OpTac International News Bulletin:

Supreme Court case of Van Buren v. United States

OpTac International News Bulletins present topics of interest for the law enforcement and military communities. This edition presents excerpts from the Supreme Court case of Van Buren v. United States, which was decided on June 3, 2021.

Supreme Court Decision - "Opinion of the Court"

"JUSTICE BARRETT delivered the opinion of the Court. Nathan Van Buren, a former police sergeant, ran a license-plate search in a law enforcement computer database in exchange for money. Van Buren's conduct plainly flouted his department's policy, which authorized him to obtain database information only for law enforcement purposes. We must decide whether Van Buren also violated the Computer Fraud and Abuse Act of 1986 (CFAA), which makes it illegal '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.' He did not. This provision covers those who obtain information from particular areas in the computer—such as files, folders, or databases—to which their computer access does not extend. It does not cover those who, like Van Buren, have improper motives for obtaining information that is otherwise available to them" (p. 1).

Facts of the Case - "Syllabus"

"Former Georgia police sergeant Nathan Van Buren used his patrol-car computer to access a law enforcement database to retrieve information about a particular license plate number in exchange for money. Although Van Buren used his own, valid credentials to perform the search, his conduct violated a department policy against obtaining database information for non-law-enforcement purposes. Unbeknownst to Van Buren, his actions were part of a Federal Bureau of Investigation sting operation. Van Buren was charged with a felony violation of the Computer Fraud and Abuse Act of 1986 (CFAA), which subjects to criminal liability anyone who 'intentionally accesses a computer without authorization or exceeds authorized access.' 18 U. S. C. §1030(a)(2). The term 'exceeds authorized access' is defined to mean 'to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter.' §1030(e)(6). A jury convicted Van Buren, and the District Court sentenced him to 18 months in prison. Van Buren appealed to the Eleventh Circuit, arguing that the 'exceeds authorized access' clause applies only to those who obtain information to which their computer access does not extend, not to those who misuse access that they otherwise have. Consistent with Eleventh Circuit precedent, the panel held that Van Buren had violated the CFAA" (p. 1).

"The Government's interpretation of the 'exceeds authorized access' clause would attach criminal penalties to a breathtaking amount of commonplace computer activity. For instance, employers commonly state that computers and electronic devices can be used only for business purposes. On the Government's reading, an employee who sends a personal email or reads the news using a work computer has violated the CFAA. The Government speculates that other provisions might limit

its prosecutorial power, but its charging practice and policy indicate otherwise. The Government’s approach would also inject arbitrariness into the assessment of criminal liability, because whether conduct like Van Buren’s violated the CFAA would depend on how an employer phrased the policy violated (as a 'use' restriction or an 'access' restriction). Pp. 17–20. 940 F. 3d 1192, reversed and remanded" (p. 4).

Conclusion

While the Supreme Court reversed and remanded Van Buren's felony conviction on the grounds that it "would attach criminal penalties to a breathtaking amount of commonplace computer activities," great care must be taken by law enforcement officers not to abuse their power in accessing and subsequently disseminating privileged information.