Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

What To Watch As High Court Takes On Computer Crime Law

By **Ben Kochman**

Law360 (November 25, 2020, 7:12 PM EST) -- A computer crime law whose scope has been hotly debated since it was passed in 1984 will have its moment in the limelight Monday, when the U.S. Supreme Court considers whether a Georgia police officer violated the law by abusing his access to an online government database.

The high court's ruling in Van Buren v. United States is expected to resolve a circuit split over what it means for someone to "exceed authorized access" to a system under the Computer Fraud and Abuse Act. The decision will have an immediate impact on how both prosecutors and businesses apply the statute — which allows for both criminal charges and civil remedies — to scenarios where insiders are accused of misusing computer networks.

The case will also test how newly seated Justice Amy Coney Barrett applies her self-avowed textualism to a statute critics have called dangerously vague, as well as challenge the high court to consider what Congress intended to accomplish with a computer crime bill passed before the dawn of the modern internet.

Here's a breakdown of three key questions that may arise during Monday's arguments and could influence where the court ultimately comes down.

How Seriously Will SCOTUS Take Alarming Hypotheticals?

The case centers on Nathan Van Buren, a former police sergeant in Cumming, Georgia, who was convicted of breaching the CFAA and on federal corruption charges after accepting $6,000 from an acquaintance to check a law enforcement database to determine whether someone was an undercover police officer.

Van Buren accepted the cash from a local man named Andrew Albo who, while working with the FBI as part of a sting operation, told Van Buren he needed to know whether a woman he had met at a strip club was a police officer before deciding whether to pursue her further, according to court records.

Van Buren's attorneys have argued the Eleventh Circuit's October 2019 decision to uphold the conviction on the basis the officer "exceeded" his "authorized access" defined the law in terms that could criminalize seemingly innocuous behavior — like an employee violating an employer's terms of service by setting up an NCAA basketball "March Madness" bracket on a work computer, or a law

student using a database meant for "educational use" to research housing laws in a dispute with their landlord.

The federal government has countered there's no evidence to date of prosecutors or businesses bringing criminal charges or civil suits based on the scenarios brought up by Van Buren, who will be represented at arguments by Jeffrey L. Fisher of Stanford Law School's Supreme Court Litigation Clinic.

But Eric J. Feigin, the U.S. Department of Justice deputy solicitor general expected to represent the government, could face questions Monday about whether there should be checks in place on prosecutors' ability to bring claims for "exceeding" one's "authorized access" to networks, attorneys say.

"This is going to be one of those great line-drawing cases," said Mark Srere, co-leader of the investigations, financial regulation and white-collar practice group at Bryan Cave Leighton Paisner LLP. "The question will be, can you draw a line within the words of the statute that can prevent Van Buren's conduct, but also prevent prosecutors from using the CFAA whenever they want to?"

Should the High Court Apply the Rule of Lenity?

Van Buren's attorneys have urged the high court to apply the rule of lenity — a principle of criminal law that requires courts to apply ambiguous laws favorably to defendants — in the ex-officer's case.

Appeals courts have reached different conclusions on whether the CFAA's definition of "exceeds authorized access" is clear. In December 2015, for example, the Second Circuit in United States v. Valle found the clause to be ambiguous and rejected the federal government's bid to hold a New York City police officer criminally liable for allegedly searching government databases for information on a former high school classmate he had discussed kidnapping as part of a sexual fantasy he had talked about in online chatrooms.

"Where, as here, ordinary tools of legislative construction fail to establish that the government's position is unambiguously correct, we are required by the rule of lenity to adopt the interpretation that favors the defendant," the appeals panel wrote.

The Eleventh Circuit, on the other hand, upheld Van Buren's conviction based on the standard set in its 2010 ruling in U.S. v. Rodriguez, in which it found a former Social Security Administration employee had breached the CFAA by accessing information on government databases for non-business reasons. Van Buren had admitted to investigators he "knew it was 'wrong' to run the tag search," the appeals court added.

In the past, the high court has been critical of criminal laws that it is perceives to be vague, and Monday's case could come down to whether the justices agree with the government that the statute "unambiguously" covers Van Buren's conduct, attorneys say.

"The court has expressed concern with broad criminal statutes and the discretion that that places in prosecutors to have good judgment," said William Ridgway, a partner in the privacy and cybersecurity practice at Skadden Arps Slate Meagher & Flom LLP.

"The government has tried to save those line-drawing issues for a later time, but it could face tough questions about whether this statute would then apply to activity that everyone agrees should not be criminal," Ridgway added.

How Might 'Textualism' Apply Here?

In its ruling in the Valle case, the Second Circuit cited the late Justice Antonin Scalia, who wrote in a 2005 decision in United States v. Santos that "when interpreting a criminal statute, we do not play the part of a mind reader."

When it was passed in 1984, the CFAA did not define the term "exceeds authorized access." But a 1986 amendment to the law, written while the internet was still in its infancy, states that it covers people who "access a computer with authorization and use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."

The government has argued the 1986 amendment clearly covers the Georgia officer's search — or, in other words, that no mind-reading is needed in this case — because he obtained information that he was "not entitled so to obtain" by using his official credentials to search the database in return for cash.

The case presents a challenge for the high court justices who pay particularly close attention to the plain text of statutes rather than lawmakers' intent when passing them — including, potentially, Justice Barrett, who has described herself as a textualist in the vein of Justice Scalia, whom she clerked for in the late 1990s.

Barrett has indicated a clear preference for interpreting laws based on their strict textual meaning and relying on the federal government's own interpretation of laws when the text is unclear, legal experts have said.

"The court will have to wrestle with the plain meaning of the statute when it defines exceeding authorized access," said Mark Krotoski, a former federal cybercrime prosecutor and co-head of the privacy and cybersecurity practice at Morgan Lewis & Bockius LLP. "And if legislative history comes up, the question will be: Was the 1986 amendment that gave us those terms a substantive change from the 1984 language?"

The case is Van Buren v. United States, case number 19-783, in the U.S. Supreme Court.

--Additional reporting by Allison Grande and Suzanne Monyak. Editing by Alanna Weissman and Philip Shea.