in exchange for $6,000, in what turned out to be an FBI sting.

CFAA and Circuit Court Split

The CFAA has generated much debate among the courts on the scope of its application.

Some forms of "unauthorized access" are obvious. A hacker breaking into a protected computer system resulting in data theft, for example, is clearly a CFAA violation and is the type of event the CFAA was originally designed to protect against.

However, other circumstances, particularly in the employment environment, can blur the lines of what is considered "unauthorized access" under the CFAA.

The First, Fifth, Seventh, and Eleventh Circuits have adopted a broad construction of the statute, allowing CFAA claims alleging an employee misused employer information that they were permitted otherwise to access. For example, in *International Airport Centers, LLC v. Citrin*, 440 F.3d 418 (2006), the Seventh Circuit held that, where an employee accesses an employer's computer or information to further interests adverse to the employer, the employee has violated the duty of loyalty and, in turn, "exceed[] authorized access" under the CFAA. *Citrin* is a particularly good example of the importance of the CFAA in the context of departing employees stealing or otherwise diverting employer information without authorization.

The Fifth Circuit took a similar approach as the Seventh Circuit in *U.S. v. John*, 597 F.3d 263 (2010), holding an employee violated the CFAA when she retrieved confidential customer account information she was authorized to access and transferred it to her half-brother for the purpose of committing a fraud.

On the other hand, the Second, Fourth, and Ninth Circuits have taken a narrower approach to CFAA application. In these circuits, employers' claims under the CFAA are limited. Such claims must be based on the actions of employees who lack permitted *access* to information on computers, not the intent of employees who exceed a permitted *use* of employers' information under company policies. However, employers may assert traditional state law claims against employees for breaching restrictive covenant agreements and misappropriating trade secrets.

Meet the Authors

Clifford R. Atlas

Principal
New York Metro
New York City
212-545-4017
Email

Jason C. Gavejian

Principal
Berkeley Heights
908-795-5139
Email

Joseph J. Lazzarotti

Principal
Berkeley Heights
908-795-5205
Email

For example, in *United States v. Valle*, 807 F.3d 508 (2015), the Second Circuit held that an individual "exceeds authorized access" only when they obtain or alter information on a computer that they do not have authorization to access for *any* purpose. The Second Circuit noted that a broad interpretation of the CFAA would allow private parties to manipulate their computer-use and personnel policies to turn their relationships into ones policed by the criminal law. Consequently, any employee who, for example, checked sports scores in violation of the employer's use policy could be subject to criminal penalties. In effect, the Second Circuit declined to rely on prosecutors or employers to determine responsibly whether to prosecute or sue individuals for computer activities at work that may range from innocuous (*e.g.*, checking Facebook) to nefarious (*e.g.*, downloading customer lists). A narrow construction of the statute, the Second Circuit said, ensures that every violation of a private computer-use policy does not become a federal crime or lawsuit.

Likewise, the Fourth Circuit held in *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199 (2012), that an employee with authorized access to his employer's computer system who allegedly downloaded proprietary information from that system for the benefit of his subsequent employer did not violate the CFAA. The Fourth Circuit emphasized that the CFAA is a criminal statute that should be construed narrowly and is meant to target hackers as opposed to "workers who access computers or information in bad faith, or disregard a use policy."

The Sixth Circuit has not addressed CFAA violations in the employment context, however, most district courts within the Sixth Circuit have concluded that there cannot be a CFAA violation where an employee had permissible access to the computer system. Most recently, in *Wachter Inc. v. Cabling Innovations LLC*, No. 3:18-cv-00488 (M.D. Tenn. May 7, 2019), a district court in Tennessee concluded that two former employees who allegedly shared with a competitor confidential company information found on the company's computer system did not violate the CFAA.

U.S. Supreme Court and CFAA

Given the split of decisions from the Circuit Courts of Appeal, review by the U.S. Supreme Court was likely. However, until now, the Supreme Court has avoided addressing issues of CFAA vagueness. In 2017, the Supreme Court denied review in *Nosal v. United States*, No. 16-1344, declining to weigh in on the scope of unauthorized access under the CFAA. The Ninth Circuit held in *Nosal* that David Nosal violated the CFAA by using his former assistant's password to access his former employer's computer system after his access credentials were expressly revoked.

Van Buren is a much-anticipated chance for the Supreme Court to clarify the scope of "unauthorized access" under the CFAA, which would provide greater certainty for parties facing CFAA litigation. The Court will hear arguments and rule on this case in its next term, which begins in October. We will monitor the case.

Companies should continue to review their policies and procedures to ensure access rights and limitations to their information and information systems are clearly defined and effectively communicated to their employees. Further, when faced with apparent unauthorized access to computer systems, companies should conduct an analysis to determine if a potential CFAA violation has occurred. Jackson Lewis attorneys, particularly in our Non-Competes and Protection Against Unfair Competition and Privacy, Data and Cybersecurity practice groups, can assist.

Ravindra K. Shaw

Principal
New York Metro
New York City
212-545-4041
Email

Erik J. Winton

Principal
Boston
617-367-0025
Email

Practices

Privacy, Data and Cybersecurity
Restrictive Covenants, Trade Secrets and Unfair Competition