SAUL EWING ARNSTEIN & LEHR LLP

ALERT

White Collar & Government Enforcement Practice
Cybersecurity and Privacy Practice

JUNE 2021

Supreme Court narrows the scope of the Computer Fraud and Abuse Act in *Van Buren v. United States*

Patrick M. Hromisin | Kelsey Marron

On June 3, 2021, the Supreme Court drastically narrowed the reach of the Computer Fraud and Abuse Act of 1986 ("CFAA"), a federal statue prohibiting individuals from "exceeding authorized access" to computers and computer systems. In *Van Buren v. United States*, the Court grappled with the meaning of "exceeding authorized access"– does this phrase cover those who misuse computer access that they otherwise lawfully have, or only those who obtain information on a computer to which they do not have lawful access? In a 6-3 majority opinion authored by Justice Amy Coney Barrett, the Court held that the provision only covers the latter group: "those who obtain information from particular areas in the computer—such as files, folders, or databases—to which their computer access does not extend." In recent years, federal prosecutors regularly claimed that individuals with otherwise lawful access to a computer who exceeded the stated purpose of their access could be criminally liable under the CFAA, but the Court's decision undermines that argument.

In *Van Buren*, police officer Nathan Van Buren accessed computerized license plate records on a police database, in exchange for a bribe, to determine whether an individual was an undercover officer. Van Buren's conduct violated a department policy which only permitted him to access the records for a legitimate law enforcement purpose. Van Buren was convicted of exceeding his authorized access under the CFAA, and his conviction was upheld by the Eleventh Circuit Court of Appeals.

The Supreme Court took up the matter to resolve the nationwide circuit split over the meaning of "exceeding authorized access" and clarify the scope of potential criminal liability under the CFAA. In the statute, "exceeds authorized access" means "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*."[1] The Court's analysis focused on the impact of the word "so" in the definition, and interpreted the word according to its plain meaning. Using this interpretation, the Court agreed with Van Buren's view of the law and held that "the phrase 'is not entitled so to obtain' is best read to refer to information that a person is not entitled to obtain by using a computer that he is authorized to access." As such, while Van Buren's conduct may have violated a department policy, the conduct did not amount to a violation of the CFAA because he was authorized to access the computer system at issue. The fact that he did so for an allegedly improper purpose did not criminalize his actions under the Court's reasoning.

As part of its analysis, the Court expressed concern that the government's interpretation of the statute criminalized a wide breadth of otherwise innocuous online activity. In the government's view, any violation of a given website's terms of use could amount to a criminal act under the CFAA. Website terms of use are not always displayed conspicuously, and can be established or altered entirely at the discretion of the website operator. Under the government's broad interpretation, for example, if a social media site's terms of use prohibited posting incorrect information in a profile, a user could have criminally violated the CFAA by exaggerating their wealth, age, or education. Further, website operators could impose capricious restrictions via their terms of use (e.g., "no access of the website by left-handed people"), and users who violated those terms would have also violated the CFAA. The Electronic Frontier Foundation ("EFF"), a non-profit advocate for electronic privacy, submitted an amicus brief in which it stated flatly that "users routinely violate computer use policies in the course of their employment or as a part of their daily lives." The potential consequences for such violations would be employment actions or being restricted from the use of a site, but the government's broad reading of the CFAA would add criminal penalties to these widely-committed violations. Based on these concerns and its statutory analysis, the Court overturned Van Buren's conviction.

The Court also reasoned that its interpretation of the definition was the most consistent with another provision of the CFAA, which prohibits access to a computer without authorization.[2] Under this analysis, both provisions are to be read as "gates-up-or-down inquir[ies]—one either can or cannot access a computer system, and one either can or cannot access certain areas within the system." For example, if an employer grants an employee access to a database containing confidential product schematics and the employee copies those schematics and sells them to a competitor, that would not amount to a CFAA violation (though, of course, the employee and competitor would be subject to a range of other legal consequences). If, on the other hand, the employee gained access to a database the employer hadn't allowed him or her to use and copied the schematics to sell them to a competitor, that would be a CFAA violation.

One key question the Court did not address was whether the CFAA's access restrictions mean only "technological (or 'code-based') limitations on access, or instead also look to limits contained in contracts or policies." In a footnote, the Court stated that the present case did not require it to decide this issue, but the question is likely to arise in further CFAA cases. In the example above, does the employee violate the CFAA only if he/she circumvents technological security measures by, for example, spoofing another user's credentials? Or does the employee violate the CFAA if the files are accessible on a shared drive, but there is a provision in the employee handbook specifying that users are not to access files unless specifically required to do so for business purposes? The *Van Buren* Court did not decide this question, but future courts likely will be called upon to do so.

Privacy commentators had mixed reactions to the *Van Buren* ruling. The EFF heralded the decision as a victory, noting that a contrary ruling would have criminalized the acts of security researchers who test websites for vulnerabilities and report such vulnerabilities to the site operators. While these reports might be highly useful and actually prevent hacking, the actions of the researchers frequently amount to violations of the website's terms of use. The International Association of Privacy Professionals ("IAPP") noted that the CFAA was drafted in the 1980's, when computer use was a fraction as prevalent as it is now, and that the CFAA was mainly aimed at preventing hacking by external miscreants, and not misdeeds by company insiders. In the view of the IAPP, the government's attempt to use the CFAA to penalize acts like Van Buren's emphasized the need for a federal data privacy law that would directly address the misuse of individuals' personal information, whether such misuse was the result of hacking or previously authorized access.

Saul Ewing Arnstein & Lehr LLP's Cybersecurity & Privacy and White Collar & Government Enforcement practices are closely monitoring developments in this area, and are available to assist with any questions related to the Computer Fraud and Abuse Act or other cybersecurity issues.

---

1. 18 U.S.C. §1030(e)(6).
2. 18 U.S.C. §1030(a)(2).

This alert was written by Patrick Hromisin and Kelsey Marron, members of the Firm's Cybersecurity and Privacy Practice. Patrick can be reached at (215) 972-8396 or Patrick.Hromisin@saul.com. Kelsey can be reached at (617) 912-0909 or Kelsey.Marron@saul.com. This alert was prepared for information purposes only.

Did you find this information useful? Please provide your feedback here and also let us know if there are other legal topics of interest to you.