Litigation Alert: The U.S. Supreme Court Hears Oral Argument Regarding the Computer Fraud and Abuse Act

12/17/2020

On November 30, 2020, the U.S. Supreme Court heard oral arguments for Van Buren v. United States, No. 19-783 (U.S.) to resolve a circuit split as to what it means to "exceed authorized access" under the Computer Fraud and Abuse Act (CFAA). At issue is whether the federal statute, which was intended to prevent hacking from "outsiders," also applies to "insiders," such as employees and others who have access to a database and exceed their authorized access for an improper purpose. If so, which "insiders" does the statute restrict and what exactly is an improper purpose?

Regardless of how the Court rules, this decision will have important consequences for all who have access to a database, computer, and/or website, including employees, independent contractors, and others, who must all abide by restrictions related to access. For example, a key question posed to the Court is whether the statute applies to an employee who is subject to the employer's policies. What about the applicability to an employee who has access to a computer for work and uses it for personal reasons? An IT technician who has broad discretion to access the company network but exceeds the scope of his authority? Users who agree to abide by the terms and conditions on a social media or other website, but exceed the terms and conditions of the website? Students who are granted access to a database for a specific educational purpose? How will the Court apply the statute to these circumstances?

Since the statute contains a criminal component, the Court's decision can dramatically expand or eliminate the range of conduct subject to criminal penalties and civil liability under the statute and could expand or limit claims in trade secret and employment litigation.

The Computer Fraud and Abuse Act

The CFAA was passed in 1986 and recently amended in 2008. At issue is 18 U.S.C. § 1030(a)(2), which states that an individual may be subject to criminal penalties or civil liability if he or she "intentionally accesses a computer without authorization or exceeds authorized access." There is currently a circuit split as to the definition of "exceeds authorized access." The First, Fifth, and Seventh Circuit Courts of the United States Court of Appeals have held that accessing a computer for an unauthorized purpose violates the statute, even if the person was otherwise authorized to access the information. However, the Second, Fourth, and Ninth Circuits have held that a person violates the statute only if a person accesses information on a computer that he or she is prohibited from accessing. Please see our August 10, 2020 alert, "The Computer Fraud and Abuse Act: Does it Protect Against the Improper Use of Electronically Stored Information?"

The case arises from the criminal conviction of Nathan Van Buren, a sergeant with the police department in Cumming, Georgia. Van Buren ran an unauthorized search for a woman in the government database to determine if she was an undercover police officer at the request of an individual in exchange for a personal loan to Van Buren. He was convicted of violating the CFAA. The Eleventh Circuit affirmed the conviction.

The Court will resolve whether Van Buren's conduct "exceeds authorized access" under the applicable section of the CFAA.

What SCOTUS Will Likely Consider

On one hand, with the broad range of conduct potentially implicated by the CFAA, the Court may try to read the statute narrowly, so as not to expand the wide range of conduct noted above and to allow Congress to resolve the issue by additional legislation. Arguments have been made that in criminal cases, statutory ambiguities should be resolved in favor of the

defendants, so as not to criminalize more conduct than originally intended by Congress. There is also a question as to whether the statute only applies to users of a certain type of "database," such as a work or government database, or whether it applies to users of any system where you have to "log on" or abide by terms and conditions, including websites.

On the other hand, a broad reading of the statute will protect the privacy interests of many and prohibit authorized users from obtaining information for an improper purpose, such as someone who accesses GPS information or social security numbers for a criminal purpose or personal profit. However, it could also tie the hands of others, including a company's IT personnel who may require more flexibility to identify and resolve computer problems and may fear that innocent conduct could violate the statute. Employers may prefer a broader reading of the statute to prohibit employees from stealing trade secrets or confidential information. Other critical issues the Court should consider include who provides the "authorized access" under the CFAA, and whether the CFAA is violated if actions are inconsistent with a company policy, website terms and conditions, or instructions from an authority figure.

The Supreme Court's resolution of this case will have an important impact on employers, employees, and other users of databases and websites. It remains important for companies to stay informed on recent developments in the law as they apply to technology, particularly today, as the COVID-19 pandemic has increased employee access to employer data, chiefly through remote working arrangements, with little oversight.

In some instances, litigation may be necessary to protect your company's interests. If you have any questions about this alert, please contact:

Rose A. Suriano, Esq., Member and Co-Chair, Litigation Practice, at rsuriano@bracheichler.com or 973-403-3129

Robyn K. Lym, Esq., Associate, Litigation Practice, at rlym@bracheichler.com or 973-403-3124