Legal Update Article

Supreme Court Adopts Narrow Interpretation of Computer Fraud and Abuse Act

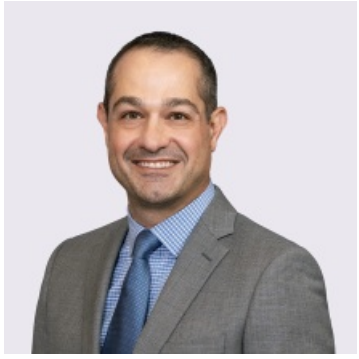
By Clifford R. Atlas, Jason C. Gavejian, Joseph J. Lazzarotti & Erik J. Winton

June 4, 2021

Meet the Authors

Clifford R. Atlas

(He/Him)
Principal
(212) 545-4017
Clifford.Atlas@jacksonlewis.com



Jason C. Gavejian

Office Managing Principal
908-795-5139
Jason.Gavejian@jacksonlewis.com

Joseph J. Lazzarotti

In a landmark decision, the U.S. Supreme Court has ruled that the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030 *et seq.*, does not prohibit improper use of computer information to which an individual has authorized access. Rather, the law prohibits obtaining information from areas of a computer, such as files, folders, or databases, that are outside the limits of the individual's authorized access. ***Van Buren v. United States***, No. 19-783 (June 3, 2021).

Circuit Split

Before the Court took up the case, a sharp split existed among circuit courts, with serious ramifications for employers. The First, Fifth, Seventh, and Eleventh Circuits had adopted a broad construction of the CFAA, allowing claims to go forward when an individual misused information they were otherwise permitted to access. The Second, Fourth, and Ninth Circuits took a narrower approach, concluding that CFAA claims were limited to situations in which an individual accessed information off-limits to them, and mere misuse of information to which they had authorized access could not constitute a violation.

The Supreme Court resolved this split in favor of the narrower reading.

Background

The CFAA prohibits two forms of "hacking": (1) "outside" hacking, achieved by "access[ing] a computer without authorization"; and (2) "inside" hacking, where an individual "exceeds authorized access" by accessing a computer "with authorization" and then obtaining information they are "not entitled *so* to obtain." (Emphasis added.)

The defendant, former police sergeant Nathan Van Buren, was caught in an FBI sting operation using his valid credentials to pull license information from a police database in exchange for money. There was no dispute Van Buren accessed a computer "with authorization" and "obtained information in the computer" when he acquired the license information. The issue was whether Van Buren was "not entitled *so* to obtain" the information he accessed.

Opinion

The Court's opinion seems destined for law school textbooks on the canons of construction. Exploring Black's Legal Dictionary, "common parlance," and the structure of the statute itself, the Court debunked the government's argument that the word "so" referred to information one was not allowed to obtain "in the particular manner or circumstances in which he obtained it," which could be unlawful under any number of unidentified statutes, rules, or private agreements. This broad interpretation, according to the Court, ignored that the word "so" referred to something already stated or described in the statute.

Principal
908-795-5205
Joseph.Lazzarotti@jacksonlewis.com

Erik J. Winton
Principal
(617) 367-0025
Erik.Winton@jacksonlewis.com

Related Services

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

The Court observed that the only manner of obtaining information Congress described in the definitional provision was through a computer one is otherwise authorized to access. Thus, the Court interpreted the phrase "is not entitled *so* to obtain" to mean "is not entitled to obtain by using a computer that the individual is authorized to access." Under this interpretation, the accessor's reason for using the information once obtained is irrelevant.

To illustrate its holding, the Court gave an example. If a person has authorized access to information stored in "Folder Y" on a computer, he does not violate the CFAA by obtaining that information, no matter if he did so for an unlawful purpose. If the information were stored on "Folder X," to which the individual lacked authorized access, he would violate the CFAA by obtaining the information with a computer.

The Court described liability for both "outside" and "inside" hacking as a "gates-up-or-down inquiry." Either the individual has authorized access to that part of the computer system from which they are obtaining information, or they do not. If they do have authorized access, there is no CFAA violation, no matter how the accessor uses the information.

Implications for Employers

The Court's narrower interpretation of the CFAA no doubt removes an arrow from the quiver of employers seeking to protect their information from improper use. Employees routinely access authorized areas of their employers' computer systems before departing for a competitor, sometimes with an eye towards using that information in their new employment. This behavior will no longer trigger liability under the CFAA, and as a result, litigants will be unable to use a CFAA claim as a ticket into federal court when dealing with this fact pattern.

It is incumbent on employers to be proactive in protecting their information. Although not a violation of the CFAA, improper use or acquisition of information from a computer system to which an employee has authorized access could constitute breach of contract, if there is an enforceable business protection agreement in place. It also could result in a violation of other laws, even if not the CFAA. For example, an employee accessing patient information without authorization may result in a violation of HIPAA for covered healthcare providers. Improper use or acquisition of sensitive information also could constitute trade secret misappropriation, or a breach of some common law duties, under the right circumstances. Additionally, to the extent personal information is accessed or acquired without authorization, it may constitute a data breach under applicable law. Finally, the Supreme Court's decision on the CFAA also does not foreclose an employer from enforcing its policies on authorized access to company data and imposing discipline for employees who violate those policies.

The key inquiry under the CFAA will focus now on whether an individual had "authorized" access to the areas of a computer system at issue. Employers with strong digital security protocols will be more likely to benefit from the CFAA's protection than those who lack control over what their employees can access. This includes implementing role-based or other forms of access control to ensure employee access to employer systems and data is appropriately defined and limited.

Employers should assess whether they have sufficient safeguards in place to protect against the conduct in *Van Buren*. While improper use of information through

authorized access may no longer violate the CFAA, it can still wreak havoc on a business. Jackson Lewis attorneys in the Restrictive Covenants, Trade Secrets and Unfair Competition practice group and the Privacy, Data and Cybersecurity practice group are available to assist with these issues.