June 16, 2021

Supreme Court Narrows Reach of Computer Crime Statute

Authored by Kevin P. Daly, Linn F. Freedman, Seth B. Orkand, and Kathryn M. Rattigan

On June 3, 2021, the U.S. Supreme Court issued its first-ever interpretation of the Computer Fraud and Abuse Act (CFAA), the federal criminal and civil statute intended to deter and punish unauthorized access to computer systems. The decision in *Van Buren v. United States* adopts a narrow construction of a key provision of the CFAA addressing whether a computer user "exceeds authorized access." In doing so, the Court echoed the concerns of many commentators who have warned against a broad reading of the statute that might over-criminalize computer activity. The Court's decision removed the CFAA as a tool to address certain circumstances in which someone accesses a computer in violation of an authorized purpose, such as violations of workplace technology policies or a website's terms of service.

Purpose and Scope of the Computer Fraud and Abuse Act

The CFAA was enacted in 1986 to combat computer crimes that may not be actionable under other criminal statutes. Among other prohibitions, the statute makes it a criminal offense to "intentionally access[] a computer without authorization or exceed[] authorized access." 18 U.S.C. § 1030(a)(2). The term "exceeds authorized access" is defined as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6). The CFAA also contains a private right of action permitting civil actions against those who violate the CFAA's prohibitions. 18 U.S.C. § 1030(g).

As computers, and computer crimes, became ever more pervasive, a debate emerged over the breadth of the term "exceeds authorized access." In its broadest interpretation, it could be read to encompass not only breaking into a computer system, but also violating terms of service or other limitations that operators of computer systems place on their users. Under this broad interpretation, violations of a website's terms of service or an employer's computer-use policies could violate the CFAA. Because it potentially criminalized conduct that is commonplace, many commentators have criticized the CFAA as being overbroad. The circuits split sharply over how broadly to read this provision of the CFAA.

Facts of Van Buren's Prosecution

The Court resolved a key aspect of this circuit split in *Van Buren*. The case arose from Van Buren's conduct as a police sergeant in Georgia. Van Buren's employer maintained a policy prohibiting use of law enforcement databases for personal purposes. In a sting operation, an FBI informant paid Van Buren to search a law enforcement database for license plate information for personal reasons, in violation of the police department's policies. The government charged Van Buren with violating the CFAA because departmental policy prohibited such searches for personal use. Van Buren was convicted and sentenced to 18 months in prison, and the U.S. Court of Appeals for the Eleventh Circuit affirmed the conviction.

The Court's Rationale for Narrowing the CFAA

The Supreme Court reversed Van Buren's conviction in a 6-3 decision authored by Justice Amy Coney Barrett. Van Buren argued that the CFAA does not prohibit accessing systems the user is otherwise permitted to access, even if the user does so for an improper purpose. He claimed that this interpretation

would be consistent with the CFAA's anti-hacking purpose and ensure that authorized users would not be criminally liable for violating workplace computer-use policies or website terms of service. The Court agreed, rejecting the government's argument that violation of a purpose-based restriction can be the basis for a violation of this portion of the CFAA. The Court characterized its ruling as a "gates-up-or-down inquiry." In other words, "one either can or cannot access certain areas" of a computer system. Under the Court's interpretation announced in *Van Buren*, the CFAA prohibits accessing an area of the computer system that is off limits entirely to the user. But it does not prohibit accessing an area of a system that is accessible to the user for certain purposes, even when the user accesses the area for a different, improper purpose.

Implications for Companies

The *Van Buren* decision represents a significant narrowing of the reach of the CFAA in that it no longer reaches persons who misuse their access to an area of a computer system for an improper purpose. For example, an IT vendor who is authorized to access parts of a client's system for the purpose of maintaining or performing technical work could abuse that access to misappropriate trade secrets or other technical information located on that system. Or a hospital employee who is permitted to access a medical records system to view records of patients they treat may impermissibly view the records of an acquaintance or a celebrity patient whom they do not treat. *Van Buren* now clarifies that this type of misconduct is not a violation of the CFAA; whether it violates other state or federal laws is a separate inquiry. Some of this conduct, if used to defraud another out of money or property, could be prosecuted under the federal wire fraud statute. But the *Van Buren* decision clarifies that this type of misconduct is not actionable under the CFAA. As a result, companies may wish to assess technological access controls (such as passwords or other technological blocks to access) to control sensitive data rather than relying on internal policies.

Impact on Civil CFAA Cases

The provisions of the CFAA that provide for criminal liability also provide a private cause of action for "any person who suffers damage or loss by reason of a violation of this section." 18 U.S.C. § 030(g). Although the *Van Buren* decision considered the criminal implications of the statute, the Court appears inclined to limit the civil remedies under the CFAA to cases in which a plaintiff suffers "technological harm" to computer systems or data as the result of unauthorized access.

An Open Question: Can Contractual Use Limitations be Enforced under the CFAA?

In a footnote, the Court reserved decision on the scope of the CFAA: Must the "gate" prohibiting access to an area of a computer system be technological in nature, such as a code-based restriction that a user would have to "hack" to circumvent? Or can the "gate" also be a restriction in a contract, terms of service, or other policy? In footnote 8, the Court expressly did not resolve this question. However, portions of the opinion suggest that the Court is likely to adopt a narrower interpretation on this issue as well. The Court expressed concern that a broad interpretation of the CFAA could "criminalize[] every violation of a computer use policy." The Court appears unwilling to embrace an interpretation that would criminalize, for example, checking sports scores or personal email on a work computer or embellishing a profile or using a pseudonym on a social media site. The Court cites each of these examples and suggests that it is unwilling to adopt an interpretation of the CFAA that reaches these types of conduct. Permitting the CFAA to reach violations of contractual limits on access likely would lead to exactly these outcomes that the Court seems to want to avoid. But because of the reservation language in footnote 8, these hypotheticals could be litigated in the lower courts in the coming years.

Other Effects on Access to and Use of Computer Systems

Van Buren's limits on the scope of the CFAA also may be favorable to cybersecurity researchers, who often access computer systems in violation of terms-of-use to detect security vulnerabilities or other threats. Most websites include prohibitions on the use of automated requests (even if such requests are limited to public URLs and cause no damage), such as those used for detecting these vulnerabilities. Until *Van Buren*, white-hat cybersecurity researchers were deterred from carrying out such tests due to the threat of criminal prosecution under the CFAA for exceeding authorized access. The *Van Buren* decision removes this threat for white-hat researchers by rejecting the interpretation that the CFAA allows for criminal penalties for violating "circumstance-based restrictions" (e.g., terms-of-use prohibitions on automated access to public systems). As noted above, instead the CFAA is limited to those who "access[] 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." This widens the playing field for white-hat researchers.

Additionally, the Court's interpretation in *Van Buren* of the CFAA might impact individuals and businesses that engage in data scraping. Data scraping is a technique in which a computer program extracts data from output generated from another program. Data scraping is commonly manifest in web scraping, the process of using an application to extract valuable information from a website. As with automated requests, many terms of service prohibit both their own customers/users and third parties from using and accessing data on their websites for these purposes.

Previously some courts had determined that data scraping was a violation of the CFAA, especially if the data were protected by some form of access permissions (e.g., username and password). With that interpretation, some companies could assert claims under the CFAA saying that data scraping 'exceeded authorized access' to the website. While *Van Buren* does not explicitly permit data scraping, its narrow reading of the CFAA may limit the legal remedies available to address it.

FOR MORE INFORMATION

Contact any member of Robinson+Cole's Data Privacy + Cybersecurity team listed below:

Linn F. Freedman | Kathleen E. Dion | Conor O. Duffy | Deborah A. George

Jessica A.R. Hamilton | Edward J. Heath | Benjamin C. Jensen | Virginia E. McGarrity

Kathleen M. Porter | Kathryn M. Rattigan | Norman H. Roos | Daniel F. Sullivan | Jean E. Tomasco

For insights on legal issues affecting various industries,
please visit our Thought Leadership page and subscribe to any of our newsletters or blogs

Boston | Hartford | New York | Providence | Miami | Stamford | Los Angeles | Wilmington | Philadelphia | Albany | rc.com