Supreme Court in Van Buren Narrows Scope of the Computer Fraud and Abuse Act

by Edward B. Magarian and Briana Al Taqatqa

On June 3, 2021, the U.S. Supreme Court resolved a long-standing question about how the Computer Fraud and Abuse Act ("CFAA") applies to employees who access their employers' computer systems for their personal benefit. Specifically, the Court's decision in *Van Buren v. United States* addressed whether someone "exceeds authorized access" under the CFAA when they use otherwise valid credentials to access a computer for an unlawful or unauthorized purpose. The case arose when Nathan Van Buren, a former police sergeant, ran a license-plate search in a law enforcement computer database in exchange for money. Although Van Buren was *permitted* to use the database in the course of his work, his *purpose* in doing was not related to law enforcement purposes and violated department policy. Van Buren was therefore charged criminally, under the CFAA.

The case made it to the Supreme Court, which ultimately decided that the CFAA prohibits individuals from accessing computers with authorization but then obtaining information located in particular areas of the computer that are off-limits to them. Put differently, a person does *not* violate the CFAA by accessing a computer he or she is allowed to access and obtaining information in areas of the computer that he or she is allowed to view, regardless of the individual's purpose in accessing such data. The Court emphasized that punishing authorized access that occurs for unauthorized purposes would create boundless criminal liability:

If the "exceeds authorized access" clause criminalizes every violation of a computer-use policy, then millions of otherwise law-abiding citizens are criminals. Take the workplace. Employers commonly state that computers and electronic devices can be used only for business purposes. So 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.

Although *Van Buren* was a criminal case, it has clear implications for employers who learn that their employees (oftentimes, *departing* employees) have accessed company

Related People

- Edward B. Magarian
- Briana Al Taqatqa

Related Capabilities

- Labor & Employment
- Labor & Employment Guides
- Privacy & Social Media

servers and downloaded confidential information for their own purposes. In the past, some employers have tried to assert civil claims under the CFAA for such conduct. But the Court's decision effectively closes that door: the purpose of the CFAA is to punish computer hacking and not "commonplace computer activity." After *Van Buren*, employers will have to rely on other types of claims (breach of non-disclosure agreements, trade secret misappropriation, and breach of common law duties of loyalty) to address employees who misuse electronically stored information.

Ultimately, *Van Buren* serves as a useful reminder that employers must be vigilant about controlling access to their internal computer systems. Employers should password-protect confidential information and strictly limit access to that information. Additionally, employers should have clear policies and procedures that prohibit improper access to confidential information, and they should use confidentiality agreements for employees in sensitive positions. While the CFAA may no longer provide a legal remedy for many types of improper computer access, employers still have a number of tools available to protect sensitive business information.

The full opinion in *Van Buren v. United States*, is available here.