CARLTON FIELDS

U.S. Supreme Court to Weigh in on Computer Fraud and Abuse Act (CFAA) for the First Time

June 12, 2020

For the first time, the U.S. Supreme Court has taken up a case involving the federal Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030. In *United States v. Van Buren*, the court will address the question whether an individual who has the authority to access a computer violated the CFAA by using that access for an inappropriate or unauthorized purpose.

The CFAA, enacted in 1986 as an amendment to the Counterfeit Access Device and Computer Fraud and Abuse Act, provides criminal penalties and civil remedies for intrusions into "protected computers." "Protected computers" are broadly defined to include computers used by or for financial institutions and the U.S. government or any computer that is used in or affects interstate or foreign commerce. 18 U.S.C. § 1030(e)(2). While initially intended as a tool to combat the growing threat of "the technologically sophisticated criminal who breaks into computerized data files," i.e., hackers, subsequent amendments expanded its scope. A 1996 amendment extended the definition of a protected computer to include non-governmental computers. A 2008 amendment made it a violation of the CFAA when an individual "intentionally accesses a computer without authorization or exceeds authorized access." 18 U.S.C. § 1030(a)(2)(C). To exceed authorized access under the CFAA is "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." 18 U.S.C. § 1030(e)(6).

Although referred to at times as the "federal anti-hacking" law, the CFAA has been amended to include actions that extend beyond traditional computer hacking. As the volume and value of information stored and accessible on computers in 2020 is exponentially greater than in 1986, statutes protecting electronically stored data have changed. Today, the CFAA covers the closely guarded electronically stored information of companies in interstate commerce, such as trade secrets, intellectual property, financial and banking information, personal information of employees

or customers, and other sensitive or valuable information, against incursions from both inside and outside the company.

However, the CFAA has split the federal circuit courts on whether a user who is authorized to access both the computer and the electronically stored information, such as an employee, contractor, or agent, violates the CFAA if he or she is accessing and using the information for an improper purpose (the First, Fifth, Seventh, and Eleventh Circuits find that it is a violation; the Second, Fourth, and Ninth Circuits disagree). Now, the question is before the U.S. Supreme Court in the case of a Georgia police officer who was bribed to search a license plate number in the Georgia Crime Information Center database.

In *Van Buren*, FBI informant Andrew Albo paid officer Nathan Van Buren to run a license plate search. Albo allegedly told Van Buren that the plate number belonged to a woman he liked but that given his prior run-ins with the law, he wanted to make sure she wasn't an undercover police officer. Van Buren agreed and ran the search for Albo in exchange for $6,000. The FBI arrested Van Buren the next day, and he was charged with a felony violation of the CFAA.

Van Buren argued that he did not violate the CFAA because he was authorized to access both the computer database and the information he obtained, regardless of whether his access was for an inappropriate or unauthorized purpose. Van Buren's argument was rejected, and he was convicted under the CFAA and sentenced to 18 months in prison. The Eleventh Circuit upheld the conviction. The Supreme Court has now agreed to opine on the question whether a person who is authorized to access information on a computer for certain purposes violates the CFAA if he or she accesses the same information for an improper purpose. This is an important case to watch for its implications on cybersecurity.

Authored By

Amanda Romfh Jesteadt

Stacey K. Sutton

Related Practices

Telecommunications
Technology
Cybersecurity and Privacy

Related Industries

Telecommunications
Technology