wiley

NEWSLETTER

Supreme Court Limits Application of Computer Fraud and Abuse Act, Impacting Use of Online Information

June 2021

Privacy In Focus®

In *Van Buren v. United States*, No. 19-783, 593 U.S. _ (2021), the U.S. Supreme Court weighed in on the scope of the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. 1030, bringing much needed clarity to how people and businesses conduct life online. Specifically, the Supreme Court addressed conflicting interpretations of the CFAA's "exceed[ing] authorized access" provision and found that the provision does not prohibit the misuse of information on a computer so long as an individual is authorized to access the information in question. This decision should bring comfort that a wide variety of innocuous online activity does not give rise to federal criminal and civil liability. But, organizations are now more limited in their ability to protect confidential information from misuse.

The CFAA prohibits "access without authorization" to computers – which is generally understood as traditional computer hacking, such as a criminal deploying malware and bypassing security to steal terabytes of someone else's data. *See* 18 U.S.C. 1030(a)(2). As the Supreme Court affirmed, the "without authorization" clause of the CFAA "protects computers themselves by targeting so-called outside hackers." This portion of the CFAA has not been controversial.

CFAA Prohibitions and Ambiguities

The CFAA also prohibits anyone who "exceeds authorized access" to a computer. *See* 18 U.S.C. 1030(a)(2). In contrast to traditional computer hacking, the "exceeds authorized access" clause protects

Authors

David E. Weslow
Partner
202.719.7525
dweslow@wiley.law

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Practice Areas

Cyber and Privacy Investigations, Incidents & Enforcement

Cybersquatting & Internet IP

Privacy, Cyber & Data Governance

computers from "so-called inside hackers" – those who have permission to access a computer, but then engage in nefarious activity.

Courts and scholars have long struggled with how to handle "inside hackers" and the scope of the "exceed [ing] authorized access" provision. *See, e.g.*, *hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985 (9th Cir. 2019) (stating that the CFAA prevents conduct "analogous to breaking and entering"); *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 583–84 (1st Cir. 2001) (holding that violations of a confidentiality agreement or other contractual restraints could give rise to a claim for unauthorized access under the CFAA).

In particular, is it a violation of the CFAA when the user already has access to information, and the only "hacking" involved is misuse of the information? For example, does a person violate the CFAA when they access a database with authorization as part of their job, but misuse the information in the database in violation of company policy? What about similar cases, like violating the Terms of Service on a social media site, or a security researcher using a service in ways not intended by the provider, or a business partner misusing corporate databases? What about scraping data from a publicly available website that includes terms of use prohibiting scraping?

Van Buren resolves these questions.

Van Buren **Background**

In *Van Buren*, a Georgia police officer was approached by an acquaintance to search the state law enforcement computer database for a license plate purportedly belonging to a woman whom he had met at a local strip club. The acquaintance claimed he wanted to ensure that the woman was not in fact an undercover officer, and he offered to pay Officer Van Buren $5,000 in exchange for the search. Critically, Officer Van Buren had access to the license plate database as part of his job, but department policy did not allow him to use it for personal reasons. As the government acknowledged, Officer Van Buren was clearly "authorized" to use the license plate database for legitimate law enforcement purposes – he wasn't a traditional "outside" hacker. However, the government argued he illegally exceeded authorization because he had been trained "on the proper and improper uses of the system" and admitted to investigators that he knew his actions were "wrong."

Treating Officer Van Buren as an "inside hacker" based on his misuse of the license plate database, the government charged Officer Van Buren with violating Section 1030(a)(2) of the CFAA. Van Buren was convicted at trial, and his conviction was upheld by the U.S. Court of Appeals for the Eleventh Circuit. The Supreme Court reversed Van Buren's conviction and held that "exceed[ing] authorized access" does not include misuse of information lawfully accessed. Rather, it prohibits access to parts of a computer that an individual is not authorized to access.

Supreme Court Analysis and Implications

As the Court explained:

If a person has access to information stored in a computer – e.g., in "Folder Y," from which the person could permissibly pull information – then he does not violate the CFAA by obtaining such information, regardless of whether he pulled the information for a prohibited purpose. But if the information is instead located in prohibited "Folder X," to which the person lacks access, he violates the CFAA by obtaining such information.

The Court's decision provides significant clarity, but questions remain. For example, the Court did not rule on computer crime scholar Orin Kerr's question of what an organization must do under the CFAA to indicate that a person does not have authorization to access "Folder X" or some other part of a computer. *See Van Buren* at fn 8. Can an organization rely on a policy to state that a part of a computer is off-limits, and thereby create CFAA liability? Or are technological measures, like encryption or identity access management controls, also required?

Van Buren will have repercussions well beyond criminal prosecutions. Using a computer today generally means using someone else's computer, whether an employer, a social media site, a cloud service provider, or a business partner. Entities that allow the public to use their computers face challenging questions about how much they can open their networks and still protect their intellectual property and confidential information. Relationships with these third parties are often dictated by Terms of Service, Employee Handbooks, and other contractual arrangements that set out the intended rules of the road. The Supreme Court has now held that misuse of information in violation of these rules of the road will not be a criminal or civil violation of the CFAA.

As the Court noted, a contrary reading "would attach criminal penalties to a breathtaking amount of commonplace computer activity," including using a work computer to read the news in violation of an employer's policy, violating the terms of service of a website by, for instance, "embellishing an online-dating profile [or] using a pseudonym on Facebook." Instead, the Court's reading should bring solace to people and businesses whose otherwise innocuous activities online happened to be in technical violation of website policy.

However, the organizations that relied on the CFAA to protect sensitive information have lost a potential legal action and may need to rethink business arrangements and terms of service that relied in part on the CFAA to help enforce the rules of the road. In some cases, misuse of information may still give rise to criminal and civil liability, perhaps under the Defend Trade Secrets Act or the wire fraud statute. *See* 18 U.S.C. 1836 (protecting trade secrets); 18 U.S.C. 1343 (wire fraud statute). But in many cases, organizations may be left with only contractual remedies. In light of *Van Buren,* businesses, social media companies, website operators, and employers may need to reevaluate and strengthen their contractual remedies to address situations where the CFAA no longer applies.