STINSON

News & Insights

Justices Clarify Scope of Anti-Hacking Law

Alert
06.10.2021

By David Barnard, Scott Eidson, Kevin Conneely, Jason Conway, Steve Cosentino and Nicci Warr

Last week, in a 6-3 opinion delivered by Justice Amy Coney Barrett, the U.S. Supreme Court settled a long-running question about the scope of the Computer Fraud and Abuse Act of 1986 (CFAA). In *Van Buren v. United States*, the Court determined that the CFAA provision that prohibits exceeding authorized access of a computer must be analyzed under a "gates-up-or-down" approach where the defendant's ability to access the information is the determinative factor. The holding limits the usefulness of the CFAA for civil claims where a potential wrongdoer misuses information but doesn't necessarily go beyond their access rights.

The Court's Opinion

The CFAA—popularly known as the "anti-hacking" law—makes it a crime for any person to knowingly access a computer without authorization or exceed the person's authorized access to obtain information from a protected computer. 18 U.S.C. § 1030(a)(2). The key issue in *Van Buren* was whether using an accessible computer system for an "improper purpose" is within the scope of the CFAA's ban on exceeding authorized access. In exchange for money, a police officer ran a license-plate search in a law enforcement database to which he had access. The Court recognized that the conduct clearly violated the police department's policy (which permitted access to the database only for law enforcement purposes), but held that the conduct did not violate the CFAA.

The Court explained that the CFAA is "ill-fitted to remediating 'misuse' of sensitive information that employees permissibly access using their computers." Instead, the CFAA applies when a person commits the "act of entering a part of the system to which a computer user lacks access privileges." (emphasis added). In endorsing this "gates-up-or-down" approach, the Court made clear that the primary question under CFAA is whether the defendant "can or cannot access a computer system" or "can or cannot access certain areas within the system." The Court provided an example to illustrate its holding: "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 that 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 that information."

The Court rejected the government's construction, which sought a broad reading of the act to cover obtaining authorized information in a "manner or circumstances" that were prohibited. According to the Court, the "government's interpretation would attach criminal penalties to a breathtaking amount of commonplace computer activity," including every violation of a computer-use policy. Instead, the Court opted for a narrow interpretation implementing an "access as entry" approach, where the CFAA's "without authorization" clause protects computer systems from outside hackers while the "exceeds authorized access" clause protects such systems from inside hackers.

While the Court answered an important question, it left questions for the lower courts to debate. In footnote eight, the Court indicated that it need not address whether the "gates-up-or-down" inquiry turns only on code-based limitations or also applies to contractual or policy limits. Lower courts will have to decide whether the restrictions on access under the CFAA are required to be technological—e.g., a password does not permit access to certain files—or whether non-technological limits can have the same effect. In the meantime, in light of the Court's holding in *Van Buren* and the unanswered issue in footnote eight, it would be prudent for those who want to provide the maximum legal protection for their computer systems to evaluate whether additional technological barriers are appropriate.

What This Means for Your Business

The CFAA has been frequently used by civil litigants against employees, former employees, contractors and other related personnel who exceed the scope of their authority to misappropriate information. This decision narrows the reach of the CFAA for such claims because misuse must have an element of exceeding access. One way to address this issue going forward is to set more specific parameters around access. In particular, access to sensitive information should be limited—by policy, contract *and technology*—to only those who need the information to perform their functions.

CONTACTS

David R. Barnard

Kevin D. Conneely

Jason H. Conway

Stephen J. Cosentino, CIPP

B. Scott Eidson

J. Nicci Warr

Justices Clarify Scope of Anti-Hacking Law

RELATED CAPABILITIES

Intellectual Property & Technology