Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

2nd Circ. Set To Weigh In On CFAA Circuit Split

Law360, New York (July 16, 2015, 10:38 AM ET) --

The Second Circuit is poised to take sides in the current federal circuit court split about the extent to which the Computer Fraud and Abuse Act covers an employee's misappropriation of information from his/her employer. The split arises from the following typical fact pattern: The employee uses her work computer to take company information for use in planned future employment but does not perform any technical "hacking" beyond accessing and taking the information. Application of the CFAA is important because the statute provides access to the federal courts as well as powerful civil and criminal remedies.

Daniel Winston

Some federal circuit courts hold that the CFAA creates a cause of action only for true hacker-style access to computers, such as where the employee circumvents technical protections to access company information. Yet other circuits read the CFAA much more broadly, and interpret it to cover the actions of the employee who merely accesses company information permissibly as an employee and then uses that information outside of or after employment for purposes at odds with those of her employer. The status of this issue is an important consideration for any employer, depending in part on which federal court might address any employee misappropriation.

Why the CFAA Matters

The CFAA, enacted in 1986, created a cause of action against an individual who "intentionally accesses a computer without authorized access or exceeds authorized access, and thereby obtains" "information from any department or agency of the United States; or information from any protected computer." 18 U.S.C. § 1030(a)(2). The phrase "exceeds authorized access" is defined as "access[ing] a computer with authorization and … us[ing] such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6). Violators are subject to criminal penalties including fines and up to 10 years imprisonment. Moreover, in 1994, the CFAA authorized a victim to file a civil action against the violator.

The question of liability in CFAA cases often turns on whether the employee "exceeds authorized access" rather than acts "without authorization," because the employee usually has some level of authorization. The subject of current debate among the United States Circuit Courts of Appeals is

whether an employee "exceeds authorized access" when she is permitted by her employer to access certain information on a computer, but then uses that information for an unauthorized purpose, such as in connection with subsequent employment, often in violation of the original employer's computer use policy and often for the benefit of a competitor.

Whether the CFAA applies is important for several reasons. First, it provides the rare opportunity in the employer-employee context for an employer to access to the federal courts. Other remedies that might apply — for example, breach of contract, breach of fiduciary duty, misappropriation of trade secrets, conversion, or tortious interference — often restrict the employer to state court. In addition, the CFAA introduces a lower bar than is required by a traditional misappropriation of trade secrets claim, which requires proof that the misappropriated information qualifies as a trade secret. The CFAA has no such requirement for improperly accessed information. Employers can bring CFAA claims in the absence of a noncompete, nondisclosure, or confidentiality agreements. Finally, the CFAA provides the possibility of criminal enforcement, compensatory damages and injunctive relief.

The Federal Circuit Split

The Fourth and Ninth Circuits have recently adopted the narrower reading of the CFAA, holding that the CFAA applies only when the employee engages in true hacking. WEC Carolina Energy Solutions v. Miller, 687 F.3d 199 (4th Cir. 2012); United States v. Nosal, 676 F.3d 865 (9th Cir. 2012). Yet the First, Fifth, Seventh and Eleventh Circuits have previously applied the broader reading, holding that an employee acts without authorization or in excess of his authority whenever the employee acquires an interest adverse to his employer or breaches an obligation owed to the employer. EF Cultural Travel BV v. Explorica Inc., 274 F.3d 577 (1st Cir. 2001); United States v. John, 597 F.3d 263 (5th Cir. 2010); Int'l Airport Ctrs. LLC v. Citrin, 440 F.3d 418 (7th Cir. 2006); United States v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010). Thus, these courts hold that an employer cause of action arises against an employee whenever the employee permissibly accesses computer information and then uses that information in a manner inconsistent with the employer's computer use policies. In this way, the broad-reading courts add an intent element into the statue: Liability turns on the employee's purpose for using the accessed materials.

The Second Circuit's Dilemma

The Second Circuit has not yet taken sides on the question of the CFAA's breadth and is poised to weigh in. On June 30, 2014, the United States District Court for the Southern District of New York applied the broad reading in United States v. Valle, 301 F.R.D. 53. The case involves rather remarkable allegations against a New York City police officer for (1) conspiring to kidnap and torture a group of women (including his own wife) with plans of rape, murder and cannibalism, and (2) violating the CFAA. The district court judge reversed the jury's conspiracy to kidnap conviction, but found (relevant here) that Valle's use of a federal law enforcement database for personal reasons (to look up a woman's personal information) violated the CFAA.

Specifically, the NYPD had issued Valle a laptop and log-in credentials authorizing him to access various law enforcement databases but only for official police business. Valle did not dispute that he used the law enforcement databases to run searches to investigate a woman's date of birth, address, height, eye color, restrictions on her driver's license, and other similar information, and that there was no work-related purpose for his searching. He argued that because he, as an NYPD officer, was authorized to access the database, he was not liable under the CFAA because he had not "exceeded authorized access." The district court held, however, that he exceeded his authorization when he used the database

for personal purposes, in violation of employer policies or regulations limiting computer use to official purposes, and therefore violated the CFAA. Valle appealed.

The case was argued before the Second Circuit on May 12, 2015. Valle, in his brief, encouraged the Second Circuit to adopt the narrow reading of the CFAA to require actual hacking. A broader reading, he argued, would create a cause of action against, for example, a person who simply misrepresents himself on a dating website in violation of its terms of use or against a court law clerk who merely uses the court's Westlaw account to see whether his personal law school note has been published. Valle focused on the difference between unauthorized "access" (which is explicitly prohibited by the statute) and unauthorized use (which is what Valle did). In Valle's view, the broad reading of the CFAA would transform every violation of a computer-use policy into a violation of a federal statute. In response, the government focused on a strict statutory approach to the CFAA, highlighting the fact that it creates a cause of action for unauthorized access of information irrespective of the future use of the improperly accessed information. The access was unauthorized — the government argued — because it occurred outside the NYPD's permitted use.

The Second Circuit is now left to decide whether to affirm the district court's broad interpretation, or to join the Fourth and Ninth Circuits — the two most recent circuits to address the issue — in the narrow interpretation. At the May 2015 hearing of the Valle case, at least one Second Circuit judge was interested in Valle's argument that the broad reading of the CFAA proscribes too much. She asked the government whether an employee playing solitaire or using Facebook — in violation of corporate policy — could face federal litigation. The government responded that those actions would not involve "accessing information [from a protected computer]" as required by the statute.

As we await an answer from the Second Circuit, employers and employees alike should take note. If an employer can bring litigation in a broad-reading jurisdiction, restrictive computer use policies might provide an avenue for assertion of CFAA claims against employees. Employees in broad-reading jurisdictions should also proceed with caution, as even seemingly benign computer-based activities may lead to liability. In a narrow-reading jurisdiction, however, employers must take extra caution to adequately protect their confidential and proprietary information as they may not have access to the CFAA.

—By Daniel Winston and Anita Spieth, Choate Hall & Stewart LLP

Daniel Winston is a partner and Anita Spieth is an associate in Choate's Boston office.