BARNES & THORNBURG LLP

ALERTS

Supreme Court Narrows Scope Of Computer Fraud And Abuse Act In Van Buren V. United States

July 16, 2021

Highlights

A recent Supreme Court decision narrows the scope of liability under the Computer Fraud and Abuse Act (CFAA)

According to the Court, the CFAA does not apply to a person who has been granted access to electronic information and uses that information for an improper purpose

The statute now only imposes liability where a person hacks into, or accesses, electronic databases that the person does not have permission to access

A June U.S. Supreme Court opinion has clarified the scope of the federal Computer Fraud and Abuse Act (CFAA). In *Van Buren v. United States*, the Court issued a 6-3 ruling, with an opinion authored by Justice Amy Coney Barrett, holding that while the CFAA prohibits a person from wrongfully gaining access to electronic information in a computer that is "off limits" to the person, the statute does not prohibit a person who has been granted access to electronic information through their employment from obtaining and using that information for an improper purpose.

The Court vacated Van Buren's conviction under the CFAA. The ruling

RELATED PEOPLE

John M. Moye
Partner
Atlanta, Raleigh

P 404-264-4006
F 404-264-4033
jmoye@btlaw.com

RELATED PRACTICE AREAS

Data Security and Privacy
Internet and Technology
Litigation
Trial and Global Disputes

narrows the scope of liability under the statute and resolves a long-standing split among the federal circuits regarding the breadth of the CFAA.

The ruling in *Van Bure*n is noteworthy because it limits the scope of the CFAA as an enforcement tool. The CFAA can no longer be used to pursue civil claims or criminal charges for an employee or individual who has access to sensitive electronic information and uses that information for an improper purpose – for example, an employee who had been granted access to a company's confidential information and improperly downloads it and shares it with a competitor.

Instead, in light of *Van Buren*, the CFAA will only give rise to liability when the individual or employee electronically hacks into, or otherwise breaches, a computer database to which the person was not granted access. The ruling clarifies that the CFAA is primarily directed to hackers who access or obtain information they do not have permission to access. But the CFAA does not apply to a person who obtains electronic information that they are otherwise authorized to access and then misuses that information.

Facts of *Van Buren*

The *Van Buren* case involved Nathan Van Buren, now a former police sergeant in Georgia, who developed a relationship with a man named Andrew Albo. Albo asked Van Buren to use his police credentials to access a license plate database used by law enforcement and obtain information about a woman in exchange for a payment of approximately $5,000. Van Buren did so, using his valid credentials, and offered to provide Albo with the information he obtained from the database in exchange for the cash payment.

Such conduct plainly violated his department's computer-use policies. The FBI believed such conduct also violated the CFAA, and Van Buren was charged with a felony violation of the statute, on the theory that his running a license plate search and offering to provide the information to a third party violated the "exceeds authorized access" clause of the CFAA. Following a jury trial, Van Buren was convicted and was sentenced to 18 months in prison. The U.S. Court of Appeals for the Eleventh Circuit, following prior precedent, affirmed his conviction.

On appeal to the Supreme Court, Van Buren argued that the CFAA's phrase "exceeds authorized access" only applies "to those who obtain information to which their computer access does not extend," but that it does not apply to those, like Van Buren, who "misuse" information to which they are granted access as part of their job.

Background on the CFAA

The CFAA was passed by Congress in 1986 after a spate of highly publicized computer attacks by outside hackers. The statute imposes criminal and/or civil liability for a person who "intentionally accesses a computer without authorization or exceeds authorized access" and thereby obtains electronically stored information. The phrase "exceeds authorized access" is defined as "to access a computer with authorization and to use such access to obtain . . . information in the computer that the

accesser is not entitled so to obtain." The statute applies to computers that are "used in or affecting interstate or foreign commerce," which, in practical terms, means any computer that is connected to the internet. The CFAA imposes criminal liability for violation of the statute; it also permits a civil cause of action for money damages when a violation occurs.

Over the past few decades – particularly as misuse and/or theft of electronic information has become a widespread problem – both prosecutors and civil litigants have used the CFAA to pursue electronic theft of information, either by outside hackers or by "inside hackers," i.e. individuals within an organization. In addition, in some jurisdictions, the CFAA was frequently used as an ancillary claim to a civil trade secret misappropriation claim, i.e. where an employee or individual electronically misappropriated electronic trade secrets to which they had access and passed them along to a competitor or otherwise misused the information.

In recent years, however, the federal circuit courts have been divided over the CFAA and its "exceeds authorized access" language. Some circuits, like the Eleventh, Fifth, and Seventh, have held that a person may "exceed authorized access" (and be liable under the statute) if the person has access to electronic information but uses that information for an improper purpose, e.g. by stealing it or using it to break the law.

Other circuits, however, most notably the Second, Fourth, and Ninth, pushed back against this broader interpretation of "exceeds authorized access"— construing the phrase as meaning that liability attaches under the statute only if the person either hacks into or gains access to information that is "beyond the boundaries" of the access the person has been granted. These circuits have held that an "improper motive," or even a misuse of electronic information, does not implicate the CFAA if the person in question had authorized access to the information he or she is accused of misusing.

The Supreme Court had previously denied certiorari in a Fourth Circuit case that might have resolved the confusion among the circuits as to the breadth of the statute. *Van Buren* provided another opportunity to the Court to clarify the scope of the CFAA – and, this time, the Court took up the opportunity, hearing oral arguments in the case in November 2020.

The Court's Ruling in *Van Buren*

It was undisputed that Van Buren had been granted credentials and access to the license plate database as a sergeant within the police department. The question before the Supreme Court was whether Van Buren had "exceeded authorized access" under the CFAA by running a search on a private citizen using that database (in hopes of receiving a cash payment).

In its opinion, Justice Barrett wrote that Van Buren had not "exceeded authorized access" under the CFAA by obtaining information from a database that he was entitled to access as part of his job, even if his motives for doing had been improper. The Court's ruling hinged on the statutory definition of "exceeds authorized access," that is, to "use . . . access [to information] to obtain . . . information in the computer that the accesser is not entitled so to obtain."

Applying tools of statutory interpretation, the Court held that the use of the

word “so” in the definition (information the accesser is “not entitled to so obtain”) refers to “information that one is not allowed to obtain” using a computer to which he otherwise had access. Put another way, the Court held that the CFAA prohibits a person from using the access granted to them to obtain information that is “off limits” – but that the statute did not apply to a person who uses their access to obtain and/or misuse information to which they have been granted authorized access, even if the person acts with an improper motive.

Through its ruling, the Court clarified that the CFAA is directed primarily to hackers – both outside an organization (e.g. someone who accesses information “without authorization”) and “inside hackers,” such as someone who has permission to access a computer database but “exceeds authorized access” by entering electronic databases to which the person does not have access. In Van Buren’s case, because he had clearly been granted access to the license plate database, he did not “exceed authorized access” under the CFAA by running a search on a private citizen, even if his motives were untoward. Thus, the Court vacated his conviction under the CFAA.

In a dissent, Justice Clarence Thomas (joined by Justices John Roberts and Samuel Alito) argued that the CFAA should impose liability for conduct like Van Buren’s – that is, where a person obtains information they are entitled to access for an unlawful or improper purpose. Relying on principles of property law, Justice Thomas opined that “access” is circumstance-specific and can be exceeded when a person goes beyond the scope of the access that he been granted. For example, a valet parking attendant may have “access” to park a car, but the attendant would “exceed [the] authorized access” if he or she took the car for a joy ride. Similarly, a person might have “access” to visit someone’s property, but if the person overstayed his or her welcome (e.g. setting up a campsite and refusing to leave), the person would “exceed” the authorized access and become a trespasser. The dissent argued that the majority’s reading of the CFAA was too narrow and that it was inconsistent with the statutory language and the legislative history.

What the *Van Buren* Ruling Means

In the wake of *Van Buren*, it is clear that the CFAA’s “exceeds authorized access” provision may only be used by litigants or law enforcement personnel when a person obtains or uses electronic information to which they have not been granted access, *e.g.* by accessing directories or database that they are not authorized to access.

By narrowing the scope of the statute, however, *Van Buren* means that the CFAA will no longer afford a cause of action to an aggrieved party when an individual within a company or organization obtains and/or uses electronic information to which they have been granted “access,” even if the individual uses the information for an improper purpose – such as to steal trade secrets or (in Van Buren’s case) to exchange the information obtained for money.

For more information, please contact the Barnes & Thornburg attorney with whom you work, or John Moye at 404-264-4006 or jmoye@btlaw.com.