GIBSON DUNN

Supreme Court to Resolve Longstanding Circuit Split Over Scope of Federal Anti-Hacking Statute

Client Alert | April 22, 2020

On Monday, April 20, 2020, the U.S. Supreme Court granted certiorari in *Van Buren v. United States*, No. 19-783, to address a decade-long circuit split regarding the scope of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, a statute the Supreme Court has never before interpreted and that is routinely invoked in both criminal and civil settings. The case gives the Court an opportunity to decide whether a person or entity legitimately authorized to access a computer for one purpose, but accesses it for some other unauthorized purpose, violates the CFAA. The case has far-reaching implications for how millions of Americans interact with websites and use the Internet, including shaping potential criminal and civil liability for individuals who violate commonplace terms of service or exceed the scope of authorized use of their employer-provided email, computers, and databases. It also has implications for companies drafting or revising their terms of service, updating their employee Internet or email policies, or engaging in business operations that may be seen as data "scraping," among other situations.

Statutory Background

Congress first enacted Section 1030 in 1984, long before worldwide access to the Internet existed and before personal computers became ubiquitous. The purpose of the statute was to deter "the activities of so-called 'hackers' who" were accessing "both private and public computer systems." H.R. Rep. No. 98-894, at 10 (1984). Two years later, Congress amended the statute, and it became known as the CFAA. Over the years, Congress has further amended the statute to cover a broad range of "protected" computers, which include servers and other technologies connected to the Internet.

The CFAA covers multiple types of unlawful computer access and, in relevant part, provides that "[w]hoever . . . intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer," commits a federal crime and may face civil liability. 18 U.S.C. § 1030(a)(2). The phrase "exceeds authorized access," which is an operative clause in a number of the provisions in the statute, 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." *Id.* § 1030(e)(6); *see also id.* § 1030(a)(1), (2), (4), (7). A "protected computer" is any computer that "is used in or affect[s] interstate or foreign commerce or communication of the United States." *Id.* § 1030(e)(2)(B).

Violations of the CFAA can result in both criminal and civil liability. A criminal conviction under the "exceeds authorized access" provision of the CFAA is typically a misdemeanor, but can be a felony punishable by fines and imprisonment of up to five years in certain situations, including where the offense was committed for "commercial advantage or private financial gain." *Id.* § 1030(c)(2)(A), (B).

Importantly, the statute also authorizes civil suits for compensatory damages and injunctive or other equitable relief by parties who show, among other things, that a

Related People

Matt Benjamin

Doran J. Satanove

violation of the "exceeds authorized access" provision caused them to "suffer[ ] damage or loss." *Id.* § 1030(g). That provision is often invoked in civil suits around the country.

Circuit Split

For years, the courts of appeals have split over whether a person "exceeds authorized access" under Section 1030(a)(2) by using authorized computer access for an unauthorized purpose.

On the one hand, the Second, Fourth, and Ninth Circuits have taken a narrow view, holding that a person "exceeds authorized access" only if he accesses information on a computer that he is prohibited from accessing—activity analogous to "breaking and entering" in the digital space. *See United States v. Valle*, 807 F.3d 508, 523–28 (2d Cir. 2015); *WEC Carolina Energy Sols. LLC v. Miller*, 687 F.3d 199, 205–06 (4th Cir. 2012); *United States v. Nosal (Nosal I)*, 676 F.3d 854, 857–63 (9th Cir. 2012) (en banc); *see also hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985, 999–1002 (9th Cir. 2019). Under this view, for example, an employee who downloads confidential information from a company database that he is authorized to access, but who does so for the improper purpose of disclosing the information to someone outside the company, has *not* violated the CFAA. *See Nosal I*, 676 F.3d at 857–63. Nor has a company that uses automated bots to scrape information from another company's public webpage in violation of the website's terms of use. *hiQ Labs, Inc.*, 938 F.3d at 999–1002.

On the other hand, the First, Fifth, and Seventh Circuits have taken a broader view, holding that a person "exceeds authorized access" if, even using a computer to access information that he is legitimately authorized to access, he does so for an improper or unauthorized purpose. *See United States v. John*, 597 F.3d 263, 271–72 (5th Cir. 2010); *Int'l Airport Ctrs., L.L.C. v. Citrin*, 440 F.3d 418, 420–21 (7th Cir. 2006); *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 581–84 (1st Cir. 2001). Under this view, for example, an employee who downloads confidential information from an internal company system that he is authorized to access in the course of his official duties, but who does so for the improper purpose of using that information to perpetrate a fraud or for some other unauthorized purpose, *has* violated the "exceeds authorized access" prong of the CFAA. *See John*, 597 F.3d at 272–73. So too has a company that uses data?scraping software to systematically glean a competitor's prices from the competitor's public website. *EF Cultural Travel BV*, 274 F.3d at 583–84.

In *Van Buren*, the Eleventh Circuit joined those circuit courts that have taken a broader view of the CFAA's statutory sweep, affirming the conviction and eighteen-month sentence of a police officer who used a computer to look up an exotic dancer's license plate number in exchange for a loan. The Eleventh Circuit reasoned that Van Buren "exceed[ed] authorized access" to the law-enforcement computer system when he used his legitimate access for an improper purpose, even though he had permission to access the database for other purposes. *United States v. Van Buren*, 940 F.3d 1192, 1205–07 (11th Cir. 2019). The court explained that it was bound by a previous decision in *United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010), which established that "even a person with authority to access a computer can be guilty of computer fraud [under the CFAA] if that person subsequently misuses the computer," *Van Buren*, 940 F.3d at 1207. Under that interpretation of "exceeds authorized access," there was "no question" that the record contained sufficient evidence for a jury to convict Van Buren of computer fraud. *Id.* at 1208.

Policy Implications

Although the Supreme Court might decide *Van Buren* narrowly based on the unique facts and procedural posture of the case, it is possible that the Court will take this opportunity to resolve the circuit split and to provide guidance about the scope of the CFAA's "exceeds authorized access" provision. If the Court does so, it will need to balance many competing policy interests.

For example, those in favor of a narrow interpretation of the CFAA assert that the statute was not intended to be an all-purpose computer and Internet policing statute, but instead was intended to prohibit more egregious unauthorized access to computer systems akin to hacking. An expansive reading of the statute, they contend, would subject individuals to civil or criminal liability for innocuous computer or Internet use, as when an individual violates a website's terms of service or a school's or employer's computer use policy.

In support of the petition for a writ of certiorari, the Electronic Frontier Foundation and other *amici curiae* even hypothesized that thousands of employees of federal government agencies, such as the Department of the Interior and U.S. Postal Service, would risk criminal prosecution under a broad interpretation of the statute if they violate their respective agency's prohibitions against personal video streaming from commercial or news organizations on government-issued devices while connected to a government network.[1] The same rationale would apply in the context of potential civil liability, wherein a broad interpretation of the CFAA could subject countless individuals to substantial damages awards or onerous court-ordered injunctions for violations of computer or Internet policies.

Those endorsing the narrow view also contend that a broad construction of the statute would give prosecutors too much discretion and lead to arbitrary or discriminatory enforcement. They cite as an example Internet "hacktivist" and Harvard University student Aaron Swartz, who was indicted for unlawfully accessing MIT's computer network (where he was in fact an authorized user) and downloading a large number of academic journal articles in violation of the network's terms of use. Swartz tragically took his own life before standing trial.

Supporters of the narrow view further posit that a broad construction of the CFAA would put the statute on a collision course with the First Amendment by punishing online investigative techniques commonly used by journalists, academic researchers, private investigators, and others engaged in expressive conduct or speech that may also run afoul of computer or Internet terms of use.

By contrast, those in favor of a broader interpretation of the CFAA contend that an expansive interpretation of the statute is more consistent with congressional intent—to stop bad actors from computer-facilitated fraud and theft, in addition to hacking. These proponents argue that fears of over-zealous or arbitrary criminal enforcement are overblown, particularly in light of DOJ guidance setting forth a uniform charging policy for computer crimes. They also contend that a more expansive interpretation of the CFAA promotes a safer Internet that benefits and protects both companies and consumers alike, and can curb what some perceive to be unfair competitive intelligence practices, such as when a company scrapes data from the websites of competitors.

The Supreme Court's decision in *Van Buren* may provide much-needed clarity on these and other issues, giving companies, consumers, and law enforcement a better understanding of what type of online and computer conduct is subject to civil and criminal liability under the CFAA. Any such guidance, in turn, would establish new parameters that companies—and others potentially liable for the activities of their agents—should closely follow when revising both their online terms of use and their internal policies governing how employees may use email, computers, and other technologies when logged onto an internal (or external) network.

---

[1] Brief for Electronic Frontier Foundation et al. as Amici Curiae Supporting Petitioner, *Van Buren v. United States*, No. 19-783 (2020), at 18–19.

Gibson Dunn's lawyers are available to assist with any questions you may have regarding these developments. For additional information, please contact the Gibson Dunn lawyer with whom you usually work, any member of the firm's Appellate and Constitutional Law

and Litigation practice groups, or the following authors:

Authors: Avi Weitzman, Matthew Benjamin, Joel M. Cohen, Alexander H. Southwell, Brandon Boxler, Erica Sollazzo Payne, Doran Satanove, and Samantha Weiss

Related Capabilities

Appellate and Constitutional Law

Privacy, Cybersecurity, and Data Innovation