WINSTON & STRAWN LLP

BLOG

SCOTUS to Consider the Scope of Federal Anti-Hacking and Computer Fraud Law

MAY 8, 2020

The Supreme Court recently agreed to decide whether it is a federal crime for someone **authorized** to access information on a computer system to take or use that information for an **unauthorized** purpose.

A former Georgia police officer, Nathan Van Buren, is the subject of the case: he was convicted of violating the Computer Fraud and Abuse Act (CFAA) after selling license plate information to an acquaintance in exchange for $6,000. Van Buren was able to obtain the license plate information by using his law enforcement credentials to search a police database. The CFAA makes it a federal crime to obtain information via unauthorized computer access, or through a level of access that exceeds one's authorization. On appeal, the Eleventh Circuit upheld his conviction, rejecting Van Buren's argument that he could not have violated the CFAA because he had permission to access the database, even if his use of the information was unauthorized.

There is a federal circuit split regarding the applicability of the CFAA: The Second, Fourth, and Ninth Circuits have held that a violation of the CFAA occurs only when an entirely unauthorized person (like a hacker) accesses information on a computer that he or she is prohibited from accessing. Under this analysis, Van Buren could not have been prosecuted under the CFAA for the license plate search. However, the First, Fifth, Seventh, and Eleventh Circuits apply the statute more broadly, sweeping in authorized users that are using information for unauthorized purposes. Van Buren, in his appeal to the Supreme Court, argued that, if the Eleventh Circuit (and the other likeminded Circuits) are correct, any "trivial breach" of conditions imposed by an employer, or a website's terms of service could result in a federal crime. Van Buren even suggests that one could be found in violation of the CFAA for "checking sports scores at work" or "inflating one's height on a dating website."

Though SCOTUS will not weigh in until at least October 2020, the implications of the Court's decision are significant. Not only will the Supreme Court's decision guide prosecution efforts by law enforcement but, because the CFAA allows for a private right of action, the decision could encourage more private litigants, like employers, to pursue relief for the misuse of sensitive data and information. In particular, plaintiffs pursuing trade secret claims stand to gain a powerful tool, should SCOTUS adopt the broad reading of the CFAA. Because many trade secret misappropriation claims occur in circumstances where an employee initially accesses private information via authorized means, the CFAA could offer a different standard than is otherwise available to plaintiffs. For example, though the federal Defend Trade Secrets Act (DTSA) and other trade secrets laws can operate to safeguard the same type of information, these claims can be difficult because they require a plaintiff prove that the information

legally qualifies as a “trade secret,” including proof that the plaintiff took reasonable measures to protect the information, while the CFAA does not require a similar showing.

TIP: Should the Supreme Court adopt the Eleventh Circuit’s broad view of CFAA’s scope, the CFAA could be a powerful tool to address improper use of confidential information without having to meet the requirements of trade secret statutes.
2 Min Read

Author

Steven Grimes

Related Locations

Chicago

Related Topics

Online Privacy | Workplace Privacy | Data Breach | Trade Secrets

Related Capabilities

Privacy & Data Security | Trade Secrets, Non Competes & Restrictive Covenants | Litigation/Trials | Compliance Programs

Related Regions

North America

Related Professionals

Steven Grimes