NOW + NEXT

GOVERNMENT INVESTIGATIONS & WHITE COLLAR DEFENSE ALERT | NIXON PEABODY LLP

JUNE 10, 2021

SCOTUS narrows the Computer Fraud and Abuse Act in *Van Buren v. United States*

By Christopher Hotaling, Henry Caldwell, and Krithika Rajkumar

Last week, in *Van Buren v. United States*, No. 19-783, the Supreme Court rendered a major decision narrowing the "exceeds authorized access" clause under the Computer Fraud and Abuse Act ("CFAA"). In a 6–3 opinion authored by Justice Amy Coney Barrett, the Court vacated the conviction of a police officer who accessed a law enforcement database to obtain information available to him for an unofficial purpose. The Court held that the "exceeds authorized access" clause is violated when a user permissibly accesses a computer to obtain information "off-limits" to the user, as opposed to information otherwise available to the user but obtained for improper reasons. The *Van Buren* decision significantly curtails the CFAA's civil and criminal enforcement provisions, and diminishes protections for private information.

The *Van Buren* decision

The question before the *Van Buren* Court was: "Whether a person who is authorized to access information on a computer for certain purposes violates Section 1030(a)(2) of the Computer Fraud and Abuse Act if he accesses the same information for an improper purpose." The CFAA makes it a crime to "intentionally access[ ] a computer without authorization or exceed[ ] authorized access, and thereby obtain[ ] information from any department or agency of the United States." The appellant Van Buren argued that his actions were not a violation of the CFAA because he accessed a database that he was already authorized to use even though he did so for an unofficial purpose. He argued that this did not violate the "exceeds authorized access" clause of the CFAA. The government urged the Court to adopt a broader view of the CFAA, arguing that Van Buren's actions were the type of conduct the CFAA was intended to prevent. After analyzing the statutory construction, congressional intent, and the scope of the CFAA, the Court ultimately determined that the CFAA's "exceeds authorized access" provision "does not cover those who, like Van Buren, have improper motives for obtaining information that is otherwise available to them."

Van Buren's impact on federal criminal prosecutions

The likely impact of the Court's decision in *Van Buren* on the work performed by federal prosecutors can fairly be described as mixed. On the one hand, following the Court's decision, federal prosecutors will continue to use the provisions of 18 U.S.C. § 1030 to target the actions of outside hackers who infiltrate the computer systems of not only government entities (at the

federal, state, and local level) but also computer systems of private entities and corporations. This is because the Court's ruling was explicitly limited to those provisions of Section 1030 that address defendants who access a computer by "exceeding authorized access." Left untouched are defendants criminally liable under Section 1030's provisions targeting those who "intentionally access a computer without authorization." This distinction between an individual "exceeding [his or her] authorized access" and accessing a computer "without authorization" is the critical dividing line. If a defendant, like a hacker located overseas (or anywhere for that matter), has never been granted authorization or approval by an organization to access that organization's computer systems and she forces entry to those systems, then *Van Buren* poses no roadblock to charging her with a federal crime. Interestingly, however, if the intruder is actually an insider to whom the targeted organization has given permission to use its computer system in order for her to perform her job, usually under carefully crafted rules and regulations, *Van Buren* now says that the insider intruder can no longer be prosecuted for a Section 1030 offense.

This inability to prosecute insider intruders with a computer crime under Section 1030 potentially will have broad implications. The most obvious one is that corporate insiders who knowingly and intentionally attempt to steal sensitive information from their employers' computer systems to which they were given access can no longer be prosecuted under Section 1030. However, the *Van Buren* decision may also significantly diminish federal prosecutors' ability to investigate and charge police misconduct cases. As the facts in the *Van Buren* case itself show, Section 1030(a)(2) has been regularly used by U.S. Attorney's Offices across the country to prosecute local law enforcement officers who trade their access to sensitive law enforcement information and databases (such as those maintained by state police agencies that contain drivers' license and license plate information or the FBI's National Crime Information Center ("NCIC"), which houses criminal history information) for profit. While federal prosecutors remain able to charge corrupt law enforcement officers with a number of different crimes, including bribery, obstruction of justice, and civil rights offenses, the Court's decision in *Van Buren* removes an important item from the federal prosecutor's corruption toolbox.

Workplace implications following *Van Buren*

The *Van Buren* decision will inevitably affect how employers pursue legal remedies against employees who have authorized access to company networks who may have accessed a company database and copied or used proprietary data for an unauthorized purpose. The government's interpretation of the statute would attach criminal penalties to "a breathtaking amount of commonplace computer activity," Justice Amy Coney Barrett wrote, potentially criminalizing "everything from embellishing an online-dating profile to using a pseudonym on Facebook."

Now, given the Court's narrow construction of the CFAA, in many circumstances, employers may only be able to gain an avenue into federal court under the federal trade secret statute, the Defend Trade Secrets Act (DTSA). If the information an employee accessed does not meet the DTSA's definition of a "trade secret," then employers may need to rely on any contractual provisions that prohibit disclosure or misuse of confidential information. Employers can still bring CFAA claims against employees who access information they are not authorized to access.

Data-scraping in the wake of *Van Buren*

The *Van Buren* decision could also have consequences on how companies protect against, or pursue, third-party misuse of data. Many companies with public-facing websites are often exposed to the practice of "data scraping"—an automated process using computer algorithms to extract data from

the internet. Civil lawsuits have been filed under the CFAA against companies using data scraping tools to obtain, for example, pricing information from competitors' websites or data from public profiles that is then consolidated and sold to downstream users. In both instances, and similar to *Van Buren*, the data being scraped is otherwise available to defendants, but obtained in ways, or for reasons, that contravene policies and terms of use established by the owners or custodians of the data.

In the past, federal appellate courts have split over whether the use of data scraping tools to extract data violates the CFAA. Currently, there is a petition for writ of certiorari pending in *LinkedIn Corp. v. hiQ Labs, Inc*., No. 19-1116, which, if granted, will address that question but in the context of the CFAA's "without authorization" prong. Now, with the *Van Buren* decision, the Court's narrow approach to interpreting the CFAA's "exceeds authorized access" prong suggests that the CFAA might not be an effective tool to prevent data scraping of public-facing websites moving forward. The practical effect is that companies with public-facing websites will have to be more diligent in monitoring online visitors, enforcing terms of use to revoke visitor authorization, and, if considering litigation, pursuing other theories of liability, including common law breach of contract or trespass.

Looking ahead

At least for now, commonplace computer activity will not result in penalties under the CFAA. It is not clear yet how *Van Buren* will change CFAA enforcement or if Congress may consider amending the CFAA or pass other legislation to address the Court's ruling. Nixon Peabody will continue to monitor the aftereffects of *Van Buren*. For more information on the content of this alert, please contact your Nixon Peabody attorney or:

- Christopher Hotaling, 312-977-4418, chotaling@nixonpeabody.com
- Henry Caldwell, 312-977-4435, hcaldwell@nixonpeabody.com
- Krithika Rajkumar, 617-345-1376, krajkumar@nixonpeabody.com