Insights, News & Events

SCOTUS DECISION USHERS IN THE "GATES UP OR DOWN" ERA FOR EMPLOYERS SEEKING TO PROTECT WORKPLACE COMPUTERS AND ESI

The Post-Van Buren Workplace and the Computer Fraud and Abuse Act

Insights
Jul 6, 2021

The U.S. Supreme Court has once again defined the rules of the road for millions of employers and employees in the American workplace with its recent decision in *Van Buren v. United States*. The Court's opinion resolved conflicting interpretations of a federal statute, the Computer Fraud and Abuse Act, 18 U.S.C. Section 1030 ("CFAA"), which protects workplace computers and the information stored on them from different types of unauthorized access, whether perpetrated by current employees like appellant Nathan Van Buren, former employees, or business competitors. As is the case with many of the Court's opinions, the Justices didn't just resolve the legal issue presented by *Van Buren*. The Court notably set the stage for future workplace litigation under the CFAA, and this so far is perhaps the most underdiscussed and important aspect of *Van Buren*.

FBI Undercover Sting Operation Leads to an Employee's Arrest, Conviction – and SCOTUS Exoneration

Nathan Van Buren was convicted for unauthorizedly accessing information stored in his employer's computer system. He was a police sergeant who, as part of his day-to-day responsibilities, had access to a state law enforcement database containing driver's license information. However, Van Buren used his own, valid access and log-in credentials to obtain information from this computer and database for a private citizen who paid Van Buren for the information. Not surprisingly, this was improper: it violated police department

Related People

Brent A. Cossrow
Regional Managing Partner
610.230.2135

Usama Kahf, CIPP/US
Partner

policy and training against obtaining information in the database for non-law-enforcement purposes. Unbeknownst to Van Buren, his search and bribe were part of a Federal Bureau of Investigation sting operation.

Van Buren was charged with a felony violation of the CFAA, ultimately convicted and sentenced to 18 months in prison. Van Buren appealed, arguing that the "exceeds authorized access" clause of the CFAA applies only to people who do not have access to the computer data that they took. His position was that the CFAA does not apply to employees who misuse the access that they were given by their employers or use that access for an improper purpose. These arguments were rejected by the Eleventh Circuit Court of Appeals, which affirmed Van Buren's conviction.

In a 6-3 decision, the United States Supreme Court reversed and agreed with Van Buren's understanding of the CFAA. The Court held that an employee does not violate the CFAA for obtaining information from a computer and using it for an improper purpose in violation of training or policies, where the employee was authorized to access the computer and obtain the information in the first place. The Court's decision confirmed that this misuse of the information from a computer for an improper purpose cannot give rise to civil and criminal liability for such an employee under the CFAA, even if prohibited by workplace policies.

Computer and Electronically Stored Information in the American Workplace

Van Buren is the first case involving an interpretation of Section 1030(a)(2) of the CFAA to reach the Supreme Court, and its importance and reach cannot be overstated. With each passing day, an ever-increasing number of employers provide their employees with a workplace computer and access to electronically stored information residing on them, their servers, and Clouds. Some of these same employees also are given access to one or more additional electronic devices, such as smartphones, laptop computers, and tablets. This growth trendline spans myriad industries, professions, and trades, making *Van Buren* an apex-precedent that will govern and impact an ever-increasing number of American employers and employees as time moves forward.

For Employers, It's Gates Up or Gates Down Under the CFAA's Section 1030(a)(2)

949.798.2118

Service Focus

Employee Defection and Trade Secrets

Litigation and Trials

Privacy and Cyber

This makes it even more important that employers understand the arguments that the Court accepted and rejected, and how the majority's opinion affects the American workplace.

In reversing Van Buren's conviction, the Supreme Court tackled the question that has vexed and divided federal courts when interpreting the CFAA: whether Van Buren's improper use of information that he was indisputably authorized to access violated the CFAA. The majority opinion in *Van Buren* was written by Justice Amy Coney Barrett, through which the Court concluded that if an employer gives an employee access to the computer and the information on it, then the employee does not exceed authorized access by using the information for an improper purpose. According to the Court, the employee's purpose is not the standard or the test, even when that purpose is prohibited by workplace policy or training materials – as was the case with Van Buren. Instead, the Court accepted Van Buren's argument that the CFAA is violated when employers take steps to prohibit employees from accessing information on computers they are authorized to use.

The focal point for the Court is how and what the employer did to prohibit its employees from accessing certain electronically stored information on the employer's computers. Referring to this as the "gates-up-gates-down" approach to the CFAA, the majority held that Van Buren's employer, a Georgia police department, did not "lower the gates" to protect the license plate information that Van Buren sold in the sting operation. According to the Court, "if a person has access to information stored in a computer—e.g., in 'Folder Y,' from which the person could permissibly pull information—then he does not violate the CFAA by obtaining such information, regardless of whether he pulled the information for a prohibited purpose. But if the information is instead located in prohibited 'Folder X,' to which the person lacks access, he violates the CFAA by obtaining such information." As the Court noted, under Van Buren's argument, "liability stems from a gates-up-or-down inquiry—one either can or cannot access a computer system, and one either can or cannot access certain areas within the system."

With this holding, the Court resolved a split within the federal judiciary regarding the meaning of "exceeds authorized access" under the CFAA, which was the basis for Van Buren's conviction. In the run-up to *Van* Buren, several

federal courts took what has been described as a more employer-centric view on the CFAA, which was the underpinning of Van Buren's conviction: if an employer proscribed an improper use of data or purpose on a workplace computer in an employment policy or manual, then an employee could face liability under the CFAA for violating that policy. Other federal courts took what has been perceived as the more employee-centric view, rejecting the focus on the purpose of the use of the data, which was argued by Van Buren and ultimately adopted by the Supreme Court.

The Post-*Van Buren* Workplace and The CFAA Disputes To Come

In resolving this split within the federal judiciary, the Court framed the issues that will define the next generation of litigation in the American workplace under the CFAA.

One issue that will be played out is whether *Van Buren* resolved the employer-centric versus employee-centric interpretations of the CFAA or whether the Court redefined the issue. Yes, Van Buren's conviction was reversed; the Court took an employee-centric view by rejecting "employee purpose" for obtaining the data as the standard. But something else happened in *Van Buren*. *The Court reserved to employers the power to lower the gate and prohibit access to data on their computers*. In its discussion of employers "lowering the gate," the Court noted that "for the present purposes, we need not address whether this inquiry turns only on technological (or "code-based") limitations on access, or instead also looks to limits contained in contracts or policies." These limitations, contracts, and policies are the hallmarks of the more employer-centric, pre-*Van Buren* opinions. Thus, while *Van Buren* looks like an employee-centric decision that reversed an employee's conviction for misusing data stored on his employer's computer in violation of employment policies and training, the Court in fact has given the American workplace an employer-centric precedent.

The next generation of litigation will probably focus on what an employer needs to do to lower the gate and ensure CFAA protection of data residing on workplace computers. Is a well-written contractual clause or workplace policy enough? Or is the gate only lowered when, to quote the Court, Folder Y is protected by a password that only a few people have access to within a company? The Court explicitly took a

pass on this question. To trade secrets practitioners, this issue has echoes of Uniform and Defend Trade Secrets Act language that focuses on whether a company took reasonable steps to protect the secrecy of the purported secret, and employers and employees might see equally robust litigation to determine whether the steps taken to lower the gate were sufficient to protect the employer's underlying information under the CFAA.

This will still beg another question presented by *Van Buren*: whether **every** gate in the castle must to be lowered to ensure that the access is unauthorized. Consider the following hypothetical: suppose an employer has two offices in one state. Each office maintains traditional P&L data in folders on its computer servers. One first office took the time and effort to password-protect the folders containing the P&L information. The passwords were known only to a small number of accounting department personnel, and this office published a workplace policy which stated that P&L information is accessible only to these accounting personnel. But the second office took no such steps: no passwords and no policy. What happens when two company employees, one in each office, access the information in each office's folders to jointly open a competing office in the same state? What about separate competing offices? Does each employee face liability under the CFAA? Only the employee in the office that lowered the gate? Neither employee because the employer did not lower all of the gates? This issue was not before the Court in *Van Buren*, but it is hardly a stretch to say that this hypothetical could play itself out in next generation of post-*Van Buren* litigation.

Conclusion

We'll continue to monitor developments in this area, so make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information. If you have any questions about how this decision may impact your business, please contact your Fisher Phillips attorney, the authors of this Insight, or any attorney in our Employee Defection and Trade Secrets Practice Group.