Armstrong Teasdale

June 4, 2021 • Advisory • www.atllp.com

SCOTUS LIMITS SCOPE OF CYBERSECURITY LAW

Last November, the United States Supreme Court heard oral argument in *Van Buren v. United States* to interpret the scope of the Computer Fraud and Abuse Act (CFAA), a 1986 federal statute that imposes civil and criminal liability for unauthorized computer access. Yesterday it issued its decision.

In short, the Supreme Court decided that, so long as an individual has authorization to access a computer and data, they do not violate the "exceeds authorized access" clause of the CFAA. This means that an individual's intended use for a computer and/or data is not relevant to whether the individual violated the CFAA. This may require employers to reconsider their employee handbooks, policies and procedures.

Looking more closely at the decision, the main issue decided by the Supreme Court has divided federal circuit and district courts nationwide:

Whether accessing and obtaining information from a computer system for a purpose other than the purpose for which that person was granted authorization "exceeds authorized access" in violation of the CFAA?

The *Van Buren* Facts

Nathan Van Buren was prosecuted with computer fraud under the CFAA for accessing the police department's computer database from his patrol car to obtain license plate information in exchange for financial gain.

Since as a police officer Van Buren was authorized to access the database for law enforcement purposes, but not for *non-law* enforcement purposes, he was charged under Section 1030(a)(2)(c) of the CFAA (and for honest services wire fraud) and convicted by a jury.

The Eleventh Circuit, having previously adopted a "broad interpretation" of the CFAA, affirmed his conviction. Van Buren then appealed to the Supreme Court.

Analysis of the Issue

The CFAA defines "exceeds authorized access" as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the (accessor) is not entitled so to obtain or alter."[1]

Van Buren argued that the CFAA only applies if the accessor was not entitled to obtain the information under any circumstances. Under this narrow interpretation, Van Buren asserted that access to the database, even if for an improper purpose, was not unauthorized since he had valid credentials to access the license plate information for law enforcement purposes.

PEOPLE

Lucas Amodio, C|EH

SERVICES AND INDUSTRIES

Data Innovation, Security and Privacy

The government disagreed, arguing that the CFAA criminalizes obtaining information for a particular purpose if the individual was not entitled to obtain the information for that purpose. During oral argument in November, the Justices seemed to express doubts about the government's broad interpretation.

Justice Sonia Sotomayor expressed concern that the government's broad interpretation created ambiguity, Justice Neil Gorsuch expressed concern that it expanded policing powers, and the other Justices acknowledged that there are state laws that address the same conduct, but also that exonerating the conduct could remove protections for personal privacy.

The Decision

As it indicated it might do at oral argument in November, the Supreme Court rejected the government's broad interpretation of the CFAA. Justice Amy Coney Barrett wrote for the majority and took issue with the CFAA's ambiguity and how easily the CFAA could be misapplied, holding that Van Buren did not "exceed authorized access" even though he obtained information from the database for an improper purpose.

Referring to the potential for "a sleight of hand" by the government and "millions of otherwise law-abiding citizens" being criminals, Justice Barrett wrote "on the Government's reading of the statute, an employee who sends a personal e-mail or reads the news using her work computer has violated the CFAA," and that "everything from embellishing an online-dating profile to using a pseudonym on Facebook" could be a felony.[2]

Justice Barrett's grasp of the CFAA and its application to everyday settings – "[t]ake the work place" – is in contrast to the CFAA's history. While intended primarily to thwart hackers by criminalizing their conduct, since its enactment in 1986 the CFAA has rarely been amended. This has led some states to enact their own unauthorized access statutes. Utah and Florida, for example, have enacted the Computer Abuse and Data Recovery Act to safeguard organizations from unauthorized use and access to computers, platforms and data.[3]

Now that the Supreme Court has rejected broad interpretation of "exceeds authorized access," the CFAA can no longer be used against employees who access company information for improper purposes. But as plainly stated in the last paragraph of Justice Barrett's holding, the CFAA is violated when an employee "accesses a computer with authorization but then obtains information located in particular areas of the computer – such as files, folders, or databases – **that are off limits to him**."[4] Emphasis added.

Going Forward

In the past, many employers have relied on the CFAA to pursue current and former employees who misuse computer resources and data, such as by copying client databases for use at future employers. However, now those employers should review their options, including state-based laws to protect

their data.

In view of the decision, organizations such as employers that rely on or reference the CFAA to deter misuse of information should consider:

- Restricting access to certain information either via specific contract provisions and/or segmenting or separating data in different databases to restrict access.
- Securing restricted data and implementing software that warns employees before they access restricted areas.
- Revising employee handbooks and policies and procedures to align with *Van Buren* and state-based cybersecurity and data privacy laws.
- Revise contracts to include limitations on data access.
- Providing training to management and employees that emphasizes the above limitations and restrictions, and evolving laws and industry standards.

While the CFAA is still effective for prosecuting hackers, time will tell if the federal government will amend the CFAA to address the type of situation that "exceeds authorized access." Given the central importance of data – the new electricity, gold and oil – laws relating to the confidentiality, availability and integrity of data will continue to rapidly evolve.

If you have any questions about the application of *Van Buren* and the CFAA, please contact any of the authors of this advisory or your regular Armstrong Teasdale attorney.

[1] 18 U.S.C. § 1030(e)(6).

[2] *Van Buren v. United States*, 593 U.S. ___, 18 (2021).

[3] *See* Utah Code Ann. § 63D-3-104 and Fla. Stat. § 668.801.

[4] *Van Buren v. United States*, 593 U.S. ___, 20 (2021).