Intellectual Property & Technology Law Journal

Edited by the Technology and Proprietary Rights Group of Weil, Gotshal & Manges LLP

VOLUME 33 • NUMBER 2 • FEBRUARY 2021

What's "So" Important? Computer Fraud and Abuse Act Gets a Close Look from the U.S. Supreme Court

Aime Dempsey

In a case with significant ramifications for employers concerned with protecting sensitive information, and for employees accused of abusing access to computer networks, the U.S. Supreme Court ("SCOTUS") heard oral argument[1] in *Van Buren v. United States*,[2] a case from the U.S. Court of Appeals for the Eleventh Circuit that will require interpretation of the Computer Fraud and Abuse Act ("CFAA").[3]

The argument was lively. All of the Justices asked questions, and several expressed concern about vagueness in the CFAA's definition of covered activity. Much of the discussion centered on an alleged "parade of horribles," and on the meaning of the word "so."

A relatively prompt decision is expected. Time will tell what SCOTUS will decide, but we would not be surprised to see a reversal and remand.

Aime Dempsey is a member of the firm in the Litigation and Employment, Labor & Workforce Management practices in Epstein Becker & Green, P.C.'s New York office. She handles a broad range of commercial and employment-related matters, including those involving employee mobility, and confidential information, across tribunals. Ms. Dempsey may be contacted at *adempsey@ebglaw.com*.

THE CFAA

The CFAA has been a useful litigation tool for employers when confidential or other sensitive information accessed via computer is misappropriated, misused, or otherwise compromised. The CFAA generally prohibits obtaining sensitive information from a computer without authorization, or by exceeding authorized access, and, importantly, confers federal jurisdiction. While it is a criminal statute, it also provides for a private right of action for those damaged by certain violations.

The issue now before SCOTUS in *Van Buren* is whether the CFAA is violated when someone with authorized access obtains information for an unauthorized purpose.

For example, when an employee who is authorized to access and use the employer's computer-stored customer information for business purposes downloads the information to a thumb drive and shares it with a potential new employer, the employee plainly violates company policy. But does the employee run afoul of the CFAA? Over time, a circuit split has developed regarding this issue.

VAN BUREN

Van Buren is a criminal case in which Petitioner Nathan Van Buren, a police sergeant in Cumming,

Georgia, was convicted of violating the CFAA. The Eleventh Circuit affirmed his conviction and SCOTUS granted *certiorari*.

Briefly stated, as part of his duties Van Buren was granted authorized access to a database containing license plate and vehicle registration information maintained by the Georgia Crime Information Center ("GCIC"). Training materials supplied to those with access to the GCIC database quite reasonably prohibit use of the database for personal purposes. However, in return for cash payments, Van Buren agreed to, and did, use his authorized GCIC username and password to access a woman's license and registration information in order to learn personal information about her on behalf of another individual.

There is no dispute that such use was not within the GCIC guidelines for authorized use. Accordingly, Van Buren used his authorized access to the GCIC database for an unauthorized purpose. He was charged with, among other things, violating the CFAA. He was convicted of the CFAA violation, sentenced to 18 months in prison, and he appealed. The Eleventh Circuit upheld the conviction, holding, based on precedent within the circuit, that the unauthorized use of authorized access does constitute a violation of the CFAA.

Because Van Buren was not an outsider or other unauthorized user hacking into the GCIC database, his conviction under the CFAA turns on application of the facts to the CFAA's prohibition on "exceeding authorized access." The CFAA defines "exceeds authorized access" to mean "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."[4]

CIRCUIT SPLIT

Generally, the U.S. Courts of Appeals for the First, Fifth, Seventh, and Eleventh Circuits construe the definition broadly, finding CFAA violations against employees, for example, who access information they are entitled to obtain for certain purposes, but do so for unauthorized uses.

In other words, courts in those circuits tend to focus on the purposes of authorized access and require computer users to stay within those purposes in order to avoid violations of the CFAA. This interpretation would allow an employer to bring an action under the CFAA against an employee who, for example, misappropriates sensitive business information the employee was entitled to access as part of his or her job for use with a subsequent employer.

The U.S. Courts of Appeals for the Second, Fourth and Ninth Circuits, on the other hand, favor a narrower interpretation, in which there is no violation unless the accessed information at issue is, itself, not information the user is entitled to obtain or access at all. Under that construction, an employee who obtains information from a database that the employee is not otherwise permitted to use (e.g., restricted human resources information by someone not within the permitted sphere) would violate the CFAA while someone who misuses information he or she is otherwise entitled to access would not.

THE ARGUMENTS

Van Buren is the first case to present the issue to SCOTUS. Petitioner, with robust *amici* support from organizations like Reporters Committee for Freedom of the Press, National Whistleblower Center and technology companies, largely focused his arguments on the dangers of a "parade of horribles" that could arise from the broader interpretation.[5]

Petitioner posited that, for example, computer users who check Instagram on their work computers in violation of their employer's computer use policies, or those who inflate their characteristics on a dating site, in violation of the stated terms of use of such sites, could be guilty of a federal crime should the government choose to prosecute.[6] He argued that the CFAA is impermissibly vague and that any changes should be left to Congress.

The government's position that the CFAA should be broadly read was also supported by several *amici*, including the Electronic Privacy Information Center and the Digital Justice Foundation. The government contended that, pursuant to the definition, a user "exceeds authorized access" by accessing information that he or she did not have a right to access in the particular manner or circumstances used.

Thus, Van Buren violated the CFAA, according to the government's position, because he accessed the GCIC under circumstances other than for law enforcement purposes. As part of its argument, the government closely examined the meaning of the word "so" in the definition of "exceeds authorized access," and contended that a person is "entitled so"

to do something only when he or she has a right to do it in the particular manner or circumstance authorized.[7] Van Buren, on the other hand, contended that "so" refers only to "access[ing] a computer with authorization" such that an individual does not "exceed authorized access" if entitled to access the database in question at all.[8]

The questions from the Justices during oral argument closely followed those competing themes, further discussing the proper construction of the word "so," and examining whether some of the more innocuous-sounding activities would actually constitute violations of the CFAA under the broader construction.

Some expressed concern about the privacy of the public if the CFAA is not construed to encompass, for example, government employees reviewing private information for purposes other than those called for in their jobs.[9]

Based on the overall tenor of the argument, SCOTUS may be prepared to agree with the more narrow interpretation currently favored by the Second, Fourth and Ninth Circuits, and to overturn Van Buren's criminal conviction that turned on the broader interpretation. In any case, stay tuned.

CONCLUSION

We observe use of the CFAA in civil cases to already be diminished in the last four years. Passage of the Defense of Trade Secrets provides access to federal courts in circumstances where the CFAA was used to create federal jurisdiction. And as explained above, use of the CFAA in such cases has been curtailed in several circuits.

It will be interesting to see whether the SCOTUS decision in *Van Buren* further restricts its utility.

Notes

1. *https://www.supremecourt.gov/oral_arguments/argument_transcripts/2020/19-783_7l48.pdf.*
2. No. 19-783, *https://www.supremecourt.gov/search.aspx?filename=/docket/docketfiles/html/public/19-783.html.*
3. 18 U.S.C. § 1030.
4. 18 U.S.C. § 1030(e)(6) (emphasis added).
5. *See, e.g.*, Oral Argument at 8, *supra* note 1.
6. Oral Argument 4, 22, *supra* note 1.
7. Brief for the United States at 13, *https://www.supremecourt.gov/DocketPDF/19/19-783/137649/20200310124445680_19-783%20Van%20Buren.pdf.*
8. Oral Argument at 21, *supra* note 1.
9. Oral Argument at 14, *supra* note 1.