

THE NATIONAL LAW JOURNAL

MONDAY, FEBRUARY 5, 2001

Court gives new use to 1994 law: trade secrets

Computer Fraud and Abuse Act found to apply to data copied from old employer's computer.

BY STEPHEN R. BUCKINGHAM
SPECIAL TO THE NATIONAL LAW JOURNAL

THE METEORIC RISE of the information economy, the Internet and increasing globalization have prompted a legislative trend in the United States toward the federalization of trade secret protection.¹ Although federal legislation has so far been directed primarily at the creation of criminal offenses, a recent district court decision under a little-publicized 1994 statute represents what could be a large step toward the federalization of civil trade secret litigation.

In a recent case of first impression, *Shurgard Storage v. Safeguard Self Storage*,² the U.S. District Court for the Western District of Washington held that an employer has three different causes of action under the federal Computer Fraud and Abuse Act (CFAA)³ against an employee who, without permission, copies information from his or her employer's computer to use in his or her new employment, provided that the computer is connected to the Internet and is thereby a "protected computer" under the CFAA.

Because of the expanding reliance by businesses on computers for the storage of records and information, trade secret cases increasingly involve misappropriation based on the copying of files from an employer's computer. With the ubiquity of the Internet, the CFAA, as interpreted in *Shurgard*, may prove a widely available federal-law complement to traditional state-law trade secret claims, and under some circumstances, copyright infringement cases. A CFAA claim, in addition to providing federal court jurisdiction, could provide other advantages over traditional trade secret claims, perhaps even eliminating the need to prove that the information obtained constituted "trade secrets."

Mr. Buckingham, a registered patent attorney, is a litigation partner in the Internet group at Roseland, N.J.'s Lowenstein Sandler.

In 1984, a decade before commercial use of the Internet exploded, the CFAA was enacted to create criminal penalties to combat the increased incidence of "hacking" into the computer systems of the government and financial institutions.⁴ Through a series of amendments, the statute was gradually expanded to cover a broad range of unauthorized activities relating to government and private computer systems. Most notably, in 1986, the scope of the act was expanded greatly beyond the computers of government and financial institutions to include all computers involved with interstate communications.⁵ As the *Shurgard* court observed, although "the CFAA did not intend to enact sweeping federal jurisdiction...since the advent of the Internet, almost all computer use has become interstate in nature."⁶

In 1994, an amendment to the CFAA providing a civil remedy was enacted. Under that subsection, "[a]ny person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." Although the CFAA's civil remedy has been on the books for more than six years, surprisingly few reported court decisions (all at the district court level) have interpreted and applied it. Moreover, none of the few decisions preceding *Shurgard* involved trade secret misappropriation.⁷ This delay in the use of the CFAA might be explained by the fact that when its civil remedy was added in 1994, Internet use, and hence the applicability of the CFAA, was minimal. *Shurgard* not only was the first court decision to apply the CFAA to civil trade secret claims, but it also found three different civil causes of action under the CFAA arising from the same alleged misappropriation.

The facts behind 'Shurgard'

The *Shurgard* decision was made in the context of a pre-discovery motion to dismiss for failure to state a claim on which relief may be granted under Federal Rule of Civil Procedure 12(b)(6). The factual allegations that formed the basis for the decision were few in number. *Shurgard* alleged that one of its employees was approached by defendant Safeguard Self-Storage and offered employment, which was accepted.⁸ Before leaving employment at

Shurgard, without *Shurgard*'s knowledge or consent, the employee sent e-mails to his new employer that contained trade secrets and proprietary information, including *Shurgard*'s business and expansion plans.⁹ Based on these few allegations, the court denied the defendant's motion to dismiss three separate claims asserted pursuant to three different provisions of the CFAA.

First, the court upheld *Shurgard*'s claim pursuant to 18 U.S.C. 1030(a)(2)(C). That provision of the CFAA defines a violation as occurring when a person "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains...information from any protected computer if the conduct involved an interstate or foreign communication." "Protected computer" is defined under the CFAA as a computer "used in interstate or foreign commerce or communication."¹⁰

While employed by *Shurgard*, its employee was authorized to use the computer in question. The court nevertheless found that the employee's access to *Shurgard*'s computer was "unauthorized," relying on *The Restatement (Second) of Agency*, under which an agent's authority terminates automatically when the agent acquires an adverse interest or commits a serious breach of loyalty.¹¹ Although unstated in the opinion, the court presumably found that the e-mail transmission satisfied the "interstate communication" element of this offense.

Second, the court upheld *Shurgard*'s claim pursuant to 18 U.S.C. 1030(a)(4), which penalizes anyone who "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." Importantly, the court found that the "fraud" element does not require proof of all of the elements of common-law fraud. Rather, adopting the standard used in federal mail- and wire-fraud cases¹² and in a criminal case under the CFAA,¹³ the court held that "fraud" meant simple "wrongdoing by dishonest methods or schemes."¹⁴ Using that standard, the court found the allegations that the *Shurgard* employee e-mailed *Shurgard*'s secret information to a competitor satisfied the "fraud" element.

FOCUS
ON
Trade
Secrets

Last, the court also upheld Shurgard's claim pursuant to 18 U.S.C. 1030(a)(5)(C), which applies to a person who "intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage." The defendant argued that the mere misappropriation of information was not sufficient to satisfy the "damage" element of the offense. Under the CFAA, "damage" occurs when "any impairment to the integrity or availability of data, a program, a system, or information... causes loss aggregating at least \$5,000 in value during any 1-year period."¹⁵ After reviewing the legislative history of the CFAA, the court concluded that the "integrity" of trade secret information is compromised by theft of such information, and therefore such theft could constitute "damage" within the meaning of the CFAA.¹⁶

Applications and benefits

Shurgard recognized for the first time a civil cause of action under the CFAA for a factual scenario common in trade secret cases: an employee has quit and copied confidential company information from the employer's computer to take to his or her next employer. Such copying of computer files is often the easiest and most discreet way for a dishonest employee to take large amounts of company information.¹⁷

Although *Shurgard* involved an employee who allegedly e-mailed employer information to his next employer, the court's reasoning and the plain language of the CFAA suggest that the use of e-mail or the Internet is not a necessary element of two of the three causes of action in issue. Only the claim under § 1030(a)(2)(C) expressly requires an "interstate or foreign communication."

The § 1030(a)(4) claim requires simply the use of dishonest means to obtain "anything of value" from a "protected computer." Similarly, the § 1030(a)(5) claim requires only "damage" as a result of the unauthorized access to a "protected computer." For both of these causes of action, the constitutional commerce clause "hook" consists simply of the use of a facility of interstate commerce in the form of a "protected computer," defined as one that "is used in interstate or foreign commerce." Given the language of the CFAA, a simple Internet connection to the computer, with its interstate and foreign communication capabilities, transforms it into a "protected computer."¹⁸ Accordingly, claims can arise under § 1030(a)(4) and (5) regardless of whether the Internet was used to facilitate the misappropriation of information.

What benefits arise from the availability of causes of action under the CFAA?

First, the claims give rise to federal court jurisdiction in cases in which it otherwise would not exist. Under some circumstances, plaintiffs may prefer to litigate in federal court. Such a preference may be based on docket considerations and expected time to reach trial, the litigator's general familiarity with federal litigation, federal limitations on discovery, the ease of out-of-state third-party discovery in federal court litigation and other possible strategic considerations.

Second, a plaintiff may fare better in federal court when the misappropriated information is of a type that state law frowns on in terms of common-law trade secret protection. In particular, customer lists and other nontechnical business information are often given short shrift under state law. A federal court may be less influenced by state trade secret law when applying the plain language of the CFAA, which nowhere requires that the information obtained from a protected computer rise to the level of a "trade secret."

As trade secret litigators know, establishing

Claims under the CFAA give rise to federal court jurisdiction in cases in which it otherwise would not exist.

that information is a trade secret can sometimes prove difficult. The CFAA appears to eliminate this element of proof. Under its plain terms, § 1030(a)(2)(C) protects any "information" obtained from a protected computer, § 1030(a)(4) protects "anything of value" obtained from a protected computer and § 1030(a)(5) protects simply against "damage" resulting from unauthorized access to a protected computer. This would seem to afford an injunctive and/or damages remedy for any type of information obtained from a protected computer. Nevertheless, proving irreparable harm to obtain injunctive relief, and proving damages to obtain compensatory relief may ultimately turn on the strength of the plaintiff's proofs of the value of the information and its unavailability from other sources, which would be similar to proving that the information is a trade secret.

Third, the CFAA could also provide an alternative cause of action in a copyright infringement case when the copyrighted material involved was copied from a protected computer. A CFAA claim in such circumstances might provide immediate federal jurisdiction to obtain injunctive relief when it otherwise would not exist due to the lack of registration of the copyrighted material.¹⁹ A

CFAA claim could also act as an insurance policy, in the rare event that copyright infringement remedies are unavailable due to invalidation of the copyright registration.²⁰

For a trade secret plaintiff, the availability of federal causes of action under the CFAA provides a useful alternative that can complement and provide advantages, depending on the factual circumstances. Trade secret litigators should keep the CFAA in mind as yet another arrow in their quiver.

(1) See, e.g., The Economic Espionage Act of 1996, 18 U.S.C. 1831 et seq. (EEA). The EEA criminalized trade secret theft at the federal level, 18 U.S.C. 1832, and adopted a federal definition of "trade secret," 18 U.S.C. 1839(3). Although the EEA authorizes the attorney general to seek civil injunctive relief, 18 U.S.C. 1836, it affords no private right of action. See *Boyd v. University of Illinois*, 1999 WL 782492, at *4 (S.D.N.Y.) (EEA is a "criminal statute that affords no standing to any private citizen").

(2) 119 F. Supp. 2d 1121 (W.D. Wash. 2000).

(3) 18 U.S.C. 1030.

(4) See *Shurgard*, 119 F. Supp. 2d at 1127.

(5) *Id.* Although it is now hard to remember a world without universal Internet access, as late as 1991, those few judicial decisions involving the Internet discussed it as if it were an obscure network known only to high-level scientists and military officials. See e.g., *U.S. v. Morris*, 928 F.2d 504, 505 (2d Cir. 1991) ("Morris released the worm into INTERNET, which is a group of national networks that connect university, government, and military computers around the country.").

(6) *Shurgard*, 119 F. Supp. 2d at 1127.

(7) See *America Online Inc. v. National Health Care Discount Inc.*, 121 F. Supp. 2d 1255, 1275 (N.D. Iowa 2000) (unsolicited bulk e-mailing ("spamming")); *YourNetDating v. Mitchell*, 88 F. Supp. 2d 870 (N.D. Ill. 2000) (hacking and Web traffic diversion); *Shaw v. Toshiba America Information Systems Inc.*, 91 F. Supp. 2d 926 (E.D. Texas 1999) (very novel application to defective firmware (software burned into chips) in computer disk controllers in laptop computers); *America Online Inc. v. LCGM Inc.*, 46 F. Supp. 2d 444 (spamming).

(8) 119 F. Supp. 2d at 1123.

(9) *Id.*

(10) 18 U.S.C. 1030(e)(2).

(11) *Shurgard*, 119 F. Supp. 2d at 1125.

(12) Citing *McNally v. U.S.*, 483 U.S. 350, 358 (1987) and *Hammerschmidt v. U.S.*, 265 U.S. 182, 188 (1924).

(13) *U.S. v. Czubinski*, 106 F.3d 1069, 1078 (1st Cir. 1997).

(14) *Shurgard*, 119 F. Supp. 2d at 1125-26.

(15) 18 U.S.C. 1030(e)(8).

(16) *Shurgard*, 119 F. Supp. 2d at 1226-27.

(17) See, e.g., *Tradescape.com v. Shivaram*, 77 F. Supp. 2d 408, 412 (S.D.N.Y. 1999); *Doubleclick Inc. v. Henderson*, 1997 WL 731413 (N.Y. Sup.).

(18) See generally *U.S. v. Lopez*, 514 U.S. 549, 558 (1995) ("Congress is empowered to regulate and protect the instrumentalities of interstate commerce, or persons or things in interstate commerce, even though the threat may come only from intrastate activities").

(19) See 17 U.S.C. 411(a) ("[N]o action for infringement of the copyright in any work shall be instituted until registration of the copyright claim has been made in accordance with this title").

(20) See, e.g., *Richard J. Zitz Inc. v. Dos Santos Pereira*, 232 F.3d 290 (2d Cir. 2000) (affirming invalidation of copyright registrations).