Trade Secrets and Restrictive Covenants
Data Privacy and Cybersecurity

SCOTUS Limits the Reach of the Computer Fraud and Abuse Act, with Implications for Cybersecurity, Trade Secrets Litigation, and Beyond

By: Debbie L. Berman, David Bitkower, April A. Otterberg, Shoba Pillay, Aaron R. Cooper, Andrew J. Plague, and Eric S. Fleddermann

On June 3, 2021, the US Supreme Court issued a much-anticipated decision interpreting the scope of the federal Computer Fraud and Abuse Act of 1986 (CFAA) not to cover situations in which the defendant was authorized to access information on a computer yet did so for an improper purpose.[1] The decision, which was widely expected after oral argument in November, carries a range of cybersecurity implications for businesses, such as the need to reassess employee access and website terms of service, while simultaneously narrowing the types of trade secret misappropriation that can be addressed through civil claims under the CFAA. In addition, one aspect of the Court's reasoning, involving the types of "damages" or "loss" required for civil CFAA claims, may further limit the damages available in civil claims brought under the CFAA to harm caused by the intrusion itself rather than any downstream harm caused by misappropriation or misuse of the information obtained.[2] At the same time, the decision leaves several key issues unresolved.

The CFAA and the Supreme Court's Decision in Van Buren

The CFAA creates a criminal offense, and also permits civil recovery against anyone who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains" information.[3] As amended, the CFAA applies broadly to any computer that connects to the Internet.[4]

In *Van Buren*, the Supreme Court resolved a split among federal circuit courts of appeal concerning just how broadly the law should apply. At issue was the meaning of the term "exceeds authorized access," which the CFAA defines 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."[5]

Van Buren involved the criminal conviction under the CFAA of Nathan Van Buren, a police sergeant in Georgia. Van Buren used his patrol-car computer to access a law enforcement database to run the license plates of a woman whom an acquaintance had met at a local strip club.[6] Cooperating with the FBI as part of a sting operation, the acquaintance promised to pay Van Buren $5,000 for the information.[7] Van Buren had been trained not to use the law enforcement database for improper purposes, such as personal use.[8] The Government obtained a conviction under the CFAA by arguing that, although he was permitted to access the database for law-enforcement purposes, Van Buren had unlawfully exceeded authorized access by using the database for a personal purpose.[9]

In a 6-3 decision, the Supreme Court disagreed and reversed the Eleventh Circuit's decision affirming Van Buren's conviction. The sole issue before the Supreme Court was whether Van Buren was "entitled so to obtain" the specific record from the law enforcement database.[10] There was no dispute that hewa s authorized to access the database when related to his duties as a law enforcement officer.[11]

The Court held that because Van Buren had authority to access the database as part of his job, he could not be convicted under the CFAA for misusing that access.[12] Writing for the majority, Justice Barrett explained that "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."[13] Van Buren's conduct did not satisfy this standard because he did not access any area of a computer system that was "off limits" to him; instead, he merely accessed the law enforcement database with an improper purpose.[14]

The Court's decision significantly reduces the scope of conduct that the CFAA criminalizes and subjects to civil liability.

Implications for Cybersecurity

The decision has a number of cybersecurity implications for businesses, ranging from insider threats to vulnerability disclosure programs.

Review of Employee Access and Network Management. Many companies with sensitive and proprietary data provide their employees or contractors network access conditioned on appropriate business uses, identified in click-through banners, employment contracts, or employee handbooks. For example, an employee or contractor may be granted credentialed access to a company's intellectual property or other sensitive business information on the condition that they only use the access for approved purposes. But given the Court's interpretation of authorization under CFAA as a "gates-up-or-down" concept,[15] companies may need to revisit these policies with *Van Buren*'s holding in mind. In particular, if the goal is to deter harmful computer use through civil or criminal enforcement of the CFAA, revising contractual, policy, or banner language to explicitly bar access to certain content or files will be a critical step, potentially with accompanying technological restrictions.[16] In addition, companies concerned with potential insider threats will want to engage in a comprehensive review of their network management to identify which users have access to sensitive information, where that information is located, and whether the access is warranted. The effort would ideally involve both IT and legal departments, with the goal of ensuring that (1) sensitive data is clearly identified and separated within the network, and (2) authority to access data is clearly and unambiguously conveyed and/or technically restricted to only those with a need to know.

Data Scraping and Terms of Service. 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 copying data or taking up bandwidth. But the *Van Buren* decision makes clear that the CFAA's "exceeds authorized access" provision does not apply to data scraping if the offending party is authorized to access the website at all, thereby limiting the legal effect of the terms of service.[17] Under *Van Buren*, the federal CFAA is not a remedy for website owners absent further action to revoke authorization from an offending party. As a practical matter, website owners that seek to protect their information may—at a minimum—need to take additional steps to monitor and detect efforts by scraping entities, identify the source, and clearly revoke all authorization (again, including through the use of technological measures). In the alternative, website owners will want to consider whether to shift from a publicly-accessible site to a gated one, in which they can exercise a greater degree of control over who may access the site in the first instance and more easily monitor and revoke authorization as desired.

Computer Security Research. 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. The computer security research community largely favored Van Buren's position because of the chilling effect of a potential CFAA prosecution on their work. Now that the Court has adopted that view, however, entities engaged in a bug bounty program may want to revisit how their authorizations are structured and the technical accesses that are granted, in consultation with counsel.

Impact on Trade Secrets Litigation

As the law and technology developed since the CFAA was enacted in 1986, the CFAA's civil liability provisions (§ 1030(g)) became an additional tool for victims of trade secret misappropriation that occurred by use of a computer. Before *Van Buren*, the First, Fifth, Seventh, and Eleventh Circuits had adopted the broad view of "exceeds authorized access" espoused by the Government in *Van Buren*.[18] In those circuits, an employee with access to his employer's computer network for business purposes could be prosecuted or sued under an "exceeding authorized access" theory if the employee accessed data for the employee's own self-interest.[19] This interpretation allowed trade secrets plaintiffs to bring CFAA claims alongside applicable trade secrets claims, and in some instances to prevail under the CFAA even where they could not meet all of the elements of a claim for trade secret misappropriation.

The *Van Buren* holding, which sided with the narrow reading that had been adopted by the Second, Fourth, Sixth, and Ninth Circuits, will significantly restrict those types of claims.[20] However, the CFAA after *Van Buren* still imposes civil liability for traditional hacking, as well as situations where an employee accesses a location—defined by Justice Barrett to include "files, folders, or databases"—on the employer's computer system that the employee is not permitted to access at all or that the employee accesses only after authorization had been terminated or revoked.

A Narrowed Definition of "Loss"?

The *Van Buren* decision may suggest an additional hurdle for trade secret and other plaintiffs seeking to prove civil liability under the CFAA. As part of its analysis explaining that the CFAA was designed to address traditional hacking, the Supreme Court articulated a view of the CFAA's civil "damage" and "loss" provisions that is narrower than the interpretation adopted among some lower courts.

Under the CFAA, plaintiffs pursuing a private cause of action must demonstrate, in addition to the other elements of liability, either "damage" or "loss."[21] The CFAA defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information,"[22] and "loss" as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service."[23] Reviewing these definitions as part of its assessment of the meaning of the CFAA's "exceeds authorized access" provision, the Supreme Court stated that the terms "damage" and "loss" "focus on technological harms—such as the corruption of files—of the type unauthorized uses cause to computer systems and data" and are "ill fitted . . . to remediating 'misuse' of sensitive information that employees may permissibly access using their computers."[24]

Defendants facing a CFAA claim may point to the Court's comments about the definition of "loss" to try to further narrow the scope of CFAA's civil liability provisions. Before *Van Buren*, some courts had focused on the "any reasonable cost to any victim" portion of the definition of "loss" and concluded that "loss" could occur without any technological damage or interruption in service and cover the use (or misuse) of data obtained by a party in violation of the CFAA. For example, some district courts around the country had determined that "loss" under the CFAA means both (1) the costs associated with technical interruptions, restoring affected data, and responding to the violation, as well as (2) consequential losses from the misuse of data obtained by the defendant.[25] The Court's reasoning in *Van Buren*—though arguably only *dicta*—affirmatively endorses only the first type of loss. The Supreme Court's comments thus reinforce the need for trade secrets plaintiffs who seek to assert a claim under the CFAA to evaluate carefully the costs they have incurred as a result of the defendant's unauthorized access and to pay particular attention to gathering evidence of any costs related to remedying technological harms caused by the unauthorized access, and not just the misuse of data thereby obtained (which now may be outside the scope of recovery entirely).

Open Questions and What Comes Next

While this decision resolves a long-standing circuit split, the Court leaves open a number of important issues that are likely to be front and center in future CFAA litigation. First and foremost, the opinion expressly reserves whether the concept of "authorization" under the CFAA "turns only on technological (or 'code-based') limitations on access," or "also looks to limits contained in contracts or policies."[26] In other words, *Van Buren* tells us that CFAA liability for "exceeds authorized access" turns on whether a party has the requisite authorization, but does not clarify what that authorization must consist of. How authorization is defined and communicated (and in particular, whether it requires code-based restrictions, such as password requirements) will almost certainly be the next significant dispute.

Second, and relatedly, the decision does not tell us what the default is with respect to authorization. In other words, must authorization be expressly given in order for computer resources to be accessed, or must it be expressly revoked to limit access? For example, it may be that a person browsing the public internet is presumed to have authorization to access any website that they can navigate to. But a person who is on a sensitive corporate system might be presumed to lack authorization unless explicitly granted. Whether authorization is a one-size-fits-all or a context dependent inquiry remains an open question.

Finally, it is important to keep in mind that the CFAA is an important computer crime law, but not the only one. Many states have CFAA analogs that are worded or interpreted differently. Some of them may clearly prohibit the type of computer misuse at issue in *Van Buren*, while others may use different language that the Court's reasoning does not reach. Whether and to what degree this opinion influences interpretation of analogous state laws remains to be seen.

Contact Us

Debbie L. Berman

dberman@jenner.com | Download V-Card

David Bitkower

dbitkower@jenner.com | Download V-Card

April A. Otterberg

aotterberg@jenner.com | Download V-Card

Shoba Pillay

spillay@jenner.com | Download V-Card

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

Andrew J. Plague
aplague@jenner.com | Download V-Card

Eric S. Fleddermann
efleddermann@jenner.com | Download V-Card

Meet our Trade Secrets and Restrictive Covenants Team

Meet our Data Privacy and Cybersecurity Team

Practice Leaders

Debbie L. Berman
Co-Chair, Trade Secrets and Restrictive Covenants
dberman@jenner.com
Download V-Card

Nick G. Saros
Co-Chair, Trade Secrets and Restrictive Covenants
nsaros@jenner.com
Download V-Card

Andrew W. Vail
Co-Chair, Trade Secrets and Restrictive Covenants
avail@jenner.com
Download V-Card

David Bitkower
Chair, Data Privacy and Cybersecurity
dbitkower@jenner.com
Download V-Card

[1] *Van Buren v. United States*, 593 U.S. ___ (2021).

[2] Jenner & Block previously wrote about the case and the parties' positions here: Why the Supreme Court's Decision in Van Buren May Be Felt beyond Criminal Law (jenner.com).

[3] 18 U.S.C. § 1030(a)(2), (c), (g).

[4] *Id.* § 1030(a)(2)(C), (e)(2)(B).

[5] *Id.* § 1030(e)(6).

[6] *Van Buren*, slip op. at 3.

[7] *Id.*

[8] *Id.* at 4.

[9] *Id.*

[10] *Id.* at 5.

[11] *Id.*

[12] *Id.* at 1.

[13] *Id.* at 20.

[14] *Id.*

[15] *Id.* at 13–14.

[16] As noted below, whether authorization requires technological measures or may be communicated in other ways, such as policies, contracts, or other terms of use, remains unresolved.

[17] *Van Buren* does not touch on the CFAA's prohibitions on computer damage, at 18 U.S.C. § 1030(a)(5). Data scraping that meets the statutory definition of "damage" under the statute may still be prohibited.

[18] *See United States v. Rodriguez*, 628 F. 3d 1258 (11th Cir. 2010); *United States v. John*, 597 F, 3d 263 (5th Cir. 2010); *Int'l Airport Ctrs., L.L.C. v. Citrin*, 440 F. 3d 418 (7th Cir. 2006); *EF Cultural Travel BV v. Explorica, Inc.* 274 F. 3d 577 (1st Cir. 2001).

[19] *See id.*

[20] *See Royal Truck & Trailer Sales & Serv., Inc. v. Kraft*, 974 F. 3d 756 (6th Cir. 2020); *United States v. Valle*, 807 F. 3d 508 (2nd Cir. 2015); *WEC Carolina Energy Solutions LLC v. Miller*, 687 F. 3d 199 (4th Cir. 2012); *United States v. Nosal*, 676 F. 3d 854 (9th Cir. 2012) (en banc).

[21] 18 U.S.C. § 1030(g).

[22] *Id.* § 1030(e)(8).

[23] *Id.* § 1030(e)(11).

[24] *Van Buren*, slip op. at 15.

[25] *See, e.g.*, *C.H. Robinson Worldwide Inc. v. Command Transp. LLC*, No. 05 C 3401 (SE), 2005 WL 3077998, at *2–*3 (N.D. Ill. 2005); *Four Seasons Hotel & Resorts BV v. Consorcio Barr, SA*, 267 F. Supp. 2d 1268, 1324 (S.D. Fla. 2003).

[26] *Van Buren*, Slip Op. at 9 n.8.
