Published on *The National Law Review* https://natlawreview.com

Supreme Court Update: Borden v. United States (No. 19-5410), Van Buren v. United States (No. 19-783), Sanchez v. Mayorkas (No. 20-315)

Article By:

Tadhg A.J. Dooley

David Roth

This morning, the Court continued its march toward the end of the OT2020 term, issuing its decision in Borden v. United States (No. 19-5410). There, a five-justice majority held that a criminal offense with a mens rea of recklessness does not satisfy the Armed Career Criminal Act's elements clause. That leaves 20 outstanding cases (a few less if you count consolidations) before the Court's term wraps up at the end of June. We'll talk more about *Borden* in a future issue, but for now we have summaries of last Thursday's decision in ***Van Buren v. United States* (No. 19-783)** and Monday's ***Sanchez v. Mayorkas* (No. 20-315)**.

Van Buren v. United States (No. 19-783) marks the Court's first significant decision on the Computer Fraud and Abuse Act of 1986 ("CFAA"). Among other things, CFAA's "exceeds authorized access" clause criminalizes accessing a computer *with* authorization but then using that access "to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter." In recent years, lower courts have disagreed about whether people violate this provision by accessing information they are allowed to see for one purpose (such as in furtherance of their job responsibilities) for some improper reason (such as for personal gain). An unusual combination of six Justices concluded that they do not.

Nathan Van Buren is a former police sergeant in Georgia. Suspecting he may be crooked, the local FBI asked one of Van Buren's friends—himself no stranger to the law—to pay Van Buren $5000 to search law enforcement databases for information about a particular license plate, which the friend told Van Buren he suspected belonged to an undercover police officer. Van Buren took the bait and used his access to the databases to search for information about the plate. The plate, of course, was a phony, and when he relayed information about it to his friend, he was arrested and charged with violating the CFAA under the "exceeds authorized access" clause because police department policy prohibited officers like Van Buren from accessing this database for personal use. He appealed his ultimate conviction, arguing that CFAA's prohibition on exceeding authorized access applies only to those who obtain information outside their permissible access and not those, like Van Buren, who simply *misuse* their access. While many courts of appeals have read the statute Van Buren's way,

the Eleventh Circuit took a broader view and affirmed. The Court granted cert to resolve this conflict.

A six-justice majority consisting of the Court's three liberals (Breyer, Kagan, and Sotomayor) and three of its conservatives (Barrett, Gorsuch, and Kavanaugh) reversed. Justice Barrett's majority opinion began with CFAA's text. Its "exceeds authorized access" provision criminalizes accessing a computer "with authorization . . . to obtain information in the computer that the accessor is not *entitled so* to obtain." 18 U.S.C. § 1030(e)(6) (emphasis added). All agreed that Van Buren accessed the database "with authorization." All agreed he "obtained information" from it. But was he "entitled so" to obtain that information?

Van Buren argued he was. "Entitled so" looks back to "with authorization," meaning that the statute prohibits accessing a computer one is authorized to use to reach information one is notauthorized to get. Thus if a user is authorized to access Folder X but not Folder Y, the user violates CFAA by accessing Folder Y. The government, by contrast, argued "entitled so" refers to the *manner or circumstances* in which one obtains the information, meaning that a person violates the statute if they access information they are allowed to access for one purpose for some other purpose. Thus (continuing the hypothetical) a person violates CFAA by accessing Folder X for a purpose not allowed by some restriction on their access (like their employer's terms of use). But in the majority's view, this reading of "so" went too far, because it did not refer to anything even mentioned in the statute but instead any circumstance-based limit anywhere, such as in some other statute or even a private contract.

After brushing aside several textual counter-arguments (which we won't try to summarize here), the majority found further support for its interpretation in the rest of the statute. While Van Buren was charged under CFAA's "exceeds authorized access" clause, an adjacent provision of the statute criminalizes obtaining information "without authorization." Under Van Buren's approach, there's harmony between these two clauses: One protects against accessing a computer without any permission at all (e.g., outside hackers), while the second protects against exceeding authorized access to reach off-limits information (sometimes called inside hacking). Both provisions, then, use a "gates-up-or-down" approach, criminalizing obtaining information from a computer one is not allowed to reach. But on the government's approach, the exceeds authorized access clause bears little resemblance to the "without authorization" clause because it turns not on whether one is permitted to access the information but instead the reasons and circumstances in which one does so.

Finally, the Court emphasized just how broad the government's theory was. Nearly every employer has computer-use policies specifying that their computers and electronic devices should be used only for business purposes. On the government's interpretation, then, someone who sends a personal email or reads the news using their work computer (a group that definitely includes **you**) is seemingly a criminal. But it doesn't stop there, as websites, services, and databases often provide information only upon the user's agreement to follow certain terms of service. If the government were right, then everyone who violates any term of service has seemingly violated CFAA. If Congress really intended that sort of result, one would've expected it to be a bit more clear about it. Since Van Buren indisputably had authorization to access the law-enforcement database at issue, the Court vacated his conviction.

Justice Thomas, joined by the Chief and Justice Alito, dissented. They agreed with the majority's (and Van Buren's) interpretation of the word "so." But in their view, the word to focus on was "entitled." It ordinarily asks whether someone has a "right" to do something. And while Van Buren might have had a right to access information on the computer for law-enforcement purposes, ordinary people would say he had no right to search the database for personal gain. The dissent further

supported its interpretation by looking to basic principles of property law, which recognize that one's right to use property for a specific purpose does not allow one to use it for other purposes: one's entitlement to use property is limited by the terms of that use. The dissent also briefly responded to the majority's concerns about overbreadth, noting that CFAA has strict mens rea requirements and is limited to obtaining or altering information *in* the computer (something that would not ordinarily be satisfied by using your company laptop to check the news). They would have affirmed Van Buren's conviction.

Our second case for today is ***Sanchez v. Mayorkas* (No. 20-315)**. It asked whether those who enter the United States illegally but subsequently are granted Temporary Protected Status ("TPS") can become lawful permanent residents ("LPR") of the United States. Writing for a unanimous Court, Justice Kagan held that they cannot.

Section 1255 of the immigration laws specifies when a nonimmigrant (that is, a foreign national lawfully present in the United States) can become an LPR. All of Section 1255's conditions depend on "admission" into the United States, which in turn is defined as "lawful entry" here. A separate provision of the immigration laws establishes the TPS program. It provides humanitarian relief to foreign nationals from specific countries by allowing nationals of those countries already present in the United States to obtain TPS status and remain here so long as the TPS designation remains in place.

Jose Santos Sanchez is a citizen of El Salvador. He entered the United States unlawfully in 1997 and has remained ever since. In 2001, the United States designated El Salvador under the TPS program, and Sanchez obtained TPS status. In 2014, he applied for LPR status, but the U.S. Citizenship and Immigration Service denied his application, reasoning that he was ineligible for LPR because he had not been lawfully admitted into the United States. That was so even though after his unlawful entry, he obtained TPS status. The issue ultimately reached the courts, and the Supreme Court granted cert to resolve a circuit split about whether a TPS recipient who entered the United States unlawfully can become an LPR.

Justice Kagan quickly concluded that they cannot. By its plain terms, Section 1255 requires LPR applicants to have entered the country "lawfully" and with an "inspection," that is, to have been admitted here. Sanchez indisputably had never done that. And nothing in the TPS program changed that result. While those like Sanchez with TPS status are treated as having nonimmigrant status (and so are eligible to receive LPR under Section 1255), nothing in the TPS statutes address Section 1255's admission requirement. The concepts of admission and lawful status have long been treated as distinct, and the TPS statutes didn't change that. Thus the Court agreed Sanchez was not eligible for LPR status because he had never properly been admitted.

National Law Review, Volume XI, Number 161