Data Privacy and Cybersecurity

Why the Supreme Court's Decision in *Van Buren* May Be Felt beyond Criminal Law

By: Aaron R. Cooper, David Bitkower, Clifford W. Berlow, and Grace C. Signorelli-Cassady

In *Van Buren v. United States*, the US Supreme Court will soon resolve a circuit split concerning an important computer crime law known as the Computer Fraud and Abuse Act. Depending on how it is decided, the case may have several important impacts beyond the criminal space. For one, it may have broad potential consequences for how domestic businesses, websites, and tech companies handle access and use restrictions at work, on social media platforms, in the computer security space, and in any other context where authorized individuals have access to sensitive digital information. Moreover, even international entities with data in or accessible from the United States should be aware of the Court's pending decision, due to the increasingly cross-border nature of computer networking and data flows. And in addition, the Court's ruling could set the stage for legislative reform that establishes new lines between lawful and unlawful computer activity.

The Legal Dispute

On Monday, November 30, 2020, the justices heard oral argument in *Van Buren v. United States*, a case involving a Georgia police sergeant convicted under a provision of the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030(a)(2)(C), that prohibits "exceed[ing] authorized access" to a protected computer and thereby obtaining information, including for personal financial gain. (A companion prong of § 1030(a)(2)(C)—which concerns accessing a computer "without authorization"—is generally understood to prohibit computer hacking and is not implicated directly here.) As part of his job, Van Buren had authorization to access a confidential law enforcement database for official purposes. But when he accessed the database instead to sell license plate information about a potential undercover officer to an FBI informant, the government successfully prosecuted him for violating the CFAA. On appeal, the Eleventh Circuit upheld the conviction.

At issue is the interpretation of "exceeds authorized access," a phrase defined by the CFAA at 18 U.S.C §1030(e)(6) to mean "access[ing] a computer *with* authorization" but then "us[ing] such access to obtain or alter information in the computer that the accesser is *not* entitled so to obtain or alter" (emphasis added). According to the government's position, this language targets "insider" threats—that is, a person who is authorized to access information on a computer for one purpose, but instead does so for an unauthorized one. In contrast, Van Buren has taken the position that the CFAA does not prohibit computer misuse, but only "hacking"—whereas the "without authorization" prong applies to "outsider" hacking, the "exceeds authorized access" prong applies to "insider" hacking. That is, one "exceeds authorized access" to a computer when granted permission to access a computer system in general, but given no authorization whatsoever to access a specific part of it, or specific information on it.

The parties' positions reflect an existing circuit split: Van Buren's interpretation is consistent with recent precedent in the Second, Fourth and Ninth Circuits, while the government's interpretation has been endorsed by decisions in the First, Fifth, Seventh, and Eleventh Circuits. A variety of amicus briefs in support of Van Buren—from entities such as the National Association of Criminal Defense Lawyers (represented by Jenner & Block) to computer security researchers—along with filings in support of the government—from the financial industry and entities such as the electronic voting application Voatz—illustrate the broad range of concerns on both sides of the dispute.

Oral Argument

While it is always challenging to predict an outcome from oral argument alone, the justices' questioning largely seemed to favor Van Buren's view. Some of the justices, including Justices Thomas and Alito, appeared sympathetic to the government's broader reading of the CFAA as necessary to protect against insider misuse of sensitive or private data. But more voiced skepticism that the government's interpretation could, as Van Buren argued, "brand most Americans criminals on a daily basis."

The argument crystallized in particular a disagreement over the phrase "so to obtain." In Van Buren's interpretation, "so" referred back to the use of a computer, while under the government's construction, it referred back to "uses such access." To illustrate the language's ambiguity, Justice Sotomayor observed to the government: "Imagine a law that says anyone who drives on Elm Street who is not authorized so to drive shall be punished. The 'so to drive' to me could mean if you're not authorized to drive on Elm Street. But under your theory, it could be, and might very possibly be read as saying you can't ride on Elm Street if you're driving on it with an illegal purpose, you're speeding, you're breaking the law on curfew, you're texting, it could even cover people who drive on Elm Street on their way to commit a different crime, because they weren't authorized to be on Elm Street for the purpose of committing a crime." In other words, if the phrase "so to obtain" requires conformity with every restriction on access, then most Americans who have ever clicked (or ignored) terms of service are doing *something* wrong; but if it only requires permission to access in general, then the law focuses more narrowly on computer trespassers.

Against this, the government sought to explain that other terms in the CFAA already narrow the statute's scope; "authorization," for example, could be understood as "specifically considered and individually authorized," which would mean the statute wouldn't police access to a public website like Facebook. But several justices still appeared reluctant to embrace this approach. Chief Justice Roberts, for example, commented: "I don't understand your focus on 'authorization' as a limiting term." And Justice Sotomayor responded: "My problem is that you are giving definitions that narrow the statute that the statute doesn't have."

The justices also seemed unpersuaded that the government's broader reading of the CFAA was necessary as a policy matter, appearing to agree instead with Van Buren that nefarious conduct would already be criminalized under other state and federal laws. Justice Gorsuch, for example, expressed significant concern about the over-federalization of criminal law, including for contractual violations or computer use policies that would be "making a federal criminal of us all." Justice Kavanaugh added his concern over "a fairly substantial expansion of federal criminal liability based on one word"—"so"—that appeared ambiguous.

Implications Beyond Criminal Law

The Supreme Court's decision—whichever way it goes—will likely settle the circuit split and resolve a long-standing dispute over criminal enforcement of the CFAA in computer misuse cases. But the decision's potential consequences beyond the criminal space are equally important.

Though largely unmentioned during oral argument, the CFAA includes a civil enforcement provision, 18 U.S.C. § 1030(g), which permits private parties to seek money damages or injunctive relief for certain statutory violations. So, under the present circuit split, a company in the First, Fifth, Seventh or Eleventh Circuit may, for example, successfully sue an employee under the CFAA for stealing confidential information and handing it to a competitor, or a website may seek to enjoin a competitor from scraping information the website posts online. But, in similar suits in the Second, Fourth or Ninth Circuits, the result could differ, depending on the specific authorization at issue. A ruling that rejects the government's approach could therefore have consequences for civil litigants under the CFAA, cutting off entirely a viable cause of action, shifting pressure to alternative theories of legal relief, or causing entities to reconsider how they design network security and administer user restrictions. Several examples help to illustrate where the ripples might be felt:

Employment Agreements. Many companies with sensitive and proprietary data provide their employees or contractors network access conditioned on appropriate business uses, identified in click-through banners or employee handbooks. For example, an employee or contractor may be granted credentialed access to a company's trade secrets or other sensitive business information on the condition that they only use the access for approved purposes. If the Court rules in favor of Van Buren, however, violation of such an agreement by an employee would likely no longer be enforceable via the CFAA. Alternative legal theories, such as an action for theft of trade secrets or for breach of contract, may still be available, but perhaps be more challenging to pursue.

Web Crawling and Data Scraping. Many public-facing websites seek to limit third-party use (or misuse) of data through terms of service, as a way to prevent data scrapers or competitors from misappropriating data or taking up bandwidth. Over the past several years, the Ninth Circuit has repeatedly held that the CFAA does not prohibit data scraping of public information on the sole basis of terms-of-service violations, including in cases involving Facebook and LinkedIn. A decision favoring Van Buren would extend that rule to the rest of the country, thereby requiring such websites to take further action to more closely monitor visitors and take other steps to revoke authorization of an offending party.

Computer Security. Entities seeking to improve network and product security have increasingly turned to bug bounty programs, offering compensation to third-party computer security researchers for authorized discovery of vulnerabilities. In an amicus brief filed in *Van Buren* on behalf of computer security researchers, the Electronic Frontier Foundation argued that the risk of liability created by the CFAA chilled their participation in such programs. Yet at the same time, entities with existing bug bounty programs—or that anticipate creating one—may want to reconsider the ways in which they formalize and administer those programs. For instance, it is not uncommon for a program to distinguish between authorized and unauthorized ways of accessing the network; if the Court rules in favor of Van Buren, such a distinction may be harder to enforce under the CFAA, a possibility that appeared to trouble the mobile voting company Voatz.

International Data. The ruling will not just affect the rules of the road within the United States, but also activity outside the United States that involves a US computer. In today's often borderless internet, individuals and entities outside the United States thus should take time to understand the implications of the Court's eventual ruling for their own networks as well.

What Comes Next

Regardless of the Court's decision, many of the questions raised by the justices suggest that new legislative proposals may be needed to address the range of policy issues surrounding the CFAA. So, beyond the immediate legal consequences outlined above, employers, internet companies, and computer security professionals should keep an eye on the possibility of statutory reform following the decision. The precise contours of the Court's opinion will determine what those proposals address, and it may present a rare opportunity to set new rules governing Internet behavior for decades to come.

Aaron R. Cooper previously served as a cybercrime prosecutor at the US Department of Justice (DOJ) and recently joined Jenner & Block as a Special Counsel in its Cybersecurity and Data Privacy Practice. Partner David Bitkower, who formerly served as the Principal Deputy Assistant Attorney General of DOJ's Criminal Division and oversaw cybercrime prosecutions at DOJ, is Chair of Jenner & Bock's Cybersecurity and Data Privacy Practice. Earlier this year, Partner Clifford W. Berlow and Associate Grace C. Signorelli-Cassady wrote an amicus brief in Van Buren on behalf of the National Association of Criminal Defense Lawyers, urging the Supreme Court to reverse Van Buren's conviction and, among other things, explaining that an expansive reading of the CFAA would raise due process concerns.

Contact Us

Aaron R. Cooper
acooper@jenner.com | Download V-Card

David Bitkower
dbitkower@jenner.com | Download V-Card

Clifford W. Berlow
cberlow@jenner.com | Download V-Card

Grace C. Signorelli-Cassady
gsignorelli@jenner.com | Download V-Card

Meet Our Team

Practice Leaders

David Bitkower
Chair
dbitkower@jenner.com
Download V-Card

David P. Saunders
Co-chair
dsaunders@jenner.com
Download V-Card