GT GreenbergTraurig

Alert | White Collar Defense & Investigations/ Trade Secrets

June 2021

US Supreme Court Limits Scope of Computer Fraud and Abuse Act, Excludes Violations of Restrictions on Use of Digital Data

In *Van Buren v. United States*, No. 19-783, the U.S. Supreme Court issued an important opinion clarifying the scope of the Computer Fraud and Abuse Act (CFAA) that may have a broad impact on criminal and civil actions arising out of accessing digital information for improper purposes, including those relating to alleged accessing of company computers to obtain trade secrets.

The Issue. CFAA provides for criminal and civil liability if a person intentionally "accesses a computer without authorization or exceeds authorized access" in certain specified circumstances. *See* 18 U.S.C. § 1030. The phrase "exceeds authorized access" is defined as "to access 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." Circuit courts of appeals had been split on whether the term "exceeds authorized access" applied to situations where a person violated policies or terms that limited a person's use of computer data for certain purposes. In a 6-3 decision, the Supreme Court held that the phrase "exceeds authorized access" only "covers those who obtain information from particular areas in the computer—such as files, folders, or databases—to which their computer access does not extend." CFAA, however, "does not cover those who . . . have improper motives for obtaining information that is otherwise available to them."

The Background. The case arose when a Georgia police officer named Nathan Van Buren was caught in an FBI sting operation in which Van Buren agreed to get paid several thousand dollars by an informant to access the Georgia Crime Information Center database to search for a license plate number ostensibly belonging to an exotic dancer so that the informant could find out if the dancer was an undercover law enforcement officer. In truth, the FBI was investigating Van Buren for public corruption after the informant allegedly confessed to a priest that Van Buren tried to "shake down" the informant, and the priest got the informant in touch with law enforcement. After Van Buren received $1,000 of the promised payment and ran the search of the fictional dancer's dummy license plate, Van Buren was arrested and indicted by a grand jury for, among other charges, exceeding authorized access of a protected computer to obtain information for private financial gain under Title 18, United State Code Section 1030(a)(2)(C) and (c)(2)(B)(i), which is one of the provisions of CFAA that carries a maximum of five years' imprisonment and a fine of $250,000. Van Buren was convicted and sentenced to 18 months in federal prison. He appealed to the 11th Circuit Court of Appeals, which upheld his conviction under CFAA, finding that Van Buren's conduct of accessing the computer for financial gain exceeded authorization for public officials. The Supreme Court granted certiorari to resolve a circuit split regarding the scope of the "exceeded authorized access" prong of CFAA.

CFAA. *Van Buren* represents the first time the Supreme Court has addressed the scope of CFAA, which was enacted in the mid-1980s as one of Congress's early attempts to respond to perceived computer hacking threats to government and financial institutions, as dramatized in the popular 1983 movie *War Games*, which was premised on a high-school student hacking into NORAD's database and nearly causing nuclear war. Over the years, in addition to other statutes addressing computer crimes, Congress has expanded the reach and remedies of CFAA. For example, in 1994, Congress provided a civil right of action for those suffering economic damage for violations of CFAA, and in 2008, Congress broadened the definition of "protected computer" from its initial focus on computers used by the government and financial institutions to include those which are "used in or affecting interstate or foreign commerce or communication," which in practical terms conceivably means any computer connected to the internet, as some courts, including the Ninth Circuit, have held. Before *Van Buren*, the majority of federal courts of appeals had held that, in addition to hacking situations, CFAA applied where a person was authorized to access computer information but exceeded the purpose of what was authorized—e.g., violated policies that restricted the use of the information. A minority of circuits, including the Ninth Circuit, had held CFAA applied only when persons accessed information that they had no authorization to access at all, regardless of the reason.

The Holding. Writing for the majority, Justice Amy Coney Barrett began with a recitation of the history of CFAA, to respond to several publicized episodes of computer hacking in the 1980s, and then focused on the specific dispute relating to the provision that CFAA applies to situations when one accesses "a computer with authorization and to use such access to obtain . . . information in the computer that the accessor is not entitled so to obtain." 18 U.S.C. § 1030(e)(6). The Court noted that there was agreement between the parties that "Van Buren 'access[ed] a computer with authorization' when he used his patrol-car computer and valid credentials to log into the law enforcement database" and "that Van Buren 'obtain[ed] . . .information in the computer' when he acquired the license-plate record" for the benefit of the informant. Thus, the dispute for the Court to resolve was "whether Van Buren was 'entitled so to obtain' the record."

Justice Barrett started with an analysis of the text of CFAA, and specifically what the word "so" meant in the context of the phrase "entitled so to obtain" in CFAA. The majority rejected the government's proposed construction that the phrase "is not entitled so to obtain" refers to "information one was not allowed to obtain *in the particular manner or circumstances in which he obtained it*." The Court said

although the government's argument had "surface appeal," it "proves to be a sleight of hand" because it offered no textual limitation to the manner or circumstances of access and thus its proposed definition "potentially would include *any* circumstance-based limit appearing *anywhere*—in the United States Code, a state statute, a private agreement, or anywhere else." The majority similarly disagreed with the dissent's interpretation of the phrase "is not entitled so to obtain," explaining that it suffered from the same problem as the government's position, as it lacked any textual limitation.

Instead, the majority agreed with Van Buren's proposed interpretation of the phrase "entitled so to obtain" in CFAA as limited by the text of CFAA itself relating to use of a computer to obtain information. As such, the majority held that "[t]he phrase 'is not entitled so to obtain' is best read to refer to information that a person is not entitled to obtain by using a computer that he is authorized to access."

The majority also rejected the government's argument that interpreting the phrase "is not entitled so to obtain" as the majority did would render the word "so" superfluous. Instead, the majority explained that the construction adopted did not read the word "so" out of the statute, as it provides an important result of foreclosing any defense to CFAA liability where, for example, persons use authorization to obtain information from a computer for an improper purpose but would have argued that they had the right to obtain the information in a non-digital form. As Justice Barrett wrote: "The statute is concerned with what a person does on a computer; it does not excuse hacking into an electronic personnel file if the hacker could have walked down the hall to pick up a physical copy."

The majority then explained why its interpretation of the "exceeds authorized access" prong of CFAA was "harmonious" with the larger statute. It agreed with Van Buren's position that CFAA was designed with hacking in mind. One provision of CFAA applies to "outside hackers"—i.e., those who access a computer "without authorization." The majority found that the "exceeds authorized access" provision has a similar application to "inside hackers"—i.e., "those who access a computer with permission, but then exceed the parameters of authorized access by entering an area of the computer to which [that] authorization does not extend." (citations and internal quotations omitted). In contrast, the majority found the government's position would have created a disjointed CFAA with a black-and-white prohibition for outside hackers but a definition for "exceeds authorization" that would have been dependent upon different factors, which the majority found opened up dangers of arbitrary enforcement.

Further, the Court found support for its construction with the provisions for civil liability under CFAA. Specifically, the majority noted that CFAA provides civil liability for loss or damage, but the loss or damages is narrowly defined under CFAA to "focus on technological harms—such as the corruption of files—of the type unauthorized users cause to computer systems and data." Justice Barrett wrote that "[l]imiting 'damage' and 'loss' in this way makes sense in a scheme aimed at preventing the typical consequences of hacking," but such limitations would not be apt if CFAA was also designed to prohibit "misuse of sensitive information that employees may permissibly access using their computers," for which CFAA does not provide consequential damages.

After finding that the government's arguments based upon precedent and statutory history were "easily dispatched," Justice Barrett turned the majority's opinion towards the real-world impact of adopting the government's position, explaining that "the Government's interpretation of the statute would attach criminal penalties to a breathtaking amount of commonplace computer activity." "If the 'exceeds authorized access' clause criminalizes every violation of a computer-use policy, then millions of otherwise law-abiding citizens are criminals." Justice Barrett used an example of workplace computers, which are typically to be used only for business purposes but where, in reality, workers will send personal emails or read news articles and thus, under the government's interpretation, would violate CFAA, according to the majority. Similarly, the majority noted that many websites have terms-of-use restrictions that users must

agree to. "If the 'exceeds authorized access' clause encompasses violations of circumstance-based access restrictions on employers' computers, it is difficult to see why it would not also encompass violations of such restrictions on website providers' computers." Justice Barrett summed up the problem with the government's interpretation of CFAA as that it would "criminalize everything from embellishing an online-dating profile to using a pseudonym on Facebook," or would reach "checking sports scores or paying bills at work."

As the majority concluded, "[i]n sum, 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 Aftermath. With the decision in *Van Buren*, the scope of civil and criminal liability for situations of people using their computer credentials for improper purposes has been curtailed. CFAA will no longer provide a mechanism to law enforcement or civil litigants seeking to address employees' misuse of their access to their employers' digital information for the employees' personal gain or the detriment of others. Instead, CFAA will be limited to punishing instances of outsider hacking into a protected computer or situations where employees access information on an employer's computer system for which they have no authorization to access at all.

Yet the Supreme Court's holding in *Van Buren* does not leave prosecutors or civil litigants without any legal means to respond to those accessing an employer's computer for an improper purpose. For example, if an employee with access to a company's digital information uses that access to obtain the company's trade secrets, the conduct may implicate federal and state trade secret misappropriation laws, both civil and criminal. Common-law claims for breach of contract relating to confidentiality agreements or employment contracts that include restrictions on misuse of a company's digital information, or for breach of fiduciary duty, may be considered by companies in instances of an employee's misuse of computer credentials for personal gain. Prosecutors may turn to other federal and state laws, including trade secret theft, economic espionage, bribery, theft of honest services, and wire fraud, to name a few. And employers themselves should continue to be vigilant about internal access to computers to avoid claims of negligence relating to employees who improperly access a company's computer to the detriment of others. With *Van Buren*, the Supreme Court removed one potential tool in dealing with those who misuse access to employer computer systems, but others remain.

Authors

This GT Alert was prepared by:

- Kurt A. Kappes | +1 916.868.0650 | kappesk@gtlaw.com
- Todd A. Pickles | +1 916.868.0628 | picklest@gtlaw.com