

CEP Magazine – September 2021

Computer fraud and abuse: Navigating the US Supreme Court's decision

By Alan Brill

Alan Brill (abrill@kroll.com) is Senior Managing Director, Cyber Risk Practice, at Kroll in Secaucus, New Jersey, USA. He is also an adjunct professor at the Texas A&M University School of Law.

The U.S. Supreme Court issued a ruling on June 3 focused on the Computer Fraud and Abuse Act (CFAA).^[1] The court held that if a person is granted access to data or a database, they cannot be prosecuted under that law even if they access the data for a clearly unauthorized purpose.

In the case, a police officer accepted several thousand dollars to use his in-car computer terminal to look up information on a license plate for an unauthorized person. The court said that once access was granted, it didn't matter why the individual accessed the data; it wasn't a violation of that law.

This decision doesn't mean that there aren't other applicable laws. Criminal prosecutions can be based on bribery, official misconduct, economic espionage, and other state and federal laws that are still in place. Prohibitions relating to privacy and intellectual property are still in effect.

Regardless of your feelings about this ruling, it is now settled. But as compliance specialists, we have to deal with the law as it is defined by the court. Clearly, we can't simply allow every computer user to decide how to use information or to put a company at risk. So, what should we do now?

This document is only available to members. Please [log in](#) or [become a member](#).

[Become a Member](#) [Login](#)