Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Improper Access Vs. Improper Use: The Meaning Of The CFAA

Law360, New York (May 12, 2016, 11:18 AM ET) --

Tyler Young

The theft of confidential and trade secret information has become a problem of staggering proportions.[1] To address this crisis, Congress last month passed the Defend Trade Secrets Act, which provides a private federal cause of action for trade secret misappropriation. For years to come, trade secret litigators will focus on the meaning of the DTSA. But in cases involving the use of a computer to commit misappropriation — an increasingly common fact pattern — litigators should also consider the application of another federal statute, the Computer Fraud and Abuse Act. The CFAA provides important remedies for victims of computer-based information theft, but the federal courts are deeply divided on the statute's reach and scope. Specifically, the courts disagree on whether the CFAA applies to an individual who has legitimate access to a computer but makes improper or unauthorized use of information obtained through legitimate access.

The applicability of the CFAA can have significant consequences for litigants because a CFAA claim has different elements than a standard trade secret claim. For instance, a CFAA plaintiff need not prove that the information at issue is actually a "trade secret," obviating the need to show that plaintiff took reasonable efforts under the circumstances to protect the confidentiality of the information or that the information has independent economic value because it is not generally known. Plaintiffs may therefore have an incentive to plead CFAA claims as a companion to their trade secret claims.

The CFAA imposes civil and criminal liability for obtaining information from a protected computer by either "access[ing]" a computer "without authorization" or "exceed[ing] authorized access."[2] Originally enacted as an anti-hacking statute, the CFAA was clearly intended to reach individuals who hack into an organization's computer system.[3] As demonstrated by a widening circuit split, however, it is less clear whether the CFAA was intended to reach the conduct of individuals who have authority to access a computer but make improper or unauthorized use of information obtained through that access.

The Second, Fourth and Ninth Circuits have adopted a narrow interpretation of the CFAA, concluding that the act does not apply to improper or unauthorized "use" of computer information if the initial access to that information was authorized.[4] The First, Fifth, Seventh and Eleventh Circuits, on the other hand, have adopted a broader interpretation, holding that CFAA liability can apply to a defendant who accesses information for a purpose other than that for which access is authorized, effectively creating liability for improper or unauthorized "use" of information.[5]

The Ninth Circuit led the way in articulating the narrow interpretation in United States v. Nosal, holding

that the CFAA targets the unauthorized procurement of information, not its misuse or misappropriation. In Nosal, the defendant terminated his employment and shortly after leaving the company convinced some of his former co-workers to access the company's confidential information to help him start a competing business. Those co-workers used their company log-in credentials to download confidential information from company computers and transferred it to defendant. Although the co-workers had authorization to access the database, the company had a policy forbidding the disclosure of confidential information.[6] The government charged Nosal under the CFAA with aiding and abetting his former coworkers in "exceed[ing their] authorized access" to company computers.[7]

The Ninth Circuit rejected the government's interpretation of the CFAA, which would have imposed liability on employees who have unrestricted access to a computer, but fail to comply with some limitation on the use to which they can put certain information. The court concluded that this interpretation of the CFAA "would transform the CFAA from an anti-hacking statute into an expansive misappropriation statute."[8]

The Fourth and Second Circuits followed the Ninth Circuit's lead, holding that the CFAA does not impose liability on an employee who violates a policy against downloading confidential information to a personal computer and then uses that information on behalf of a competitor,[9] or on a police officer who uses a government database to obtain information about a woman he intended to kidnap, in violation of a policy prohibiting use of a government database for non-law enforcement purposes.[10] These courts too have emphasized that the CFAA is not intended to "provide a remedy for misappropriation of trade secrets or violation of a use policy where authorization has not been rescinded."[11]

The First, Fifth, Seventh and Eleventh Circuits, in contrast, have focused on the purpose for which access is authorized to define liability under the CFAA. In United States v. John, for example, the defendant was an account manager at Citigroup Inc. and had access to Citigroup's internal computer system. She accessed and printed information regarding customer accounts and provided that information to her half-brother, which he used to make fraudulent charges on those accounts.[12] The defendant argued she could not be liable under the CFAA because she was authorized to use Citigroup's computers and to view and print information regarding customer accounts in the course of her official duties.[13] The court rejected defendant's argument, holding that "'authorized access' or 'authorization' may encompass limits placed on the use of information obtained by permitted access to a computer system and data available on that system."[14]

Courts following this broader interpretation have found that the CFAA applies to improper "access" in a broad range of circumstances, but the courts have used varied reasoning to reach that result. Some courts focused on the purpose for which access is granted and the ultimate use of the information.[15] Other courts found liability based solely on access in contravention of a computer use policy, even if the information was not ultimately used.[16] Other courts focused on the employee's intent at the time of accessing the computer.[17] And still others relied on a contractual or agency theory to conclude that authorized access ends as soon as an employee breaches the terms of an employment contract that granted access in the first instance.[18]

The CFAA may — depending on the jurisdiction — provide a potent cause of action for those who have been harmed by computer-based information theft. Trade secret litigators should carefully monitor the courts' evolving guidance on the scope and meaning of the CFAA.

—By Tyler Young and Cicely Miltich, Faegre Baker Daniels LLP

Tyler Young and Cicely Miltich are associates in Faegre Baker Daniels' Minneapolis office.

[1] Trade secret theft costs the U.S. economy tens if not hundreds of billions of dollars annually. See https://www.fbi.gov/news/testimony/combating-economic-espionage-and-trade-secret-theft

[2] 18 U.S.C. § 1030.

[3] See H.R. Rep. No. 98-894, at 3691-92, 3695-97 (1984); S. Rep. No. 99-432, at 2480 (1986).

[4] United States v. Valle, 807 F.3d 508 (2d Cir. 2015); WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199 (4th Cir. 2012); United States v. Nosal, 676 F.3d 854 (9th Cir. 2012) (en banc).

[5] EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577 (1st Cir. 2001); United States v. John, 597 F.3d 263, 269 (5th Cir. 2010); Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418 (7th Cir. 2006); United States v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010).

[6] Nosal, 676 F.3d at 856.

[7] Id.

[8] Id. at 857.

[9] WEC Carolina Energy, 687 F.3d 199.

[10] Valle, 807 F.3d 508.

[11] WEC Carolina Energy, 687 F.3d at 203, 207.

[12] 597 F.3d at 269.

[13] Id. at 271.

[14] Id.

[15] Id. at 271-72.

[16] Rodriguez, 628 F.3d at 1263-64.

[17] NCMIC Fin. Corp. v. Artino, 638 F. Supp. 2d 1042, 1059 (S.D. Iowa 2009).

[18] United States v. Phillips, 477 F.3d 215, 221 & n.5 (5th Cir. 2007); Shugard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1124-25 (W.D. Wash. 2000).