U.S. Supreme Court Decision Limiting Scope of Computer Fraud and Abuse Act Narrows One Legal Protection of a Business's Digital Information

Client Advisories

06.14.2021

Every business generates and maintains various types of information, and whether it be trade secrets, confidential customer records or things like customer complaints, they do not want their information to fall into the hands of a competitor or the general public. There are several laws that a business can invoke to protect its information if it takes the proper precautions. One such law is the federal Computer Fraud and Abuse Act (CFAA), which applies to unauthorized access to electronically stored or "digital" information. However, in its recent decision in *Van Buren v. United States*, the United States Supreme Court limited the protections available to owners of digital information under the CFAA.

The CFAA is a federal statute that applies to nearly any computer, as long as it is used in or affects interstate or foreign commerce, which would include all computers that connect to the Internet. Broadly speaking, the CFAA provides both civil remedies and criminal penalties for unauthorized access to and modification of digital content on a protected computer in two circumstances: (1) a traditional hacking scenario in which an individual gains access to a computer without authorization, and (2) where an individual "exceeds authorized access" to obtain or modify information. The second circumstance was the focus of the Supreme Court's decision in *Van Buren*, where it addressed the question of whether an individual "exceeds their authorized access" when they obtain or modify information with an improper motive. In other words, does the CFAA cover situations where an individual, commonly an employee, is allowed to access certain digital files to do his or her job, but then removes, copies or changes the information for an improper purpose, such as to help a competitor?

The Court's answer was "no." It ruled that the CFAA covers only traditional hacking and instances in which an individual was given access to some parts of a computer, but exceeds his authorization by accessing or using "areas in the computer—such as files, folders, or databases—to which their computer access does not extend." For example, a person may violate the CFAA if he is given access to a computer to work on a group

project, but then uses that access as an opportunity to hack into a password-protected file on that computer. On the other hand, if a person modifies or uses information that she is otherwise able to access without additional authorizations, there is no CFAA violation regardless of their motives.

On its face, the Court's holding makes sense, since Congress likely did not intend to criminalize conduct such as employees "exceeding their authorized access" by using a work computer to look at their personal email. The takeaway for employers, however, is this: if an employer gives an employee access to certain information for any reason, the CFAA will not protect the employer if the employee modifies or extracts that information, regardless of their motive or the employer's original reason for giving the employee authorized access.

Despite the Court's holding, the CFAA still provides some first line defense for all digital content. To make use of this protection, businesses should configure their computer systems to restrict their employees', contractors' and vendors' access to the digital information that they need to do their jobs, such as by tailoring permissions in software tools based upon job categories and job functions.

Moreover, to the extent that an employer needs to make certain information available to its employees, all is not lost. State and federal laws other than the CFAA protect certain types of information, such as trade secrets or confidential business information, under a variety of circumstances. These include state statutes similar to the CFAA that address unauthorized access to computer systems. But, these protections vary from state to state and law to law, and come with restrictions. For example, a business must employ "reasonable measures" to keep its information confidential in order to protect it as a "trade secret." This in turn should counsel a business to enter into clear, written policies and agreements with anyone who has access to its information, including employees, vendors and contractors, and to include appropriate provisions in an employee handbook, as well as to take other measures to effectively protect its valuable information, whether digital or otherwise.

If you have questions about the CFAA and similar laws to protect your business information, please contact Robert T. Egan, Chair of Archer's Data Privacy and Cybersecurity Group and member of Archer's Trade Secret Protection and Non-Compete Group at 856-354-3079 or regan@archerlaw.com, or Nicholas T. Franchetti, also of both practice groups, at 856-857-2786 or nfranchetti@archerlaw.com.

DISCLAIMER: This client advisory is for general information purposes only. It does not constitute legal or tax advice, and may not be used and relied upon as a substitute for legal or tax advice regarding a specific issue or problem. Advice should be obtained from a qualified attorney or tax practitioner licensed to practice in the jurisdiction where that advice is sought.

Related People

Robert T. Egan

Of Counsel

regan@archerlaw.com

856.354.3079

Nicholas T. Franchetti

Associate

nfranchetti@archerlaw.com

856.857.2786

Related Services

- Data Privacy & Cybersecurity
- Trade Secret Protection & Restrictive Covenants

© 2024 Archer & Greiner, P.C. All rights reserved.