Proskauer

Supreme Court Ends Long-Running Circuit Split over CFAA "Exceeds Authorized Access" Issue, Adopting a Narrow Interpretation That Will Reverberate in Scraping Disputes and Litigation over Departing Employees

New Media and Technology Law Blog on **June 6, 2021**

In a closely-watched appeal, the Supreme Court, in a 6-3 decision, reversed an Eleventh Circuit decision and adopted a narrow interpretation of "exceeds unauthorized access" under the Computer Fraud and Abuse Act (CFAA), ruling that an individual "exceeds authorized access" when he or she 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 or her. (*Van Buren v. United States*, No. 19-783, 593 U.S. ___ (June 3, 2021)). The majority equated "exceed[ing] authorized access" with the act of "entering a part of a system to which a computer user lacks access privileges," rejecting the Government's contention that a person who is authorized to access information from a protected computer for certain purposes violates CFAA Section 1030(a)(2) by accessing the computer with an improper purpose or motive. Put simply, the court's view suggests a "gates-up-or-down" approach where the CFAA prohibits accessing data one is not authorized to access.

Although the case involved a criminal conviction under the CFAA, *Van Buren* gave the Supreme Court the opportunity to resolve a long-standing circuit split and heavily-litigated issue that arose in both criminal and civil cases under the CFAA's "unauthorized access" provision. This provision of the CFAA is routinely pled in cases against former employees that have accessed proprietary data in their final days of employment for an improper purpose (e.g., for use in their new job or competing venture). It is also a common claim in disputes involving unwanted web scraping. On the latter point, the Court's narrow interpretation of the "exceeds authorized access" provision would appear to be right in line with the narrow interpretations of the CFAA enunciated by the Ninth Circuit in its blockbuster *hiQ* opinion, which held that that when a computer network generally permits public access to its data, a user's accessing that publicly available data will not constitute access "without authorization" under the CFAA and in its *Power Ventures* precedent, which held that, in the context of unwanted data scraping, a violation of the terms of use of a website, without more, cannot be the basis for civil liability under the CFAA.

The issue before the Supreme Court in *Van Buren* was: "Whether a person who is authorized to access information on a computer for certain purposes violates Section 1030(a)(2) of the Computer Fraud and Abuse Act if he accesses the same information for an improper purpose." Primarily a criminal statute, the CFAA is designed to combat hacking, making it a crime to "intentionally access[ ] a computer without authorization or exceed[ ] authorized access, and thereby obtain[ ] information from any department or agency of the United States." 18 U.S.C. § 1030(a)(2)(B). Those who violate §1030(a)(2) face penalties ranging from fines and criminal penalties; the statute also permits a private party "who suffers damage or loss by reason of a violation of [the CFAA]" to bring a civil action for money damages and equitable relief. 18 U.S.C. §1030(g).

The *Van Buren* case concerns an appeal of an Eleventh Circuit decision affirming the conviction of a former police officer for violating the CFAA for accessing a police license plate database he was authorized to use but used instead to run a search in exchange for money (i.e., for non-law enforcement purposes that violated department policy). (See *U.S. v. Van Buren*, 940 F. 3d 1192 (11th Cir. 2019)). The appellant Van Buren argued that he did not violate the CFAA because he accessed only databases that he was authorized to use, even though he did so for an inappropriate reason. He contended that the CFAA was being interpreted too liberally and that such a precedent could subject individuals to criminal liability merely for violating corporate computer use policies. In rebuttal, the Government pushed for a broad interpretation of the statute, as espoused by the Eleventh Circuit, and argued that Van Buren's misuse of his access to the police database was the type of harm envisioned under the statute. In the Government's view, the "exceeds authorized access" clause necessarily incorporates purpose-based limits contained in contracts and workplace policies governing database or computer network authorization.

The text of the CFAA does not define "authorization" (but courts have generally interpreted it to mean to access a computer with sanction or permission), but the Act defines "exceeds authorized access" 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." 18 U.S.C. § 1030(e)(6). As we explained in a prior post on CFAA issues, circuit courts have taken divergent views on how to interpret the "exceeds unauthorized access" provision with respect to accessing a database with an improper purpose or against posted policies. Generally speaking, the Second, Fourth, Sixth, Ninth Circuits have held that one who is authorized to access a computer does not exceed her authorized access by violating an employer's restrictions on the use of information once it is validly accessed, while decisions from the First, Fifth, Seventh, Eighth, and Eleventh Circuits have more broadly interpreted "exceeds authorized access."

In adopting a narrow version of the CFAA's "exceeds authorized access" provision, the Supreme Court took a deep dive into: (1) statutory construction (e.g., construing what the word "entitled" and "so" signify at the end of the definition of "exceeds authorized access"… 'that the accesser is *not entitled so to obtain or alter*'); the dissent based its position on the word "entitled" in the statute, stating that a determination of whether an individual "exceeds authorized access" under the CFAA should demand an analysis of intent as to whether access was proper); (2) policy arguments (whether a broad interpretation is against Congressional intent and would disrupt statutory harmony with related provisions of the statute or else grant the Government too much authority to criminalize breaches of computer access policies), and (3) common sense (whether Van Buren's obvious breach of department policy and unethical behavior actually falls within the CFAA's scope). Ultimately, the Court held that the CFAA's "exceeds authorized access" provision covers those who obtain information from computer networks or databases to which their computer access does not extend and "does not cover those who, like Van Buren, have improper motives for obtaining information that is otherwise available to them."

> "The parties agree that Van Buren accessed the law enforcement database system with authorization. The only question is whether Van Buren could use the system to retrieve license-plate information. Both sides agree that he could. Van Buren accordingly did not 'excee[d] authorized access' to the database, as the CFAA defines that phrase, even though he obtained information from the database for an improper purpose."

The Court focused on the statutory text in rejecting the Government's practical argument that Van Buren's dishonest behavior surely fell under the statute, as the phrase "exceeds authorized access" should be understood to mean that Van Buren "exceed[ed] his authorized access" to the law enforcement database when he obtained license-plate information for personal purposes. Putting aside their opinion of Van Buren's misdeeds, the Court stuck to the statute:

> "The relevant question, however, is not whether Van Buren exceeded his authorized access but whether he exceeded his authorized access *as the CFAA defines that phrase.*"

Taking a longer view, the Court also found that a narrow interpretation was suggested by the interplay between the "without authorization" and "exceeds authorized access" clauses of 18 U.S.C. § 1030(a)(2), agreeing with Van Buren's reasoning that the former protects computers from outside hackers without any permission at all while the latter provides "complementary" protection from so-called inside hackers that exceed the parameters of their access:

> "Those clauses specify two distinct ways of obtaining information unlawfully. First, an individual violates the provision when he 'accesses a computer without authorization.' §1030(a)(2). Second, an individual violates the provision when he 'exceeds authorized access' by accessing a computer 'with authorization' and then obtaining information he is 'not entitled so to obtain.' §§1030(a)(2), (e)(6). Van Buren's reading places the provision's parts "into an harmonious whole.' […] The Government's does not."

The Court went on to adopt Van Buren's analogy of the statute as employing a "gates-up-and-down" structure:

> "Van Buren's account of subsection (a)(2) makes sense of the statutory structure because it treats the 'without authorization' and "exceeds authorized access" clauses consistently. Under Van Buren's reading, liability under both clauses stems from a gates-up-or-down inquiry—one either can or cannot access a computer system, and one either can or cannot access certain areas within the system. And reading both clauses to adopt a gates-up-or-down approach aligns with the computer-context understanding of access as entry."

The Court further buttressed its interpretation with equitable arguments about the danger of a broad reading of "exceeds authorized access" that would subject otherwise law-abiding individuals to criminal penalties based on far-reaching computer use policies that often limit use of company computers and devices for business purposes only. The Court stated that the Government's interpretation of the "exceeds authorized access" clause would "attach criminal penalties to a breathtaking amount of commonplace computer activity," such that an employee who reads the news using a work computer would technically violate the CFAA.

Beyond showing concern about how a broad interpretation of the CFAA would "inject arbitrariness into the assessment of criminal liability" with respect to employees' minor violations of computer use policies, the Court also pointed out similar concerns in criminalizing users who might violate website terms of use in commonplace ways. Under the Court's holding, however, CFAA liability for exceeding authorized access would still presumably be available to those who go beyond their authorized access, such as by bypassing authentication walls or password-protected areas or closed databases they are not authorized to access without permission.

As we've seen over the years, the language of the CFAA is susceptible to wide application and has been brought to bear in many contexts beyond traditional hacking scenarios. With the *Van Buren* case, the Supreme Court's narrow view of "exceeds authorized access" brings some clarity in the criminal context as well as for CFAA civil claims based on the same §1030(a)(2) "exceeds unauthorized access" provision. The *Van Buren* ruling will necessarily affect the considerations of companies that seek legal remedies against a departing employee who may have accessed the company network and copied proprietary data for an improper purpose (while he or she still had authorized access to the network). Without the availability of the CFAA for certain instances of improper access, many companies' entrée to federal court may now rest with the federal trade secret statute (DTSA), if applicable, or another litigation strategy.

Still, when it comes to data scraping and website access, open issues remain. The majority's breakdown of the "exceeds authorized access" issue required twenty pages of analysis, but the *Van Buren* case at least presented a clean set of facts: an individual was authorized to access a system and the law enforcement license plate database at issue (even though he did so with an improper purpose). In many instances, however, it is not 100% clear that a party has authorized access to a database or website (or if that access has been revoked) or whether certain files or web pages have been effectively closed off to access.

Final Thoughts and Questions

- **Scraping Cases**. What does the *Van Buren* opinion mean for screen scraping litigation where the CFAA is routinely pled against unwanted data scrapers? One of the hot issues right now in scraping litigation involves the question of what is "unauthorized access." In the *Van Buren* case, the question of authorization and access was more or less clear-cut, but in many scraping disputes, such issues can

be muddy, particularly when technological measures are in play. For example, how would a court rule on the issue of whether a data scraper exceeded authorized access if it bypassed IP address blocks or other technical measures – are those measures more like authorization "gates" or more like use-related policies? A similar question can be asked: whether an entity that uses a bot to bypass a reCAPTCHA challenge or other code-based measure, which acts as a barrier to prevent automated access to certain website content, could constitute "exceed[ing] authorized access" under the CFAA? Or does a user have to unlawfully breach a password-protected database or similarly-restricted web page or file to be liable under the CFAA?

- **Footnote 8.** Interestingly, when the Court discussed the concept of a "gates-up-or-down:" approach to understanding the CFAA's "without authorization" and "exceeds authorized access" clauses, it dropped a footnote that left certain questions for another day: "Under Van Buren's reading, liability under both clauses stems from a gates-up-or-down inquiry—one either can or cannot access a computer system, and one either can or cannot access certain areas within the system.8" In FN8, the Court stated: "For present purposes, we need not address whether this inquiry turns only on technological (or "code-based") limitations on access, or instead also looks to limits contained in contracts or policies." Re-reading the questions presented in the prior bullet in the context of FN8, one finds that the state of the law surrounding data scraping and the CFAA remains unsettled.
- **Round Two?** Having taken its first CFAA "unauthorized access" case, will the Court accept the ongoing petition for a writ of certiorari filed in the *hiQ* web scraping case over the application of the CFAA to unwanted data scraping of publicly available website data? In that case, the issue is: ""Whether a company that deploys anonymous computer 'bots' to circumvent technical barriers and harvest millions of individuals' personal data from computer servers that host public-facing websites—even after the computer servers' owner has expressly denied permission to access the data—'intentionally accesses a computer without authorization' in violation of the Computer Fraud and Abuse Act." Since the *hiQ* and *Van Buren* cases are different, it's possible the Court may decide to accept the *hiQ* appeal. *Van Buren* turned on the meaning of "exceeds authorized access" (and how that provision fit within the "unauthorized access" provision), while *hiQ*'s focus is whether a website operator may revoke a user's access to publicly available website data and thereafter claim any future access was "without authorization." Still, there is a similar feel to both cases – for instance, a statement from hiQ's opposition brief shares the tone of the majority opinion's deliberate analysis of the "exceeds authorized access" issue (hiQ: "The interpretation of the phrase 'without authorization' to exclude viewing and gathering public information—access to

which requires no permission—flows naturally from the plain meaning of the phrase"). Using *Van Buren*'s "gates-up-and-down" approach, the question would perhaps turn on whether a revocation of access to a public website truly lowers the access gate (for purposes of CFAA liability) or whether the gate for public website content is always up and no CFAA liability may arise for such access to publicly available website data.

- **New Technologies**. How will the *Van Buren* decision reverberate in other technology law disputes? Beyond web scraping, the specter of CFAA liability has been raised in the context of security testing, right to repair, access to modern consumer devices or systems, academic research on e-commerce and social media (e.g., research into discriminatory effects of online algorithms) and claims related to breach of website terms (including claims under state computer trespass laws, many of which are modelled after the CFAA). We will see how technology continues to push the bounds of a statute originally drafted in 1984.

View Original

Related Professionals

- **Jeffrey D. Neuburger**