WALDEN MACHT & HARAN LLP

Supreme Court to Clarify Scope of the Computer Fraud and Abuse Act (CFAA)

by Sean Haran and Derek Borchardt

The Computer Fraud and Abuse Act (CFAA) makes it a federal crime to access a computer "without authorization" or in a manner "exceeding authorized access." 18 U.S.C. § 1030. Federal courts have had dramatically differing interpretations of the meaning and scope of the "exceeding authorized access" component of the CFAA. This will soon change, however, as the Supreme Court announced on Monday, April 20, 2020, that it will hear a case that asks the Court to clarify the scope of the statute.

The primary controversy over the CFAA's scope, which has divided the federal circuit courts, is whether rules imposed by computer system owners and administrators—such as, for example, a website's terms of service, or an employer's internal policies for how employees may use their workplace computers—define the forms of "authorized access" that the CFAA prohibits "exceeding." Some courts have held that, because these sorts of rules define the permissible ways that computer systems may be used, authorized computer users "exceed[] [their] authorized access" under the CFAA if they violate those rules. Other courts have interpreted the statute more narrowly, holding that something more than a rule violation—such as hacking or password theft or other malicious conduct to access a part of the computer system that is otherwise off limits—is required for authorized computer users to "exceed[] [their] authorized access."

For an example of the broader view adopted by some courts, the Fifth Circuit's decision in United States v. John, 597 F.3d 263 (5th Cir. 2010) is illustrative. The defendant in that case was a bank employee who was afforded access to the bank's computer systems in order to carry out her job duties. The bank did not, however, allow her to use her workplace computer to steal customer information for purposes of incurring fraudulent charges—which is what she did. In addition to bank fraud and any number of other crimes, did the defendant also violate the CFAA by using her workplace computer in a manner prohibited by her employer? The Fifth Circuit's answer: Yes. Conviction affirmed.

Other courts see the statute differently. For example, the Ninth Circuit's decision in United States v. Nosal, 676 F.3d 854 (9th Cir. 2012) (en banc) concerned employees of an executive search firm who downloaded confidential client information from their workplace computers, with plans to leave the firm, start a competing business, and use the misappropriated information to their competitive advantage. By stealing the firm's confidential information for their own competitive benefit, the employees violated the firm's policies. CFAA violation? The Ninth Circuit's answer: No. Under the Ninth Circuit's view of the statute, the prohibition against "exceeding authorized access" does not apply to a person "who has unrestricted physical access to a computer, but is limited in the use to which he can put the information." Id. at 857, 862-63. The Ninth Circuit explained, moreover, that reading the CFAA to cover "use restrictions" and thereby to reach activities "routinely prohibited by many computer-use policies" would improperly turn "millions of ordinary citizens" into criminals. Id. at 860-63.

The Supreme Court will now decide which side of this circuit split prevails. The Court granted certiorari to review the Eleventh Circuit's decision in United States v. Van Buren, 940 F.3d 1192 (11th Cir. 2019). The defendant in that criminal case, a Georgia police officer, was authorized to use a state computer database for legitimate "law-enforcement purposes." But he went beyond that, to say the least. The defendant took money from an unsavory associate with a checkered past who (while tape recording everything for the FBI) asked the defendant to determine whether a particular woman the associate had met at a strip club was an undercover police officer. The defendant took the money, searched the woman's information in the police department database—thereby violating department policy concerning the use of the database—and reported back the results. Serious misconduct, unquestionably, but also a CFAA violation? The Eleventh Circuit thought so, but the Supreme Court will have the ultimate say in the coming months.

The Supreme Court's decision will have ramifications far beyond one police officer's misuse of a state database. Every day, millions of U.S. citizens with internet connections access innumerable computer systems subject to use restrictions. Whether these employer policies, terms of service, and other rules imposed by computer system owners and administrators have the force of law, enforceable by criminal sanction, is a question of significant consequence. Stay tuned.

Walden Macht & Haran LLP (WMH) has deep experience in representing clients in criminal or civil litigation. We conduct thorough assessments of the legal and evidentiary strengths and weaknesses and potential risks at each stage of an engagement and execute sophisticated strategies to maximize the opportunities for the best possible outcome.

About Walden Macht & Haran LLP

WMH is a New York-based boutique law firm with deep experience in resolving complex compliance challenges. Our partners have held numerous senior positions in the public and the private sphere and have the breadth and depth of experience to advise in connection with the most pressing matters and to handle the most sensitive engagements. The partnership includes seven former federal prosecutors, many of whom held senior supervisory positions in the Department of Justice, a former counsel for national security at the Federal Bureau of Investigation, a former general counsel of a NYSE listed multinational, a former chief compliance officer of a publicly traded company, and multiple former state prosecutors. We are known for our experience, integrity, and outstanding track record in both state and federal court and in connection with banking monitorships.