MBHB *snippets* Alert **June 3, 2021**

Supreme Court Prohibits Use of Federal "Anti-Hacking" Law Against Those Who Use Otherwise Authorized Access for Improper Purpose

By Joshua R. Rich

In *Van Buren v. United States*, the Supreme Court faced the difficult task of determining whether the opaquely-written Computer Fraud and Abuse Act ("CFAA") would apply to situations in which a person who was authorized to access information for work purposes had accessed that information for improper reasons. In one of Justice Barrett's first opinions, the six-justice majority found that it would not. Justice Thomas, joined by Chief Justice Roberts and Justice Alito, dissented because he believed it should.

The *Van Buren* case began when a financially-troubled sergeant in the Cumming, Georgia police department befriended a known criminal. Sergeant Van Buren decided to leverage that friendship by asking for a loan (falsely claiming it was to pay off medical bills). But his friend wasn't all that friendly – he went to the county sheriff's office and reported that Sergeant Van Buren was shaking him down. The FBI got involved and ultimately created a sting operation in which Sergeant Van Buren would be asked to access Federal and State crime databases to provide information about a woman the friend had met at a strip club. Sergeant Van Buren agreed and ran the woman's license plate information in the databases, then texted his friend that he had the information. When the FBI and Georgia Bureau of Investigation showed up to arrest him, Sergeant Van Buren admitted what he had done, and that he knew it was wrong to obtain the information for non-police purposes. He was then charged with violation of the CFAA and honest services fraud and convicted on both counts.[1]

[1] Sergeant Van Buren's conviction on the honest services fraud count was reversed upon appeal to the U.S. Court of Appeals based on a faulty jury instruction, and was not before the Supreme Court. *See United States v. Van Buren*, 940 F.3d 1192 (11th Cir. 2019).

The CFAA, codified at 18 USC §1030, was enacted in 1986 as a response to the newly-seen threat of hacking of protected computers. Written long before the explosion of the internet, it was written to protect government, financial institution, and other "protected computers." Most importantly, it established that a person commits a crime when he or she "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer." In that context, "the term 'exceeds authorized access' means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." And the term "protected computer" includes any computer "which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States."

The first part of the prohibited offense – intentionally accessing a computer without authorization – was written to cover "outside hackers" and did not apply here. But the question before the Court was whether a person "exceeds authorized access" only when they delve into parts of the computer for which they do not have permission (acting as an "internal hacker") or also when they access otherwise authorized information for an improper, prohibited purpose.

The majority started with the text of the CFAA, and believed that the act was structured so that the two parts of the offense would be parallel in a binary "gates-up-or-down inquiry." That is, because the only question for the first part was whether the accesser had authorization or not, the second part should be limited to the question of whether the accesser had authorization to access that information in any circumstance or not. In that sense, Justice Barrett used a physical analogy for the scope of authorization, describing the prohibition as relating to "particular areas of the computer – such as files, folders, or databases – to which their computer access does not extend." In doing so, she rejected the government's assertion that it would read the word "so" (in the phrase "entitled so to obtain or alter") from the statutory definition of "exceeds authorized access." She indicated that the word "so" could be understood to distinguish the situation where an individual is not entitled to see the same information in non-computer-based means.

The majority also relied on the history of the CFAA's enactment and a parade of horrible possible applications of the law to reject the government reading that it covers access for an improper purpose. The first version of the law that the CFAA replaced explicitly considered the purpose of access and the CFAA did not. However, the legislative history (which neither the majority nor the dissent mentions) expressly stated that the change was not intended to be substantive. In addition, the majority noted that the CFAA as read by the government could be understood to encompass everyday violations of terms of service, such as use of a work computer for personal reasons or embellishing online-dating profiles or using a pseudonym on Facebook. For all of these reasons, the majority held that exceeding authorized access related to computer structures, not terms (or purposes) of access.

Justice Thomas, writing in dissent, disagreed primarily based on settled property law considerations. He saw nothing more definitive about the majority's reading – any more of a "gates-up-or-down" approach – than if exceeding authorized access considered what the circumstances of authorization were. In doing so, he analogized to property law, which generally protects against unlawful entry and unlawful use of property after entry. And he saw nothing more reasonable in decriminalizing access in all circumstances if there is a single exception than prohibiting such access if an authority had explicitly said so. For example, the majority's reading decriminalizes an IT administrator's actions in deleting every file on a

computer minutes before resigning. Thus, Justice Thomas noted, the majority's reading of the CFAA constitutes a substantial narrowing of the law.

In the end, the Supreme Court's decision may be a spur to action for Congress to rewrite the CFAA more clearly. The majority's interpretation should relieve any concerns that a person has committed a crime merely by sending a personal e-mail or shopping online at work, but it comes at the cost of protections for employers' against workers malicious or dishonest conduct with work data – the CFAA previously allowed employers to pursue employees who downloaded data improperly before the data could get out. And in the context of public integrity, following on the heels of the Court's prior narrowing of honest services fraud law, the *Van Buren* case severely limits the ability of the Federal government to pursue public officials for abuse of their position. So the best hope is that the statute is redrafted, but in the meantime the meaning of "computer fraud" has been greatly narrowed.

Decided: June 3, 2021.

The opinion can be found at https://www.supremecourt.gov/opinions/20pdf/19-783_k53l.pdf

Joshua R. Rich, an intellectual property trial lawyer and a partner with McDonnell Boehnen Hulbert & Berghoff LLP, serves as MBHB's General Counsel and Chair of MBHB's Trade Secrets Practice Group. rich@mbhb.com