LABOR AND EMPLOYMENT ALERT | DECEMBER 2020

U.S. Supreme Court Hears Argument on When Employee Misuse of Work Computers May Constitute Criminal Conduct

By Scott J. Wenner and Mana Kinoshita

The United States Supreme Court recently heard oral argument in *Van Buren v. United States*, No. 19-783. The Court granted *certiorari* last term to resolve whether a person – in particular, an employee – who is authorized to access information on a computer for certain purposes violates the 1986 Computer Fraud and Abuse Act ("CFAA") if he/she accesses the same information for an improper use.

THE STATUTE AT ISSUE

The CFAA provides that a person engages in criminal conduct if he or she intentionally "accesses a computer without authorization or exceeds authorized access, and thereby obtains information." However, the meaning of the key term "exceeds authorized access" is left unclear. The statute 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.*" The italicized words create ambiguity over the scope of the prohibition: do they refer to information that a person is prohibited from accessing at all, or do they prohibit a person who is permitted to access certain information from using it for an unauthorized or improper purpose?

This ambiguity has led to a sharp division over the scope and meaning of these disputed terms among the five circuit courts that have ruled on this question. One group of courts has construed the statute to criminalize obtaining information by way of a computer only if the accessor is simply not entitled to access that information regardless of purpose or intended use. In contrast, the other group holds that the CFAA is criminally violated even if the actor has authority to access the information but uses it for an unauthorized purpose.

THE CASE BEFORE THE COURT

In this case, Van Buren, a police officer, was authorized to access by computer, for law-enforcement purposes, a state database of license plate records. When he instead accessed that database to run a license plate check in exchange for a bribe, he was charged with a criminal violation of the CFAA. In support, the Government maintained that while Van Buren had authority to access the state database to perform his duties, he exceeded that authority by using it for personal gain, thereby violating the CFAA.[1] The defense argued that Van Buren's authority to access the state database was sufficient to avoid criminal liability under the CFAA; that how he used the data he accessed was immaterial to the CFAA and should be addressed under other criminal laws. Both the trial and appellate courts ruled in the Government's favor.

THE ORAL ARGUMENT

At oral argument before the Supreme Court, counsel for Van Buren, Jeffrey Fisher, emphasized that the CFAA was enacted strictly as an anti-hacking statute intended to criminalize attempts by outsiders to break into computers and networks. He maintained that federal prosecutors were attempting to transform the CFAA into a "sweeping internet police mandate" that defines unauthorized computer use in such a broad

[1] He simultaneously was charged with a criminal violation of state law for taking an official act in exchange for a bribe.

way that it "would brand most Americans criminals on a daily basis." Such a broad reading of the CFAA could, he asserted, criminalize insubstantial and commonplace matters such as lying on a dating website, sharing the password to a streaming service, or using a work computer for personal activities in violation of an employer's policies.

Several of the Justices suggested that Fisher's examples, which they referred to as a "parade of horribles," seemed exaggerated and questioned whether any had in fact been prosecuted under the CFAA, much less resulted in convictions. Justice Alito, seeming to support a broader reading than Fisher's, expressed concern that "many government employees are given access to all sorts of highly personal information for use in performing their jobs. But, if they use that for personal purposes to make money, protect or carry out criminal activity, to harass people they don't like, they can do enormous damage."

Justices Thomas and Barrett both expressed concern over Van Buren's premise that access to information under the CFAA was either fully authorized or entirely unauthorized – analogized by Justice Barrett as "an on/off switch" – rather than the more nuanced approach of having limits on use. Fisher maintained that the statute was not intended to have a sliding scope-based component – that as written it "simply asks whether [or not the] person . . . was entitled to obtain the information." Seemingly in agreement with this latter point, Justice Breyer appeared swayed by the notable fact that when existing law was amended to create the CFAA, language specifying access exceeding the purposes for which authorization extends was deleted in delineating prohibited activity.

Justice Sotomayor questioned whether misuse of information could be prosecuted in other ways if the narrow reading of the CFAA advocated by Fisher were correct. Fisher confirmed that various other federal statues and state laws could address misuse of information accessed from a database – including the state law under which Van Buren also was prosecuted. Justices Gorsuch and Kavanaugh also expressed interest in this line of reasoning, suggesting that the CFAA did not have to be stretched to ensure that unauthorized use of information accessed by one with authority did not go unpunished.

The Government's lawyer, Deputy Solicitor General Eric Feigin, immediately took issue with Fisher's contention that the CFAA was concerned strictly with hacking – access to a network by outsiders. He maintained that Van Buren's misuse of access was the type of "serious breach[] of trust by insiders" that the statutory language intended to cover, and that access in this context "refers to some level of consideration and affirmative thought-out permission."

Feigin's argument, based on the precise text of the law, focused on the word "so" in the phrase "not entitled so to obtain or alter" in the definition of "exceeds authorized access." He argued that "so" does not refer merely to access to the computer as Fisher argued, but it refers instead to all aspects of the defendant's access, including whether he had authority to obtain the information in the manner he did or for the particular purpose that he used it. While Van Buren had authority to access the information, he did not have authority to use it as he did.

Implicitly conceding the breadth of potential liability created by his reading of the statute, Feigin offered several constructions of that law which limited prosecutorial discretion. Justice Sotomayor in particular voiced concerns that in so doing Feigin was offering definitions to narrow the statute that the statute does not contain, "to narrow what could otherwise be viewed as a very broad statute and dangerously vague." Homing in on a point made in Fisher's argument on Van Buren's behalf, Justice Gorsuch called the case "the latest … in a rather long line of cases in recent years in which the government has consistently sought to expand federal criminal jurisdiction in pretty significantly contestable ways that this Court has rejected."

ANALYSIS

It is always risky to "read the tea leaves" after observing the Justices respond to advocates. However, most Justices appeared dubious of the Government's position in this case, both because the language of the CFAA does not seem to support the wide breadth it advocated and because of the discretion the Govern-

ment's view gives to prosecutors at a time when the Court has not looked kindly on similar grants of broad discretion. In that respect Justice Gorsuch's observation of the recent trend at the Court to limit federal criminal jurisdiction could tip the Court's hand.

The apparent skepticism of many of the Justices toward federal criminalization of employee misconduct may foretell a need for a realistic attentiveness that employers should have in creating and enforcing workplace policies governing employee access to computers. Businesses may benefit by taking this opportunity to consider reviewing their policies, providing training for workers and supervisors, and clarifying the rules to avoid misunderstandings and to allow for corrective action when warranted.

Stay tuned, as a decision will be published by July of next year. ◆

For more information about Schnader's Labor and Employment Practices Group or Criminal Defense Practice Group, or to speak with a member of the firm, please contact:

Scott J. Wenner, Partner
Chair, International Group
212-973-8115
swenner@schnader.com

Mana Kinoshita
Associate
212-973-8110
mkinoshita@schnader.com

Jo Bennett
Co-Chair, Labor and Employment Practices Group
215-751-2134
jbennett@schnader.com

Michael J. Wietrzychowski
Co-Chair, Labor and Employment Practices Group
856-482-5723
mwietrzychowski@schnader.com

Laurel Gift
Co-Chair, Criminal Defense Practice Group
412-577-5115
lgift@schnader.com

Randall P. Hsia
Co-Chair, Criminal Defense Practice Group
215-751-2462
rhsia@schnader.com