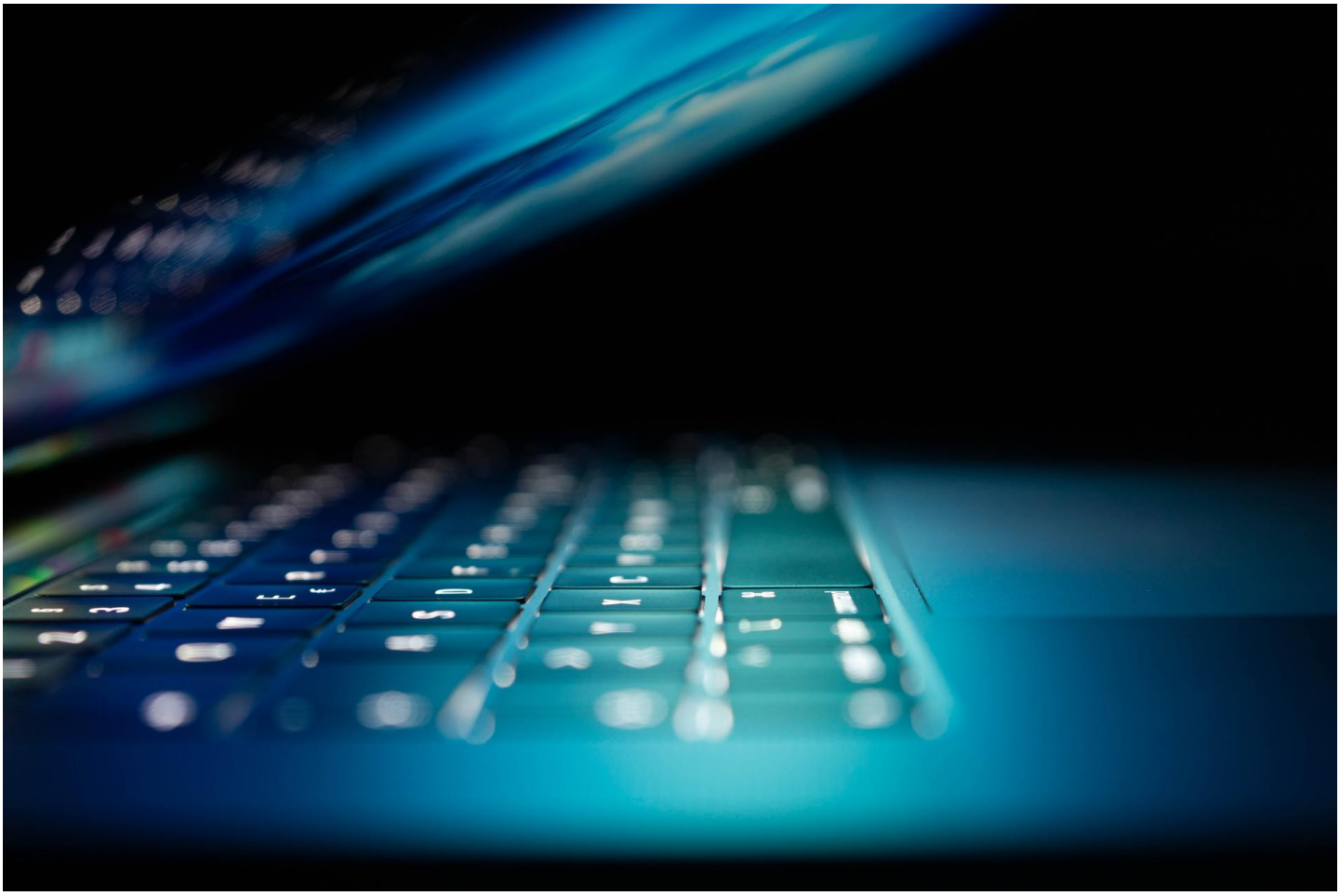
‘Leave The Gate Up or Leave it Down’: The Supreme Court’s Recent Decision Marks Changes in The Landscape of Cybersecurity and Privacy in Corporate America



By Dennis C. Vacco

July 1, 2021 | **ARTICLES**

Enacted in 1986, the Computer Fraud and Abuse Act (“CFAA”) was introduced to defeat hacking and to protect consumers against computer fraud. At its core, the CFAA seeks to prohibit access to data “without authorization.” Despite this, the CFAA’s prohibition regarding authorization has been far from clear and, instead of helping businesses protect themselves from data and security breaches, has left them exposed.

The Supreme Court’s recent decision in *Van Buren v. United States*, 141 US 1648 (2021) puts an end to any potential ambiguity regarding authorization and clearly defines the parameters of

authority outlined in the CFAA. In *Van Buren*, Georgia police Sergeant Van Buren used his patrol car to access a law enforcement database to retrieve information about a license plate number. An FBI investigation subsequently revealed that Sergeant Van Buren used his valid credentials to perform the search but used this information for non-law enforcement purposes. As a result, he was charged under the CFAA and sentenced to 18 months in prison for "accessing a computer without authorization or exceeding authorized access" 18 U.S.C. § 1030 (a)(2). In his appeal to the Eleventh Circuit, Seargant Van Buren argued that the "exceed authorized access" clause applied only to those who obtain information to which their computer access does not extend, not to those who misuse the access that they otherwise have.

The Supreme Court agreed with Van Buren that the CFAA does not reach improper motives in obtaining information through otherwise authorized channels, or the misuse of that information once obtained. In the opinion, Justice Amy Coney Barrett maintained that an "individual exceeds authorized access when he accesses a computer with authorization but then obtains information located in particular areas of the computer – such as files, folders or databases – that are off limits to him." *Id.* The result of that conclusion is that Sergeant Van Buren's misuse of information that he obtained through a system that he had authorized access to did not violate the CFFA. Accordingly, an interplay exists between the "without authorization" and "exceeds authorized access" clauses in that, first, an individual violates the provision when he accesses a computer without authorization and second, he exceeds authorized access by accessing a computer with authorization and then obtaining information he is not entitled to obtain. The Court referred to a "gates up or down inquiry," meaning the analysis turns solely on whether or not the individual had authorized access to the computer system and any files within that system, therefore authorized access, effectively means access to all information therein unless limitations on access are made clear.

The Court's decision provides a clear answer to one real-world question that arises when cyber threats of all kinds are omnipresent. For our clients and businesses, it will be important to establish well-defined limits of authorized and unauthorized access to systems and information and ensure that privacy protocols and compliance programs are in place to protect business interests and personal data.

Please contact Sabrina Marco Smith at 904.660.0020 x1546 orsmarcossmith@lippes.com with questions regarding this article or any other Government & State Attorneys General Investigations matter.