THE
NATIONAL LAW REVIEW

District Court Finds no CFAA Violation where Employee Shares Confidential Company Information with Competitor

Thursday, May 23, 2019

A district court in Tennessee recently concluded in *Wachter Inc. v. Cabling Innovations LLC* that two former employees who allegedly shared confidential company information found on the company's computer system with a competitor did not violate the Computer Fraud and Abuse Act (CFAA). The CFAA expressly prohibits "intentionally accessing a computer without authorization or exceeding authorized access, and thereby obtaining… information from any protected computer".

Article By Maya Atrakchi
Jason C. GavejianJackson Lewis P.C.
Workplace Privacy Blog

Communications, Media & Internet
Labor & Employment
Litigation / Trial Practice
Tennessee

The two former employees in question worked for Wachter Inc., a Kansas-based communications equipment provider, during which time they allegedly sent confidential company information to their personal email accounts and to email accounts of Wachter's competitor, Cabling Innovations. In addition the former employees allegedly used Wachter's resources and confidential information to obtain and perform work for Cabling Innovation.

In its reasoning, the Court emphasized that the CFAA does not define the term "without authorization" and *some* courts have found that "an employee may access an employer's computer 'without authorization' where it utilizes the computer to access confidential or proprietary information that he has permission to access, but then uses that information in a manner that is inconsistent with the employer's interest". Moreover, the Court highlighted that "the CFAA was not meant to cover the disloyal employee who walks off with confidential information. Rather, the statutory purpose is to punish trespassers and hackers".

The Court went on to state that the CFAA is primarily a criminal statute, and although it also permits "any person who suffers damage or loss by reason of a violation … [to] maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief," the rule of "lenity" directs the Court to construe the CFAA coverage narrowly. The Court reasoned, "the rule of lenity limits the conduct that falls within the criminal prohibitions, it likewise limits the conduct that will support a civil claim".

The CFAA has generated much debate among the courts regarding the scope of its application. Some forms of "unauthorized access" are obvious – e.g. a hacker breaking into a protected computer system resulting in data theft is clearly a CFAA violation and is the type of event the CFAA was originally designed to protect against. However, other circumstances, particularly in the employment context, can blur the lines of what is considered "unauthorized access" under the CFAA.

The court in *Wachter* is under the jurisdiction of the Sixth Circuit, which has not addressed the issue of a potential CFAA violation where an employee who has permission to access company information then misuses or misappropriates that information. That said, most districts courts in the Sixth Circuit have concluded that there cannot be a CFAA violation where an employee had permissible access to the computer system. Similarly, the Fourth Circuit held in *WEC Carolina Energy Solutions LLC v. Miller* that an employee who allegedly downloaded proprietary information from an employer's computer system for the benefit of his subsequent employer did not violate the CFAA.

Other circuits, however, have taken a much more expansive approach to what employee activity is considered

"without authorization" under the CFAA. For example, in *U.S. v. John*, the Fifth Circuit held that an employee violated the CFAA when she retrieved confidential customer account information she was authorized to access and transferred it to her half-brother for the purpose of committing a fraud. The First, Seventh and Eleventh Circuits have all taken a similarly expansive view that an employee violates the CFAA when he/she accesses the computer system in violation of the employer's data use policies.

The U.S. Supreme Court has avoided addressing issues of CFAA vagueness. Most recently, the Supreme Court denied certiorari in *Nosal v. United States*, 16-1344, declining to weigh in on the scope of unauthorized access under the CFAA. The Ninth Circuit held in *Nosal* that David Nosal violated the CFAA by using his past assistant's password to access his former employer's computer system after his access credentials were expressly revoked.

Given the conflicting jurisdictional interpretations of the CFAA, companies should review their policies and procedures to ensure access rights and limitations to their information and information systems are clearly defined and effectively communicated to their employees. Taking these steps will help protect company data and may be useful in preserving a potential CFAA claim.

Source URL: https://www.natlawreview.com/article/district-court-finds-no-cfaa-violation-where-employee-shares-confidential-company