BARNES & THORNBURG LLP

# Scope Of DOJ's Enforcement Of The Computer Fraud And Abuse Act After Van Buren

June 30, 2021 | The GEE Blog,Department Of Justice

**Jeanine Kerridge**
Partner

The Supreme Court's recent clarification of a circuit split on what counts as "unauthorized access" of information on a computer under the Computer Fraud and Abuse Act (CFAA) clearly has curtailed the DOJ's enforcement powers, but questions remain.

Justice Barrett, delivering the majority opinion in *Van Buren v. United States*, held unambiguously that criminal violation of the CFAA is not triggered when a user – even one with improper motives – accesses information that is otherwise available to that user. Rather, the CFAA criminal prohibition "covers those who obtain information from particular areas in the computer – such as files, folders, or databases – in which their computer access does not extend."

Petitioner Van Buren was not a sympathetic defendant, which only underscores the Supreme Court's majority opinion that the DOJ's prosecution extended beyond the language of the CFAA. Van Buren, at the time a police sergeant in Georgia, made the acquaintance of Andrew Albo, who turned FBI informant when Van Buren asked him for a personal loan. Working at the behest of the FBI, Albo asked Van Buren to run the license plate of a woman he claimed to have met at a local strip club to make sure the woman was not an undercover officer. Albo offered to pay Van Buren $5,000 for the information.

Van Buren ran the search using the law enforcement databases to which he

## RELATED PRACTICE AREAS

Data Security and Privacy
Internet and Technology

## RELATED TOPICS

Computer Fraud and Abuse Act

had otherwise legitimate access. The DOJ prosecuted Van Buren on the theory that his conduct violated the “exceeds authorized access” clause of the CFAA because Van Buren had not performed the searches for a law enforcement purpose.

The opinion turned on the interpretation of the statute’s definition of “exceeds authorized access” as “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 to so obtain or alter.” The majority determined that adopting the DOJ’s broader interpretation that a user violates the CFAA when using a computer in a way prohibited by their job or policy could criminalize millions of Americans who use their work computers to check the internet for personal reasons or who violate the terms and conditions of a website.

The majority opinion therefore made clear that it is not illegal under the CFAA for a user to access information he or she otherwise is authorized to access. The opinion explicitly left open, however, the exact scope of what constitutes “authorization” – whether it applies only to technical code-based restrictions, or whether it also looks to restrictions in contracts or policies – although the opinion did appear to favor a bright-line technological restriction approach.

As the law continues to develop on the scope of not only DOJ enforcement but also private rights of action under the CFAA, entities looking to restrict access to confidential and other information should therefore review not only their policies but also technical access to materials they wish to protect.