PLI Chronicle

July 2021

(Un)Authorized Access to Computers in the Wake of *Van Buren v. United States*

Edward R. McNicholas, Frances Faircloth, and Shong Yin

Ropes & Gray LLP

On June 3, 2021, in a 6-3 decision that created a diverse majority—uniting the most recent conservative additions—Justices Barrett, Kavanaugh, and Gorsuch—with the more liberal Justices Breyer, Sotomayor, and Kagan, the Supreme Court resolved a split among the Circuit courts regarding the Computer Fraud and Abuse Act (the CFAA), The language of the CFAA creates civil and criminal liability for intentional access of a computer if that access is either "without authorization" or "exceeding authorized access." In *Van Buren v. United States,* the Supreme Court granted review to determine whether someone who was authorized to use a computer system exceeded authorized access under the CFAA by using that computer system to access information for an unauthorized purpose. Justice Barrett wrote the majority opinion which determined that using information from a computer system for unpermitted purposes would not "exceed authorized access" under the CFAA if the user was otherwise authorized to access that information using the computer.

The question of what constitutes "exceeding authorized access" is not the only ambiguity in the CFAA to prompt litigation over the last thirty years, particularly as the thirst for alternative data has lead many companies to scrape data from websites.

That question came up in a summary disposition from the Supreme Court a few days later. On June 14, 2021, the Supreme Court granted certiorari in *LinkedIn v. hiQ Labs*, only to vacate the Ninth Circuit's decision and remand the case for further consideration in view of *Van Buren*. By issuing this summary disposition, the Court suggested that it had changed the frame of reference for reviewing CFAA cases in *Van Buren,* but it left to the Ninth Circuit to apply that new framework to the closely watched scraping issues presented by the facts in *LinkedIn*. In doing so, the Court ensured that these remaining questions about access and authorization in the CFAA will be a source of continued debate and litigation as the courts struggle to apply a decades-old law to modern technology in an environment awash in alternative data.

Background of the CFAA

The environment in which the CFAA applies has materially changed since it was passed in 1986. Congress initially enacted the CFAA to safeguard information on "protected computers" at government and financial institutions, but the law defined "protected computers" broadly to include information on any computer "used in or affecting interstate or foreign commerce or communication." As Justice Barrett notes in the *Van Buren* opinion, "the prohibition now applies—at a minimum—to all information from all computers that connect to the Internet," which includes servers and other devices that manage resources and information for a network. While the definition might have included only a limited number of computers in 1986, it now covers virtually any computer.

Originally, the law was conceived with the primary objective of imposing criminal penalties for hackers and other cybercriminals, but Congress amended the CFAA in 1994—that is, before commercial websites—to add a civil cause of action for private plaintiffs to seek compensatory damages and injunctive relief, including temporary restraining orders to prevent or limit damages from CFAA violations. Since then, the CFAA has become key to how companies operate in cyberspace by giving companies the ability to bring claims against internal and external cybercriminals but also by criminalizing some corporate behaviors, such as "hack backs" as an offensive measure by companies.

For the purposes of stating a claim, the CFAA defines "damage" broadly as "any impairment to the integrity or availability of data, a program, a system, or information," 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." Some courts have understood this to limit the CFAA's civil remedies to remediation of technical harms to computer systems rather than damages from misuse of improperly accessed data. Businesses whose computer systems were accessed illegally have been successful bringing CFAA claims to recover costs arising from harms to computer systems and disruptions in service (e.g., remediation for damages caused by ransomware and other cyberattacks). For nearly three decades, technology has evolved while the CFAA's text has stayed the same.

Considering changes in computing systems and the growing sophistication of computer users, entities have tried to use the CFAA to prevent other activities that they view as misuse of their computer systems. The *Van Buren* case is a great example in which an employee faced criminal charges for accessing information on a computer system that he was otherwise authorized to access, but which he allegedly accessed for an unauthorized purpose. Courts have been divided about whether the CFAA's prohibition on "exceeding authorized access" stretches to cover such activities. Another twenty-first century use of the CFAA that has divided courts is the law's application to scraping programs or bots that harvest large amounts of public information or customer data. Courts disagree about whether access of this publicly available information can ever be "unauthorized" under the CFAA, and there is ongoing public debate about whether these applications of the CFAA result in over-enforcement.

Van Buren v. United States

The CFAA imposes criminal and civil liability on anyone who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer." The CFAA does not define "without authorization," which has been the subject of much litigation. As discussed above, a Circuit split has emerged in recent years about the meaning of the "exceeding authorized access" provision. The Second, Fourth and Ninth circuits have followed a narrow reading, which interprets the phrase to apply only where an otherwise authorized user accesses information on the computer that they are not authorized to access. *See, e.g.*, *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*, 676 F.3d 854, 863 (9th Cir. 2012) (en banc). Meanwhile, the First, Fifth, Seventh and Eleventh Circuits have adopted a broad interpretation of the phrase, which prohibits not only accessing information without authorization but also accessing information on a computer for unpermitted purposes, even if the user was otherwise authorized to access that information. *See, e.g.*, EF *Cultural Travel BV v.*

Explorica, Inc., 274 F.3d 577, 581–84 (1st Cir. 2001); *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).

Van Buren brought this split squarely in front of the Supreme Court. The petitioner, Nathan Van Buren, was a Georgia police sergeant who accepted payment from a non-law enforcement acquaintance in exchange for providing information from a vehicle database available only to law enforcement. Van Buren's acquaintance, who was actually an informant, told Van Buren that he believed that a woman with whom he was doing business was an undercover officer. He asked Van Buren to search the police database for the woman, in exchange for money that Van Buren had asked the informant to loan him. Van Buren agreed and searched the Georgia Crime Information Center (GCIC) database, a government database maintained by the Georgia Bureau of Investigation (GBI), for a license plate number for the woman, which the informant provided. Van Buren was caught and confessed to conducting the search to learn whether the woman was an undercover officer.

As police sergeant, Van Buren had valid credentials to the GCIC database and was authorized to view the information related to the license plate record for the woman (which, incidentally, was a fake record planted as part of the sting operation). He had also, however, completed police training that explained that officers were authorized to search the database only for law enforcement purposes. Because the department viewed Van Buren's violation of this policy as exceeding his authorized access, Van Buren was tried and convicted of violating the CFAA. Van Buren appealed his conviction to the Eleventh Circuit Court of Appeals, which affirmed his conviction.

Van Buren Before the Supreme Court

Even before certiorari was granted, *Van Buren v. United States* had caught the attention of many interest groups on both sides who saw the debate as key to the ability of entities to protect their information, to the free and fair exchange of ideas, and to the potential over-criminalization of innocent behaviors. More than twenty entities filed amicus briefs in the case. Van Buren and his amici argued that extending the CFAA to criminalize accessing information on a computer for unpermitted purposes, even when the user was otherwise authorized to access that information, would lead to criminalization of even the most insignificant violations of terms-of-use and could infringe on academic and political researchers' First Amendment rights. The government, joined by amici that included business associations, argued in return that criminalizing access of information for unpermitted purposes was essential to

protecting systems from users with only minimal privileges who could steal information that is beyond their authorization.

Writing for the diverse six-justice majority, Justice Barrett focused first on the statute's text. The opinion focuses on the CFAA's definition of "exceeding authorized access"—which makes it a crime 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." Those last few words are where the crux of the dispute lies—while the parties agree that Van Buren was entitled to obtain the information, they disagree about whether he was entitled *so* to obtain the information, with Van Buren arguing that "so" has to refer to something and therefore must refer to accessing information on a computer with authorization, which he had. The government, however, argued that "so" referred to the manner in which, or purpose for which, Van Buren accessed the information, and in this case, that purpose was not authorized. The Court did not find this reading convincing, siding with Van Buren and holding that the work of the phrase is to address a user who is authorized to access a computer but may not be authorized to access all information on that computer. The opinion goes on to provide additional support for this interpretation of the statute in the structure of the law, the statutory history, and policy considerations. Justice Thomas, joined by Chief Justice Roberts and Justice Alito, penned a dissent in which he borrowed concepts from property law to argue that Van Buren was entitled to view the information but was not entitled to view it for that purpose, just as there can be limitation placed on how someone may be entitled to use property.

The Free Speech Elephant in the Room

Looming large over the opinion and the dissent, but never stated outright, are significant First Amendment considerations. The only hint at this issue in the opinion comes in the penultimate paragraph, where Justice Barrett makes "[o]ne final observation." Justice Barrett notes that the government has agreed—"as it must"—that the prohibition on access for unauthorized purposes could not be extended to later "misuse" of the information. Justice Barrett's aside of "as it must" underscores one of the key problems with the broad interpretation of the prohibition on "exceeding authorized access"—it comes dangerously close to placing impermissible speech restrictions on otherwise authorized users. While the government argues that Van Buren's later use is only evidence of the purpose for which the information was obtained, reading a purpose limitation into the CFAA would effectively restrict the way in which an individual can share information that they are authorized to obtain.

The commercial implications of these First Amendment concerns were articulated in the Court's 2011 decision in *Sorrell v. IMS Health Inc.*, which held unconstitutional a Vermont law on the grounds that it impermissibly restricted free speech based on the content of the speech and on the identity of the speaker. The law at issue prohibited the sale, disclosure or use of information about doctors' prescribing practices, but only for marketing purposes. The Court found that this purpose restriction was impermissible because it disfavored "speech with a particular content" and could not withstand heightened judicial scrutiny. Presumably, the Court avoided getting into whether the government was actually proposing a purpose or use restriction because there were more clear-cut rationales supporting Van Buren's reading of the statute, but these First Amendment considerations should not be overlooked, especially as we have not likely heard the end of litigation debating the meaning of provisions in the CFAA.

Commercial Scraping of Alternative Data: *LinkedIn* v. *hiQ Labs*

Indeed, less than two weeks after issuing its decision in *Van Buren*, the Court issued a summary disposition in another CFAA case, *LinkedIn* v. *hiQ Labs*. The *LinkedIn* case asked the Court to address whether individuals can be liable for accessing publicly posted information without any explicit authorization. LinkedIn asserted that hiQ violated the CFAA by circumventing technical barriers aimed to prevent hiQ from harvesting otherwise publicly available data related to millions of individuals across LinkedIn's platform. LinkedIn sent cease and desist letters to stop hiQ's activities and disabled access to IP addresses that hiQ was using, but hiQ continued to automatically access and scrape publicly available information from LinkedIn's sites. The trial court ruled in favor of hiQ, allowing the scraping to continue, and the Ninth Circuit affirmed.

The Ninth Circuit followed its precedent from previous cases and gave the term "without authorization" the "plain and ordinary meaning" of "accessing a protected computer without permission." The court then went on to explain that the cease-and-desist letter that LinkedIn sent hiQ did not effectively create a lack of authorization where authorization was not required, but rather it was an attempt to forbid access. The Ninth Circuit then cited statutory history, explaining that hiQ's actions were not similar to the types of activities the CFAA was designed to prevent, as they were not analogous to "breaking and entering" but rather to entering an open space; it therefore held that accessing publicly available data, for which no authorization is normally required, is not a violation of the CFAA.

The Ninth Circuit's *LinkedIn* opinion, which ruled that no authorization is necessary to access publicly posted information, created a split with the First Circuit Court of Appeals, which found in an earlier decision that there is no presumption of open access to Internet information. Citing that circuit split, LinkedIn petitioned the Supreme Court to weigh in on whether hiQ violated the CFAA by circumventing technical barriers to access its websites, even after LinkedIn expressly informed hiQ that it was not authorized to access those websites. LinkedIn's petition was pending before the Supreme Court for more than a year before, on June 14, 2021, the Court granted the petition. Immediately upon granting the petition, however, the Court issued a summary disposition vacating the Ninth Circuit's decision and remanding the case for further consideration in light of the *Van Buren* decision.

It will be interesting to see how the Ninth Circuit interprets the *Van Buren* decision as applying to *LinkedIn*. Presumably, the *Van Buren* decision will only give the court additional grounds for ruling in favor of hiQ, because LinkedIn is effectively trying to establish a proactive purpose limitation on the collection and use of information from its network. We will be watching closely for the ways in which First Amendment considerations may weave their way into these discussions of authorizing and restricting access to information. These difficulties in applying a law created in the 1980s and last amended in the 90s to the technological situation in the 2020s could of course prompt Congress to clarify these provisions instead of leaving it to the courts, but the Ninth Circuit will no doubt rule first.

Edward McNicholas is a co-leader of Ropes & Gray's privacy & cybersecurity practice, where he represents technologically sophisticated clients facing complex data, privacy, and cybersecurity issues. He is also the co-editor of Cybersecurity: A Practical Guide to the Law of Cyber Risk, available from PLI Press.

Fran Faircloth is an associate and core member in Ropes & Gray's data, privacy, and cybersecurity practice.

PLI Programs you may be interested in:

Cybersecurity 2021: Managing Cybersecurity Incidents

Also available from PLI Programs On Demand:

Cybersecurity and Legal Ethics

Cybersecurity: Data Breach Scenario

Also available from PLI Press:

Proskauer on Privacy: A Guide to Privacy and Data Security Law in the Information Age (Second Edition) (read now on PLUS)

Advanced Data Privacy, Cybersecurity and TCPA Class Action Litigation 2021 (read now on PLUS)

Disclaimer: The viewpoints expressed by the authors are their own and do not necessarily reflect the opinions, viewpoints and official policies of Practising Law Institute.

To submit an article for consideration, please contact the editor at:
editor.plichronicle@pli.edu

This article is published on PLI PLUS, the online research database of PLI. The entirety of the PLI Press print collection is available on PLI PLUS—including PLI's authoritative treatises, answer books, course handbooks and transcripts from our original and highly acclaimed CLE programs.

Sign up for a free trial of PLI PLUS at pli.edu/pliplustrial.