KANE RUSSELL COLEMAN LOGAN

One Mission. Your Mission.

How Employers Should Respond to SCOTUS' "Exceeds Access" Computer Fraud Decision

Employment Law / June 3, 2021 / Demetri J. Economou

Much has been written recently about the "new look" Supreme Court. On the heels of four 9-0 decisions favoring different sides of partisan divide, today we got *Van Buren*, a 6-3 decision delivered by Justice Amy Coney Barrett, joined by Breyer, Sotomayor, Kagan, Gorsuch, and Kavanaugh, with Thomas, Roberts, and Alito dissenting.

Van Buren

Van Buren is a Computer Fraud and Abuse Act (CFAA) case.

- Nathaniel Van Buren was once a police sergeant in Georgia.
- Targeted in an FBI sting operation, Van Buren was told to access license plate information from the police department's database and, in exchange, he'd receive a payoff of $5,000.
- The plan worked. Van Buren accessed the information and was busted. He was charged with a felony violation of the CFAA for "exceeding authorized access" of the department's database.

But Van Buren argued that the department granted him access to the license plate database. He didn't hack the system. Instead, he accessed information that he was allowed by his employer to view. His improper purpose in accessing the database should not have played into whether he violated the CFAA.

The Supreme Court agreed. Van Buren had access; therefore, he could not violate the CFAA no matter his motives.

The opinion is available here.

"Exceeds Authorized Access" and What Employers Need to Do

The broadest type of CFAA violation is under § 1030(a)(2)(C), when a person:

> "intentionally accesses a computer without authorization or exceeds authorized access, and obtains... information from a "protected computer."

Courts have aptly described a "protected computer" as "*essentially any computer connected to the internet*" as the statutory definition includes "any computer used in interstate commerce or foreign commerce or communication."

The CFAA defines "exceeds authorized access" as:

> access [to] a computer with authorization and [using] such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter.

And that's where *Van Buren* turned. While the CFAA reaches virtually every computer, it does not reach all actions that could be performed by a computer accesser.

Justice Barrett cautioned that interpreting "exceeds authorized access" to include databases to which an employee has already been granted access would: "attach criminal penalties to a breathtaking amount of commonplace computer activity."

"For instance," she wrote, "employers commonly state that computers and electronic devices can be used only for business purposes. On the Government's reading, an employee who sends a personal e-mail or reads the news using a work computer has violated the CFAA."

So how do employers respond?

The CFAA establishes both criminal penalties and civil remedies. To the extent employers want to continue availing themselves of the civil claim, "access" will have to change.

- **Compartmentalize Access.** As a matter of convenience, many employers—especially small and mid-sized employers—grant access only once. Once an employee has a login and password, he can access a broad amount of company information. Under *Van Buren*, there is no CFAA violation once the employee has access for any purpose. Consider compartmentalizing access to suit the needs of *normal* usage for particular employees. That will admittedly be infeasible for many companies.
- **Tailored Confidentiality Provisions.** Setting aside the lack of criminal penalties, a contractual confidentiality obligation can mimic the pre-*Van Buren* benefits of the CFAA when trade secrets are not in play. The drawback is that a breach of contract won't get you into federal court without diversity jurisdiction. When trade secrets are present, consider using the Defendant Trade Secrets Act (DTSA) to land in federal court.

We can't make the cure worse than the disease. If business drivers require broad access, then companies will simply need to abandon the protections of the CFAA. This makes strong confidentiality agreements all the more important.

***

Demetri Economou is a Director in Kane Russell Coleman Logan's Labor & Employment and Energy Practice Groups.

Related Attorneys

Demetri J. Economou

Related Practices

Labor & Employment