LJN LAW JOURNAL NEWSLETTERS

Business Crimes Bulletin ®

An ALM Publication

Volume 28, Number 11 • July 2021

Supreme Court Narrowly Interprets CFAA to Avoid Criminalizing 'Commonplace Computer Activity'

By Patricia Kim and Maren Messing

On June 3, 2021, the United States Supreme Court issued a 6-3 opinion in *Van Buren v. United States*, No. 19-783, resolving the circuit split regarding what it means to "exceed[] authorization" for purposes of the Computer Fraud and Abuse Act (CFAA). The Court held that only those who obtain information from particular areas of the computer which they are not authorized to access can be said to "exceed authorization," and the statute does *not* — as the government had argued — cover behavior, like Van Buren's, where a person accesses information which he is authorized to access but does so for improper purposes. This was a long-awaited decision interpreting the CFAA, which has become an important statute in both criminal and civil enforcement relating to computer crime and hacking.

Maren Messing is Counsel in Patterson Belknap Webb & Tyler's Litigation department, where she advises clients on privacy and data security matters and is an editor of the Firm's Data Security Law Blog. Ms. Messing also practices in the areas of false advertising, employment law, white collar defense, and antitrust law. She can be reached at mmessing@pbwt.com. **Patricia Kim** is an Associate in Patterson Belknap Webb & Tyler's Litigation department. Ms. Kim's work focuses on complex commercial litigation, alternative dispute resolution, products liability, and false advertising. She is a regular contributor to the Firm's Data Security Law Blog. She can be reached at pkim@pbwt.com.

Background

The Computer Fraud and Abuse Act (CFAA), 18 U.S.C. §1030 *et seq.*, was passed in 1986 as a targeted measure to combat a fairly circumscribed category of "computer trespassing" crimes. At that time, computer usage did not remotely resemble what it does today — in 1989, for example, about 15% of American households owned a personal computer and most people had never heard of the Internet. Despite significant changes in technology and an explosion in the use of electronic data since that time, many of the CFAA's provisions have not changed. Nevertheless, in recent years it has become the primary federal law used to prosecute hackers, including in a number of high-profile cases such as WikiLeaks founder Julian Assange, Aaron Swartz (co-founder of Reddit), Gilberto Valle (the "Cannibal Cop"), and Lori Drew (whose MySpace hoax was blamed for the suicide of a 13-year-old neighbor).

The CFAA prohibits accessing a computer "without authorization" or in a manner "exceeding authorized access." 18 U.S.C. §1030(a)(2). "[E]xceeding authorized access" is defined as "access[ing] a computer with authorization and … us[ing] such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter." *Id.* §1030(e)(6). Notably, the CFAA does not require that the person who accesses the computer actually *do* anything with the information they see or obtain. For that reason, many had previously expressed concern about the statute, arguing that it was subject to selective prosecution, allowing a prosecutor to bring felony charges even when there was little or no harm, just because the government disapproved of the activity. Those who violate Section 1030(a)(2) face penalties ranging from fines and misdemeanor sentences to imprisonment for up to 10 years. The CFAA also provides a private civil cause of action, which allows persons suffering damage or loss from CFAA violations to sue for money damages and equitable relief.

Prior to the Court's decision, the United States Courts of Appeals were split on how to interpret the "exceeding authorized access" language. On one hand, the Second, Fourth, and Ninth Circuits criminalized only unauthorized access to a computer system. In this view, a person who used their credentials to access information they had a right to see, but did so for an illegitimate purpose, would not fall within the purview of the CFAA. The First, Fifth, Seventh, and Eleventh Circuits, by contrast, more broadly interpreted the text to include a prohibition on the misappropriation of data, even if the offender gained access to the information permissibly. In those Circuits, a person violated the CFAA simply by downloading information from a database they were authorized to use if they did so for an impermissible reason. A Circuit split on the meaning of this statute was especially problematic given the potential for computer crime to occur in multiple jurisdictions (the location of the defendant and the computer server being accessed are often not in the same place), creating uncertainty about the dividing line between legal and prohibited conduct.

Van Buren's Alleged Violation

In the case before the Court, then-police sergeant Nathan Van Buren used his

patrol-car computer to access the law enforcement database — a database which he indisputably had authority to access. However, his search for information was done in exchange for money from an acquaintance and was not for law enforcement purposes. Caught in an FBI sting operation, Van Buren was arrested and charged with honest services fraud and a CFAA violation. The trial evidence showed that Van Buren had been trained not to use the law enforcement database for "an improper purpose," defined as "any personal use." Van Buren therefore knew that the search breached department policy. And, according to the Government, that violation of department policy also violated the CFAA. Van Buren was convicted at trial and sentenced to 18 months' imprisonment and the Eleventh Circuit affirmed his conviction, setting up the Supreme Court's review. The Supreme Court granted certiorari to resolve the Circuit split described above.

The Majority Decision And Dissent

The Court held that Van Buren's actions did not violate the CFAA, adopting the narrower reading of the statute as interpreted by the Second, Fourth, and Ninth Circuits and as advocated for by Van Buren.

Justice Amy Coney Barrett's opinion first engaged in a textualist analysis of the definition of the word "so" and its status as a qualifier for the word "entitled." She wrote that "[t]he disputed phrase 'entitled so to obtain' thus asks whether one has the right" to access information one is not allowed to obtain by using a computer that he is authorized to access. Justice Barrett stated that while the Court's decision was driven by the text of the statute, the government's proposed reading of the statute also had to be rejected as untenable because it "would attach criminal penalties to a breathtaking amount of commonplace computer activity." In other words, the "exceeds authorized access" clause would criminalize every violation of a computer-use policy, creating criminals out of "millions of otherwise law-abiding citizens" who are, for example, sending personal e-mails or reading the news on work computers. These real-world implications are likely what drove the Court's three liberal justices to join Justices Barrett, Brett Kavanaugh, and Neil Gorsuch in the majority's avowedly textualist opinion.

The dissent, written by Justice Clarence Thomas and joined by Chief Justice John Roberts and Justice Samuel Alito, focused on the term "entitled," and how Van Buren by the plain meaning of the word was not "entitled" to the information because "proper grounds" to obtain it did not exist. He also noted that the majority's reading was at odds with basic tenants of property law, and that much of the Federal Code already criminalizes common activity, such as taking a grain of sand from the National Mall, breaking a lamp in a government building, or permitting a horse to eat grass on federal land. In the dissent's view, being uncomfortable with criminalizing conduct, therefore, did not give the Court authority to alter the plain meaning of the statute.

Implications

Following the Court's decision, the CFAA only prohibits breaking into a computer system as an outside hacker or as an authorized user exceeding the scope of their authorization by accessing data in a gated part of that system. As a result, an employee who uses their credentials to access "information located in particular areas of the computer" they are entitled to access will not violate the CFAA, even if the reason for doing so is personal, in violation of company policy, or otherwise improper.

While this interpretation reflects the majority's reasonable concerns about over-criminalizing everyday actions, it also means that there is certain behavior that employers want to proscribe and prosecutors want to deter which will no longer fall within the ambit of the CFAA. For example, an employee may have legitimate access to troves of sensitive information, such as proprietary company source code, names, addresses, credit card numbers, and social security numbers, all of which can be subject to misuse. Some of that information may constitute "trade secrets," allowing an employer or the government to pursue a theft of trade secrets action, but much of it does not, leaving a gaping hole for the type of hacking behavior that prosecutors have sought to deter in recent years. But should the individual access the information and then actually *make use of it* in order to deprive someone of property, they could quickly be subject to charges of wire fraud (18 U.S.C. §1343) or bank fraud (18 U.S.C. §1344) if a bank was the victim of the scheme, or perhaps identity fraud (18 U.S.C. §1028). In other words, the result of the Court's decision is that liability may not attach to simply accessing data for an improper purpose — there has to be some use of that data following the access to which liability can attach. There may also be civil actions that could be brought against the wrongdoer for conversion, or for theft of trade secrets or other confidential information. When an employee engages in this type of behavior, they can also of course be disciplined, terminated, or sued for a breach of their duty of loyalty to their employer.

It remains to be seen whether Congress will act to amend the CFAA or pass new legislation addressing the type of behavior that was at issue in *Van Buren* and the other cases which led to the Circuit split. There is no easy or obvious fix to the statute's current language, which will make it more challenging for Congress to respond than in some other instances where the Supreme Court has narrowly construed federal law. Would Congress want to re-criminalize the commonplace, innocent conduct that *Van Buren* made expressly legal, such as checking sports scores on a work computer or violating the terms of use on Facebook by using a pseudonym? Perhaps not. In any event, one can hope that the Court's decision in this cases pushes Congress to more broadly reexamine the CFAA and work to make it more relevant to the problems of cybercrime that confront the United States today.

—❖—