***Van Buren v. United States*, No. 19-783**

Introduction: Today, the Supreme Court held in a 6-3 decision that a police officer who accessed a law-enforcement database for an improper purpose did not violate the Computer Fraud and Abuse Act (CFAA), because the officer was authorized to access that database in the course of his official duties.

Background: The CFAA makes it illegal to "intentionally access[] a computer without authorization or exceed[] authorized access." 18 U.S.C. § 1030(a)(2). In recent years, there has been significant debate in the courts of appeals about what it means to "exceed[] authorized access." For example, Judge Kozinski said in an en banc Ninth Circuit opinion that if the CFAA prohibits someone who is allowed to use a computer from using it for unauthorized purposes, then "minor dalliances" under workplace computer-use policies – like using Google Chat, watching sports highlights on ESPN.com, and playing Sudoku – could become federal crimes.

In this case, a police officer was allowed to access a law-enforcement database for his job. But he instead used the database for a personal purpose (to obtain license-plate information about a woman whom a friend had met at a strip club). He was convicted under the CFAA for exceeding his authorized access. The Eleventh Circuit upheld the conviction on the ground that the officer "exceeded his authorized access" to the database because he used the database for an "inappropriate reason."

Issue: Whether a person who is authorized to access information on a computer for one purpose "exceeds [his] authorized access" under Section 1030(a)(2) of the CFAA when he accesses information for an unauthorized purpose.

Court's Holding: In an opinion written by Justice Barrett, the Supreme Court held that the police officer had not "exceed[ed] his authorized access" because he was allowed to access the database. The Court explained that the phrase "exceeds authorized access" refers to information that a person is not allowed to obtain at all. The Court found support for that reading in the structure of Section 1030(a)(2), which takes a "gates-up-or-down" approach to whether a person is authorized to access a computer system or certain areas within that system. The Court also concluded that the government's interpretation would attach civil and criminal liability to a "breathtaking amount" of commonplace computer activity, such as violating a company's computer-use policy by using a device for non-business purposes.

Justice Thomas authored a dissent, in which Chief Justice Roberts and Justice Alito joined, reasoning that the officer exceeded authorized access to the database by using his access for an unauthorized purpose.

Read the opinion here.