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

U.S. Supreme Court Case Preview—Van Buren v. United States: Does Use of a Computer for an "Improper Purpose" Violate the Computer Fraud and Abuse Act?

Article By:

Kevin M. Cloutier

David M. Poell

For the first time, the Supreme Court has agreed to review the Computer Fraud and Abuse Act (CFAA). The Court's initial review of the CFAA comes in the wake of a federal circuit split as to whether the statute can only be deployed against hackers and unauthorized users of electronic systems, or also against authorized users who use the information for unauthorized purposes. The Court's decision may significantly affect not only how law enforcement uses the CFAA, but also whether civil litigants, such as employers, may use the CFAA to defend against unauthorized employee activities.

Enacted in 1986 to combat the perceived growing threat of hackers, the CFAA makes it a federal crime to "access[] a computer without authorization or exceed[] authorized access, and thereby obtain[] information from any protected computer." 18 U.S.C. § 1030(a)(2)(C). In addition to criminal penalties, the CFAA contains a private right of action allowing any person who sustains damages or loss because of a CFAA violation to sue for damages or equitable relief. *Id.* § 1030(g).

Since the CFAA's passage 34 years ago, access to computers for personal and work-related activities has become ubiquitous and essential for people to function in society. At the same time, prosecutors and civil litigants frequently use the CFAA's restrictions to patrol certain types of ordinary computer use engaged in by millions of Americans. For example, CFAA has been invoked in suits against individuals who have used their authorized computer access in a manner that breaches conditions imposed by employers' policies, websites' terms of service, or other third-party restrictions.

The question the Supreme Court has agreed to resolve in *Van Buren v. United States*, No. 19-783 (U.S.) is whether a person who is authorized to access information on a computer for *certain* purposes violates the CFAA if s/he accesses the same information for an *improper* purpose. *Van Buren* arises out of a criminal case involving a police sergeant in Cumming, Georgia. The sergeant, Nathan Van Buren, had run into financial troubles and asked a local man, Andrew Albo, for a loan. As part of a sting operation, the FBI instructed Albo to ask Van Buren to run a computer search on a license plate number to determine if a strip club dancer was an

undercover officer. Albo went along with the sting and told Van Buren he would pay him in exchange for the requested information. After receiving $6,000 from Albo, Van Buren used his credentials as a law enforcement officer to access the Georgia Crime Information Center (GCIC) database and run the license plate search. He then texted Albo that he had obtained the information Albo wanted.

Van Buren was arrested, convicted on one count of felony computer fraud in violation of 18 U.S.C. § 1030(a)(2), and sentenced to 18 months in prison. On appeal, he argued that accessing information on the GCIC database for an improper purpose did not "exceed authorized access" as meant by the CFAA. The Eleventh Circuit upheld his conviction, and the Supreme Court granted certiorari. *See* United States v. Van Buren, 940 F.3d 1192 (11th Cir. 2019), *cert. granted*, 2020 WL 1906566 (Mem.) (U.S. Apr. 20, 2020).

The Supreme Court's cert. grant in *Van Buren* will provide much-needed clarity on the meaning of the CFAA's "exceed authorized access" prong—an element required whether the CFAA action is civil or criminal. A stubborn 4-3 circuit split exists among the Courts of Appeals on whether use of a computer for an "improper purpose" is actionable. The First, Fifth and Seventh Circuits have agreed with the Eleventh Circuit's broad interpretation of Section 1030(a)(2) and held that accessing a computer for an improper purpose violates the CFAA, even if the person was otherwise authorized to access the information. *See* EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577 (1st Cir. 2001); United States v. John, 597 F.3d 263 (5th Cir. 2010); Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418 (7th Cir. 2006).

In contrast, the Second, Fourth and Ninth Circuits have held that violation of Section 1030(a)(2) occurs only if a person accesses information on a computer that s/he is prohibited from accessing for any reason whatsoever. If a person in those Circuits has permission to access certain information on a computer, accessing the information for an improper purpose is not illegal. *See* United States v. Valle, 807 F.3d 508 (2d Cir. 2015); WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199 (4th Cir. 2012); United States v. Nosal, 676 F.3d 854 (9th Cir. 2012) (en banc). If Van Buren had been a police officer in New York, North Carolina or California and ran the license plate search using a law enforcement database in any of those states, he could not have been prosecuted under the CFAA.

The Supreme Court's eventual decision in *Van Buren* should establish a uniform meaning of Section 1030(a)(2) applicable nationwide. As Van Buren argued in his cert. petition, "[i]t is intolerable for a broad swath of conduct to be entirely innocent in parts of the country but to constitute a federal crime in others."

But *Van Buren* will have far-reaching effects for civil litigation as well. Many cases involving the CFAA arise out of trade secrets and employment litigation where a defendant uses authorized credentials to obtain computer access to sensitive company information in a manner prohibited by confidentiality agreements or employment policies. In *Citrin*, the Seventh Circuit found a CFAA violation where a former employee accessed data on his work computer for a purpose forbidden by his employer. It was no defense that the employee was entitled to access the same information for other purposes. In the First, Fifth, Seventh and Eleventh Circuits, a CFAA claim is also available in cases where a salesperson uses a work computer to print or download confidential trade secrets in order to gain an advantage before leaving to work for a competitor. Before the enactment of the Defend Trade Secrets Act in 2016, the CFAA was often a way for plaintiffs to get into federal court on such claims where diversity jurisdiction did not exist. If the Supreme Court adopts a narrower interpretation of the CFAA in line with the Second, Fourth and Ninth Circuits, however, "improper purpose" claims could become a thing of the past.

PUTTING INTO PRACTICE: How the Supreme Court decides *Van Buren* will transform the landscape for CFAA claims that arise from breaches of conditions on computer usage by persons who otherwise have authorized computer access. Currently, criminal and civil liability under CFAA's "exceed authorized access" prong depends on the jurisdiction, which inevitably leads to forum shopping and difficult questions regarding proper venue. The Supreme Court's decision will either greatly expand or drastically narrow (if not eliminate) the scope of CFAA liability nationwide in cases where the only alleged violation is a person's use of his or her authorized computer access for an improper purpose. Until the *Van Buren* decision is delivered—probably in 2021—civil litigants should adopt a cautious wait-and-see approach to CFAA "improper purpose" claims.

National Law Review, Volumess X, Number 121