Cooley

US Supreme Court Narrows Scope of Computer Fraud and Abuse Act in Van Buren

June 9, 2021

Introduction

On June 3, 2021, the US Supreme Court issued its decision in *Van Buren v. United States* in the Court's first-ever interpretation of the Computer Fraud and Abuse Act (CFAA), the federal anti-hacking statute. *Van Buren* presented the question of whether someone "exceeds authorized access" under the CFAA, *see* 18 U.S.C. § 1030(a)(2), by accessing a computer in violation of an authorized purpose, such as provided in an employer's computer-use policy or a website's terms of service.

In a 6-3 opinion authored by Justice Amy Coney Barrett, the Court ruled against the government and for the criminal defendant, holding 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." The court rejected the Justice Department's argument that a person may "exceed authorized access" by accessing information on a computer for an "improper purpose" beyond the scope of authorized access (whether by contract, terms of service or other private agreement).

The Court's decision emphasizes that the CFAA is focused on computer hacking, as opposed to "attach[ing] criminal penalties to a breathtaking amount of commonplace computer activity."

United States v. Van Buren

Nathan Van Buren was a state police sergeant authorized to use a database of license plate records for law enforcement purposes. In a sting operation, an FBI informant paid Van Buren to access the license database for personal reasons, which was a violation of departmental policy. Van Buren was convicted of violating the CFAA and sentenced to 18 months in prison. The US Court of Appeals for the Eleventh Circuit affirmed the conviction.

The Supreme Court – which had not ruled on the meaning of the CFAA since its enactment in 1986 – took the case to resolve a circuit split about whether a person who is authorized to access information on a computer for certain purposes violates Section 1030(a)(2) if they access the same information for an improper purpose. The case turned on the meaning of "exceeds authorized access." Van Buren advocated for a narrow reading that would cover only where an authorized individual exceeds the scope of authorization by accessing an area of the computer that is prohibited. This interpretation, Van Buren argued, would align with the CFAA's purpose to prevent hacking and ensure that otherwise authorized persons would not face federal criminal penalties for violating workplace computer-use policies or website terms of service. In contrast, the Justice Department contended that the statute's plain text and historical background indicate Congress's intent to broadly cover improper computer access, including circumstances in which an authorized individual accessed a computer with an improper purpose, as Van Buren indisputably had.

In reversing Van Buren's conviction, the Court conclusively rejected the government's position, holding that the "exceeds authorized access" prohibition only "covers those who obtain information from particular areas in the computer – such as files, folders or databases – to which their computer access does not extend. It does not cover those who, like Van Buren, have improper motives

for obtaining information that is otherwise available to them." The Court rejected the government's argument that the "exceeds authorized access" clause "incorporate[s] purpose-based limits contained in contracts and workplace policies." The Court characterized its ruling as a "gates-up-or-down" approach: "[O]ne either can or cannot access a computer system, and one either can or cannot access certain areas within the system." If a person "can" access the system or certain areas within it, that person does not violate Section 1030(a)(2) by doing so for an improper purpose.

The Court underscored that adopting the government's interpretation of the statute "would attach criminal penalties to a breathtaking amount of commonplace computer activity." It would, for example, criminalize the conduct of an employee who uses a work computer to send a personal email and "everything from embellishing an online-dating profile to using a pseudonym on Facebook." The Court rejected such a sweeping interpretation.

Impact on civil cases brought under the CFAA

The same provisions of the CFAA that provide for criminal liability allow, in certain circumstances, civil remedies for "[a]ny **person** who suffers **damage** or **loss** by reason of a violation of this section," 18 U.S.C. § 1030(g). The Court's reasoning in *Van Buren* concerning the meaning of "exceeds authorized access" also indicates its inclination to limit civil remedies under the CFAA to "hacking" cases in which the plaintiff suffers "technological harms" to computer systems or data.

Specifically, in rejecting the government's position that the CFAA "incorporate[s] purpose-based limits contained in contracts and workplace policies," the Court identified a "structural problem" related to the statute's civil remedies. Justice Barrett explained that the defined terms "damage" and "loss," which are a prerequisite to a CFAA civil action, "focus on technological harms – such as the corruption of files – of the type unauthorized users cause to computer systems and data." Limiting the terms to technological harms "makes sense in a scheme 'aimed at preventing the typical consequences of hacking.'" "Damage" and "loss" as defined by the CFAA, however, are "ill fitted … to remediating 'misuse' of sensitive information that employees may permissibly access using their computers."

Impact on *LinkedIn v. hiQ*

Since September 2020, the Supreme Court has been holding the fully briefed petition for certiorari in another significant CFAA case, *LinkedIn Corp. v. hiQ Labs, Inc.*, presumably pending the resolution of *Van Buren*. *LinkedIn* presents additional interpretative issues about the CFAA's "without authorization" bar, which the Court may choose to address directly or to remand back to the lower courts to reassess in light of the *Van Buren* decision.

Analytics firm hiQ provides business intelligence based on publicly available user data it scrapes from LinkedIn. After receiving LinkedIn's cease-and-desist letter that alleged it was violating the CFAA, hiQ sued for a preliminary injunction and a declaration that its conduct did not violate the CFAA. The district court granted the preliminary injunction forbidding LinkedIn from denying hiQ access to publicly available LinkedIn member profiles. **The US Court of Appeals for the Ninth Circuit affirmed**, holding that "when a computer network generally permits public access to its data," automated data collection is not "without authorization." In other words, it held that the CFAA does not prohibit scraping of material that is publicly available on the internet.

LinkedIn's certiorari petition urges the Supreme Court to grant review to address whether companies deploying automated bots to scrape personal data from public websites – even after the website owner has expressly denied permission to access the data – violates the CFAA. Although *Van Buren* focused on the "exceeds authorized access" CFAA prong, whereas *LinkedIn* is focused on "without authorization," the Court's reasoning in *Van Buren* arguably is pertinent to several aspects of the dispute in *LinkedIn*. We will update this alert when the Supreme Court takes further action in *LinkedIn*.

Implications for cybersecurity researchers

The *Van Buren* decision appears particularly favorable to cybersecurity researchers, whose work often involves accessing computer systems in ways that violate terms of service or other policies. For instance, a researcher might send automated requests to a website or computer network for the purpose of detecting security vulnerabilities. Many websites publish terms of service that forbid all types of automated requests, even if those requests are limited to public URLs and cause no damage on their own. Many white-hat researchers have thus been deterred by the threat of criminal prosecution under the CFAA for exceeding authorized access.

Van Buren mitigates this threat by rejecting the view that the CFAA allows criminal penalties for violating "circumstance-based access restrictions," such as terms-of-service prohibitions on automated access to public systems. Rather, the criminal prohibitions are limited to someone who "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." In footnote 8, the Court expressly did not resolve the issue of whether an enforceable access restriction must be a technological restriction or it could also be contained in a policy or contract. Nonetheless, *Van Buren* is clear that the prohibition on "exceeding authorized access" is limited to areas of a computer that are off limits.

Key Contacts

Tiana Demas	tdemas@cooley.com +1 212 479 6560
Kathleen R. Hartnett San Francisco	khartnett@cooley.com +1 415 693 2071
John H. Hemann San Francisco	jhemann@cooley.com +1 415 693 2038
Travis LeBlanc Washington, DC	tleblanc@cooley.com +1 202 728 7018