Published on *The National Law Review* https://natlawreview.com

Important Developments (Including Supreme Court Review) in the Interpretation of the Computer Fraud and Abuse Act

Article By:

Jeffrey D. Neuburger

We continue to wait to see if the Supreme Court will accept LinkedIn's petition to overturn the Ninth Circuit's blockbuster ruling in the *hiQ Labs* case. In that case, the appeals court held that an entity engaging in scraping of "public" data had shown a likelihood of success on its claim that such access does not constitute access "without authorization" under the federal Computer Fraud and Abuse Act (CFAA).

In the meantime, earlier this week the Supreme Court agreed to hear the appeal of an Eleventh Circuit decision that affirmed the conviction of a police officer under the CFAA for "exceeding authorized access" for accessing police databases for personal gain. (See *U.S. v. Van Buren*, 940 F. 3d 1192 (11th Cir. 2019), *pet. for cert. granted* *Van Buren v. U.S.*, No. 19-783 (Apr. 20, 2020)). This would be the Supreme Court's first CFAA case.

And in addition to the news at the Supreme Court, late last month, a D.C. district court issued a ruling interpreting the extent of criminal liability under the CFAA for accessing websites in contravention of terms of use for academic research. In that case, the D.C. court held that the mere violation of website terms of use cannot form the basis of criminal liability for "unauthorized access" or "exceeding authorized access" under the CFAA. (*Sandvig v. Barr*, No. 16. 1368 (D.D.C. Mar. 27, 2020)).

CFAA Background

Under the CFAA, it is a crime to obtain "information from any protected computer" by "intentionally access[ing] a computer without authorization or exceed[ing] authorized access." 18 U.S.C. §1030(a)(2)(C). "Exceeding 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 accesser is not entitled [so] to obtain or alter." 18 U.S.C. §1030(e)(6). While primarily a criminal statute, the CFAA permits a private party "who suffers damage or loss by reason of a violation of [the statute]" to bring a civil action.

The law surrounding "unauthorized access" is unsettled when it comes to interpreting the CFAA "unauthorized access" provision in certain civil and criminal cases. While "authorization" under the CFAA could refer to the purposes for which one is authorized to access a computer, it could

alternatively refer to the particular files in the computer to which one's authorization extends. The circuits are split about whether an individual "exceeds authorized access" to a protected computer, in violation of the CFAA, when he or she accesses a system with permission but then uses the system for a prohibited purpose. In the web scraping context, the CFAA is regularly pleaded by website operators against third parties who purportedly access sites "without authorization" by scraping data in contravention of terms or technical measures or after the website operator expressly revokes an entity's authorization to access the website.

While all these matters involve the interpretation of the same statute, the facts and circumstances are of course slightly different, yet the Supreme Court's interpretation of the CFAA, even in a criminal matter, will likely be highly instructive to civil CFAA disputes.

Van Buren Case: Does Authorized Access to a Database with an Improper Purpose Equal a CFAA Criminal Violation?

In *Van Buren*, the defendant, a police officer, was convicted for violating the CFAA for receiving payment from an third party for running a license plate through a police database. Van Buren was authorized to access the database for lawful police work, but the jury convicted him under the CFAA for "exceeding authorized access" for using the database for a non-law enforcement purpose. The defendant appealed his conviction, arguing that he accessed only databases that he was authorized to use, even though he did so for an inappropriate reason. The Eleventh Circuit affirmed the conviction, following its own precedent which had previously rejected the argument that misusing databases a defendant lawfully can access does not constitute computer fraud. (*U.S. v. Van Buren*, 940 F. 3d 1192 (11th Cir. 2019)).

In the criminal context, circuit courts are split on how to parse the "unauthorized access" or "exceeding unauthorized access" provisions. For example, the Second, Fourth and Ninth Circuits have taken a narrow approach and ruled that access to databases that a defendant is permitted to access cannot constitute computer fraud under the CFAA, recognizing the slippery slope when prosecutors can bring charges based on violations of a workplace's usage policies or website's terms. However, the First, Fifth, Seventh and Eleventh Circuits have interpreted the CFAA to allow criminal prosecutions against an employee, like Van Buren, who accesses a protected computer with a purpose contrary to the employer's policy or interests.

According to the appellant's petition, the Eleventh Circuit's expansive view of the scope of the CFAA's access provision is out-of-line with Congressional intent and would "reach commonplace activities of nearly all computer users, going far beyond the objectives of the statute," and attach criminal liability to private computer use policies that "no one reads or understands." The government, on the other hand, contends that courts already apply the CFAA to specific criminal circumstances in the narrow manner urged by the defendant Van Buren and that under DOJ policy, CFAA prosecutions are not undertaken for trivial infractions of computer use policies, but for more serious matters.

We will have to wait until next year to see whether the Supreme Court agrees with the defendant Van Buren's argument that a person exceeds authorized access only when "he had no right at all to access the information" he obtained, or enunciates a different interpretation.

Sandvig Case: Agreeing to Website Terms Not Sufficient to Trigger Criminal Liability under the CFAA

In *Sandvig v. Barr*, No. 16. 1368 (D.D.C. Mar. 27, 2020), a group of professors brought a constitutional challenge alleging that the potential threat of criminal prosecution under the CFAA for accessing a website "without authorization" for academic research (based upon the researchers' data scraping done in violation of the site's terms of use) violates their First Amendment rights. In a preliminary decision from 2018, a D.C. district court held that the plaintiffs had standing and allowed their as-applied constitutional challenge to the CFAA to go forward with regard to the activity of creating fictitious accounts on web services for research purposes.

In March 2020, the D.C. district court bypassed the constitutional questions and held that the CFAA does not criminalize mere terms-of-service violations on consumer websites. Thus, the plaintiffs' proposed research plans involving the creation of false accounts to conduct research into algorithmic bias of certain websites is not criminal under the CFAA (though, the court cautioned that the plaintiffs' assent to website terms may have consequences for civil liability under other federal or state laws). Interestingly, the court followed the reasoning of the recent Ninth Circuit ruling in *hiQ* which interpreted the CFAA in the context of the scraping of publicly available website content. It agreed that the term "without authorization" in the statute "suggests a baseline in which access is not generally available and so permission is ordinarily required," such that, for the purposes of the CFAA, the internet is divided into two realms: "public websites (or portions of websites) where no authorization is required and private websites (or portions of websites) where permission must be granted for access." Under this rubric, the court asked what sort of permission or password scheme that governs website access constitutes enough of a barrier to trigger criminal liability under the CFAA if bypassed.

In concluding that a breach of website terms is not sufficient to trigger criminal liability under the CFAA, the court stated that terms of service do not constitute "permission requirements" that, if violated, trigger criminal liability. Under the government's position, an announcement on a website homepage that access to any further content is conditioned on agreeing to the website terms of service would be enough of a barrier to access. In rejecting the government's position and taking a narrower view of the scope of the CFAA criminal access provisions, the court opined that websites' terms of service provide "inadequate notice for purposes of criminal liability" and that "criminalizing terms-of-service violations risk turning each website into its own criminal jurisdiction and each webmaster into his own legislature." The court used similar reasoning to rule that the plaintiffs would not be considered to have "exceeded authorized access" in creating fake accounts for academic study.

What does the *Sandvig* ruling mean for civil liability under the CFAA for web scraping?

The decision would appear to be in line with the Ninth Circuit *hiQ* opinion, which took a narrow view of CFAA liability for publicly available website data and the Ninth Circuit's *Power Ventures* precedent, where the appeals court held, in the context of unwanted data scraping, that a violation of the terms of use of a website, without more, cannot be the basis for civil liability under the CFAA. However, the *Sandvig* court was careful to note that the case before it was different from the *hiQ* case, where the website operator expressly revoked access by sending the data scraper a cease and desist letter. The court stated that it was not deciding whether such express revocation of access would make further visits a criminal CFAA violation. Still, the court envisioned a line where CFAA liability would stand. It stated that a user should be deemed to have accessed a computer "without authorization" when the user "bypasses an authenticating permission requirement, or an 'authentication gate,' such as a password restriction that requires a user to demonstrate 'that the user is the person who

has access rights to the information accessed.'" In scraping disputes, often the initial precursor for unauthorized access is a violation of the website terms of service, so at the very least, the *Sandvig* ruling adds another example where a court has followed the narrow interpretation of the Ninth Circuit on that proposition.

Final Thoughts

When first enacted, the CFAA was originally directed at classic, pre-modern "hacking" activities, in which an individual's access permission was much more readily determined. But, as we've seen in the ensuing years as the statute has been amended and technology has gotten more advanced, the language of the CFAA is susceptible to broader application, as evidenced by the *Van Buren* case, and has been brought to bear in many contexts beyond traditional outside hacking scenarios. With the Supreme Court accepting its first CFAA case, it has the chance to clarify certain points of law surrounding the CFAA on a national level, including with regard to claims in civil CFAA cases. However, depending on the scope of the opinion, it may not resolve questions of civil liability in all "unauthorized access" scenarios that may arise in an unwanted data scraping dispute.

National Law Review, Volume X, Number 113