The Computer Fraud and Abuse Act: An Uncertain Path for Bringing Trade Secrets Litigation in Federal Court

1/15/2011

As part of its sweeping Comprehensive Crime Control Act of 1984, Congress enacted a criminal statute prohibiting the "unauthorized access" of information contained in federal government computers and computers employed by certain federally-related financial institutions. The law is codified at 18 U.S.C. § 1030. The Act was intended to punish hackers who tap into computers to disrupt or destroy computer functionality and persons who hack into specified computers to steal the information stored therein.

As the various methods of computer fraud grew, the Act was amended. In 1986 it became known as the Computer Fraud and Abuse Act ("CFAA"). In 1994, Congress added a private civil right of action under the CFAA (18 U.S.C. § 1030(g)), seemingly allowing federal claims for stealing trade secrets stored on a protected computer. The Act now provides that it is unlawful if a person (1) "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer [§ 1030(a)(2)(C)]; (2) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value . . . [in excess of $5,000 in one year] [§ 1030(a)(4)]; or (3) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damages or loss. [§ 1030(a)(5)(iii)]." A "protected computer" is defined as one "used in or affecting interstate or foreign commerce" [§ 1030(e)(2)(B)]. That definition is usually broad enough to cover any computer used in trade secret theft.

The private right of action provides that any person suffering damages or loss by reason of a violation of the Act "may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief [§ 1030(g)]." The Act does not define "trade secret" or require that the owner have taken reasonable efforts to protect its secrecy.

Not surprisingly, as an alternative to employing traditional diversity jurisdiction, trade secret theft plaintiffs seized upon these amendments to institute federal actions to redress state law trade secret violations. The perceived advantage of a speedier resolution and better chance of obtaining injunctive relief further encouraged this federal forum selection.

However, the CFAA nowhere defines what it means to access a computer "without authorization." Most theft of trade secret cases involve a disloyal employee who downloads an employer's information to take to a new venture. In doing so, he downloads the information from the very computer provided to him by his employer to perform his work. In *International Airport Centers, L.L.C. v. Citron*, 440 F.3d 418 (7th Cir. 2006), the court had no difficulty recognizing that such downloading of sensitive information by a disloyal employee from his employer-provided computer was unauthorized. The court held the employee's "authorization to access the laptop terminated, when, having already engaged in misconduct and decided to quit [his employer] in violation of his employment contract, he resolved to destroy files that incriminated himself and other files that were also the property of his employer in violation of the duty of loyalty that agency law imparts on an employee. . . . Breach of his duty of loyalty terminated his agency relationship . . . and with it his authority to access the laptop because the only basis of his authority has been that relationship." *Id.* at 421-22. In *Citron*, the court thus focused on the mental state of the employee at the time of the downloading rather than whether he was authorized to access the information for a business-related purpose. In *EF Cultural Travel BV v. Explorica Inc.*, 274 F.3d 577, 582-584 (1st Cir. 2001) the First Circuit utilized a similar approach.

But, in *United States v. Brekka*, 581 F.3d 1127 (9th Cir. 2009), the Ninth Circuit interpreted the "without authorization" requirement in a remarkably different and narrower fashion. It was "undisputed that when Brekka was employed by Plaintiff that he had authority and authorization to access documents and emails that were found on his home computer and laptop." *Id.* at 1132. The court, however, rejected the *Citron* analysis that an employee, having been authorized to access his employer's computer, "can lose authorization to use a company computer when the employee resolves to act contrary to the employer's interest." *Id.* at 1134. It emphasized the primarily criminal nature of the CFAA and reasoned that "when a statute has both criminal and noncriminal applications, courts should interpret the statute consistently in both criminal and noncriminal contexts. It is well established that ambiguity concerning the ambit of criminal statutes should be resolved in favor of lenity." *Id.* at 1134. The court ultimately concluded that the "without authorization" element is met only when a person has not received permission to use the computer for any purpose, like the hacker contemplated in the statute's original version, or when the computer is used by the employee after the employer rescinds its prior permission to access the computer.

A recent opinion by Judge Henderson of the Northern District of California refined *Brekka*. The court dismissed a CFAA claim with prejudice even though the employer had attempted to limit authorization by requiring employees to contractually promise not to recruit other employees or use trade secrets of his employer (concluding that "these cases—which hold that access is not established by employer's policies, but by the extent the employer makes the computer system available to the employee—[are] persuasive"). *See Accenture, LLP. v. SIDHU*, 2010 WL 4691944 (N.D. Cal. Nov. 9, 2010).

Notwithstanding that the CFAA defines "exceeds authorized access" as "a means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled to obtain or alter," Judge Henderson reasoned that the phrase "exceeds authorized access" must be viewed through the same lenity prism the Ninth Circuit used to construe the "without authorization" prong. He agreed with the ruling in *United States v. Nosal*, 2010 WL 934257 (N.D. Cal. Jan. 6, 2010), that under the CFFA an employee exceeds authorized access when he accesses information without permission to use the computer, but not when he merely violates company policies. District courts outside the Ninth Circuit appear to be following Brekka as well. *See*, *e.g.*, *Del Monte Fresh Produce N.A. v. Chiquita Brands Int'l Inc.*, 616 F. Supp. 2d 805, 812-813 (N.D. Ill. 2009).

The distinction between being denied access by company policies as opposed to the formal rescission of the right to access an employer-owned computer is fine. As noted in *Citron*, "the difference between 'without authorization' and 'exceeding authorization' is paper thin." *Citron* noted that both prongs could be satisfied if an employee accessed a computer with disloyal intent. In contrast, *Brekka* and *SIDHU* held that the employee's intent is irrelevant and that whether the downloading was "without authorization" or in excess of "authorized access" depends on whether the employer permitted the employee to access the stolen information for any purpose.

The division among the circuits poses forum selection issues for plaintiffs. In most trade secret theft cases brought in federal court, plaintiffs allege CFAA violations and also allege state theft of trade secrets claims under the Uniform Trade Secrets Act (common law trade secret cases are preempted in 45 states under the UTSA). In *Brekka*, the CFAA claims were dismissed at the summary judgment stage and the trial court declined to exercise supplemental jurisdiction over the remaining state law claims. *Brekka* at 1130. As such, the plaintiff was left to start over in state court.

In alleging a CFAA violation as a means to gain federal jurisdiction for trade secret theft claims, plaintiffs must examine the law in its chosen forum and weigh the uncertainty of a court's ultimate determination of the "unauthorized" element against the risk that the court might either dismiss the case altogether for failure to state a federal claim, or exercise pendent jurisdiction anyway, thus subjecting the plaintiff to the perceived detriments of litigating trade secrets claims in federal court. The potential downsides include the undesirability of the federal unanimous jury requirement, wider jury pools, accelerated "initial disclosure" obligations requiring the identification of "documents and witnesses" under Fed. R. Civ. P. 16(a)(2)(G), and the fact that a CFAA violation is "limited to economic damages" (18 U.S.C. § g) (*i.e.*, meaning that punitive damages are not available), may make a state forum selection the better choice in an individual case. Indeed, what appears at first to be an easy shortcut to judgment might require taking the longer route in the end.