ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

UPDATE: Can Employees Be Convicted of a Crime for Unauthorized Use of Work Computers?

Compliance and Ethics

UPDATE: The US Supreme Court has now scheduled oral argument in this case for Monday, Nov. 30, 2020, most likely starting at 10 am. The argument will be held virtually, not in person, and may be heard live-streamed through various media outlets including C-SPAN. A transcript and a recording

will also become available on the Court's website.

Businesses frequently publish rules that limit employee use of company computers. All too often they discover employees' computer use goes beyond those limits and imperils valuable information.

But when does this kind of workplace misconduct become a criminal act, and how should employers craft internal policies to deter these activities? Because the lower courts have come to vastly inconsistent conclusions about these matters, the US Supreme Court will now address them, hearing arguments later this year or early next.

On April 20, 2020, the US Supreme Court agreed to hear argument in Van Buren v. United States to address the following questions:

- Does it violate the Computer Fraud and Abuse Act (CFAA), a federal criminal statute, for a person who has permission to access information on a computer for certain purposes to exceed that permitted use?
- Does the CFAA criminalize a police officer's use of an official database for personal profit?

Implicit in the Court's conclusions on these issues will be an answer to a third important question to employers, but one that trial and appeals courts have answered both yes and no:

- Has a departing employee committed a crime under the CFAA if he or she copies the employer's intellectual property (IP) or customer lists using his or her work computer and downloads it to a personal device or emails it to a soon-to-be new employer?

The eventual Supreme Court decision should resolve the deeply divided approaches of the lower courts that have led to sharply inconsistent results. Presently, the same act that could send an employee to prison in Chicago is not even a crime in New York or San Francisco. Employers and employees alike will benefit from consistency and certainty.

Background

Congress passed the CFAA in 1986 as a tool to fight computer-related crimes at a time when the personal computer recently had become a ubiquitous part of US offices. Since then the CFAA — a criminal statute that also provides for civil liability — has developed into an important vehicle for law enforcement to attack computer fraud, as well as a tool for businesses to protect valuable information and systems.

The CFAA makes it a federal crime to "intentionally access a computer without authorization" or to "exceed authorized access," and "thereby obtain information from any protected computer." In substance, any computer with access to the internet is deemed "protected."

The courts have struggled to determine what conduct the above-quoted language prohibits, largely because the term "without authorization" is undefined in the statute. The phrase "exceeds authorized access" is defined, however, to mean "to access a computer with authorization and use such access to obtain or alter information in the computer that the accessor is not entitled to obtain or alter."

Congress's failure to define "without authorization" while incorporating that term into the definition of "exceeds authorized access" has bred a deep split in how courts interpret these critical terms, the

meanings of which are necessary to distinguish between criminal and lawful conduct under the CFAA.

International businesses with employees in the United States should be aware that the CFAA likely applies to their US workplaces, and that the law's criminal liability provisions in particular may differ from the law in their home countries.

Under some national laws, for example, a current or former employee who violates a non-disclosure obligation arising from a confidentiality agreement with an employer can be criminally prosecuted regardless of how the confidential information was acquired or transmitted. As the discussion below will illustrate, the CFAA imposes many more limits on criminal liability for employee misconduct of this nature.

The Circuit Court split

There are two prevailing interpretations of the kind of conduct that Section 1030(a)(2) of the CFAA criminalizes, and the courts are equally divided between these two distinct approaches. The courts taking the first approach tend to limit the criminal liability of employees strictly to those situations where the computer was used without permission. Courts taking the second, more expansive approach go beyond this and consider whether authorized employees exceeded their permitted use.

1. How was the information accessed?

In the Second, Fourth, and Ninth Circuits, a person using a computer with an internet connection violates the CFAA only if that person accesses a computer without permission. These courts focus their inquiry solely on how access was gained — whether or not the offender was authorized to use the computer — and do not consider why or how the offender used or intended to use the information.

Thus in states falling within these three circuits, including New York and California, an employee who is authorized to access a computer and uses it to steal the employer's trade secrets to sell for his personal profit will not have violated the CFAA, although he likely will be liable civilly under other statutory and common law theories.

2. How was the information used or intended to be used?

In the First, Fifth, Seventh, and Eleventh Circuits, however, a person using a computer with an internet connection violates the CFAA even if that person uses a computer with permission, but "exceeds" the scope of that person's permitted use (e.g., by using the information accessed for an unauthorized reason or purpose).

The three Circuit Courts of Appeals that refuse to base liability on whether a defendant's use of an employer's (or other third party's) computer exceeded the authority given have asserted that the key statutory term "without authorization" is ambiguous as used, and that the CFAA was intended to be an anti-hacking statute when Congress enacted it. They also persuasively state, as the Eleventh Circuit conceded in *Van Buren*, that the "purpose of use" test "allows employers or other parties to

legislate what counts as criminal behavior through their internal policies or their terms of use."

Employers should note that, depending on how the Supreme Court decides this case, their policies and procedures about computer and network access and authorization may become the focus of the courts and law enforcement agencies when an employer claims that a disloyal employee has stolen or otherwise abused his access to its intellectual property or other confidential information.

The facts in *Van Buren v. United States*

The facts presented in *Van Buren v. United States* illustrate the breadth and potentially arbitrary scope of criminal liability under the CFAA if a criminal violation can be found and liability can attach despite an employee's authority to use a company computer to access information, but does so for a purpose that exceeds the authority delegated — and defined — by the employer. These issues potentially affect all employees, including managers.

Van Buren was a police officer in an Atlanta suburb who, facing financial difficulties, asked a local petty criminal, Albo, for a loan, unaware that Albo was recording their conversation. Albo shared his recording with local police officers, who took it to the FBI.

Interested in what Van Buren would be willing to do in exchange for the loan he requested from Albo, the FBI told Albo to condition the loan on Van Buren's agreement to run a computer check on the license plate number of a car driven by a person who Albo was to say he suspected was an undercover officer. Van Buren agreed to Albo's request. Albo gave him US$5,000 and told Van Buren he did not have to pay back the money.

After that meeting with Albo, Van Buren accessed the Georgia Crime Information Center database, which contains license plate and vehicle registration information. As a Georgia law enforcement officer, Van Buren was authorized to access that database via computer "for law-enforcement purposes."

He ran a search for the license plate number Albo had given him. After sending Albo a text message advising him that he had the promised information, Van Buren was arrested. He was charged with computer fraud under the CFAA for accessing the state database for an unauthorized reason, as well as with "honest services fraud" for taking an official act in exchange for a bribe.

Van Buren moved to dismiss the CFAA count at trial in the Northern District of Georgia, but his motion was denied, and a jury convicted him on both counts charged.

On appeal, the Eleventh Circuit vacated the honest services fraud conviction because of an erroneous jury instruction. But the appellate court affirmed his conviction under the CFAA, finding itself bound by its 2010 holding in another case that rejected the stricter interpretation of "without authorization" urged by Van Buren and embraced by the three circuit courts referred to above.

The Supreme Court's interpretation will have meaningful consequences for employers, employees, and others

The Supreme Court's answer to the questions presented in *Van Buren* will have wide-ranging implications in the employment setting, given the conditional access employees routinely have to company-owned computers and information accessible on them. That is, while employers provide

most employees in an office setting with computers having network and internet access, employers generally condition employee access on adherence to often comprehensive rules intended to protect the employer's interests.

Those rules typically limit access to certain information residing on a network to specific employees who have a need to know, and also forbid access and use of such information for certain purposes, such as disclosure to a competitor or for personal profit. They likewise limit or prohibit the use of company computers to access the internet for certain activities, such as infringing on copyrights and downloading pornography.

Should the Supreme Court adopt the view of the Second, Fourth, and Ninth Circuits and criminalize only unauthorized access to company-owned computers by employees regardless of the purpose of the particular use, the usefulness of the CFAA as a tool to hold employees criminally and/or civilly liable for the unauthorized disclosure or use of information will be severely limited.

If, on the other hand, the Court sides with the other four circuits that have considered the question, the CFAA will become a more certain and potent weapon in an employer's arsenal for combating theft or other misuses of IP, confidential information, and other valuable materials potentially accessed by employees using company computers.

The Supreme Court will hear argument in its next term scheduled to begin in October 2020, and a decision can be expected in the first six months of 2021.

Practical takeaways

This case draws useful attention to the importance of employer policies addressing computer and network access and computer use. In general, employers may want to review their existing policies and determine whether updates are needed.

For example, employers might look at whether existing policies limit authorized use of company computers strictly to the work station or laptop assigned to each employee, and whether authorized access to parts of a network is limited strictly and explicitly to certain employees with a need to know.

For international businesses operating in the United States, computer-use policies can be particularly challenging in view of the differing data protection regimes and privacy cultures.

Stay tuned as the Supreme Court weighs in on legal questions related to these issues.

Devanshu Patel

VP of Legal, Compliance, and Information Security, North America

IGEL America Sales Corp

Patel manages legal issues for IGEL in North America and provides expertise for the IGEL Technology global information security program. IGEL provides a secure next generation edge operating system for cloud workspaces that enables remote work for the enterprise.

Scott J. Wenner

Partner

Schnader Harrison Segal & Lewis LLP

He is also co-chair of Schnader’s International Group and former chair of the firm’s Labor and Employment Practices Group. Wenner represents employers across industry lines and across borders on a broad range of labor and employment law matters, including trials and appeals, employment agreements and advice, and counsel on compliance and preventive strategies.