New York Law Journal
Technology Today
Tuesday, September 5, 2006
ALM

Disloyal Employees

Computer Abuse Law Turns on Meaning of 'Without Authorization'

BY PETER J. PIZZI

INTERNET ISSUES

Employers victimized by disloyal employees who have misappropriated sensitive computer data have successfully sued under the civil remedy provision of the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. §1030.

Section1030(g) of the act offers a right to injunctive relief and damages where the former employee "without authorization" has accessed the network in order to abscond with proprietary information and documents or interfere with relationships between the company and its customers or suppliers.

Cases decided since 2000 construed in a way favorable to employers the act's concept of "authorization" in the context of the departing employee. In the typical fact pattern, an employee with authorized access to the network decided to accept another position and, before departing, copied important electronic information to better compete with the former employer in her new job.

Judges faced with this scenario generally held that the employee's "authorization" ceased or was "exceed[ed]" when the employee engaged in conduct intended to benefit the new employer.

In *Lockheed Martin Corp. v. Kevin Speed*,[1] an August 2006 decision from the Middle District of Florida, the court went against this precedent, declining to construe "authorization" as a transient permission that the employee lost when she switched allegiance to a new master. If followed by other courts, *Lockheed* could adversely affect CFAA's utility in the employment context.

When first passed in 1984 as the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, the CFAA was solely a criminal statute directed at protecting classified, financial and credit information relating only to the government and certain financial institutions. The statute prohibited unauthorized access to "federal interest" computers.

In the early 1990s, Congress recognized the burgeoning use of computers affected nearly all aspects of modern life, and determined that the statute was inadequate to address emerging computer-related crimes and abuses.

In 1994, 1996 and 2001, Congress amended the statute to provide increased protection for all computer data involved in interstate commerce as well as for any computer "located outside of United States that is used in a manner that affects interstate or foreign commerce or communications in the United States."

The 1994 amendments also added the civil remedies provision, §1030(g). This section provides that "[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."[2]

Further, as noted, the CFAA was also amended at that time to "protect computers and computer systems covered by the statute from damage by outsiders, who gain access without authorization and by insiders, who intentionally cause damage to a computer."[3] Specifically, 18 U.S.C.§1030(a)(5)(A) was modified to prohibit not only unauthorized access to a computer system, but also "transmission of a program, information, code or command" that "intentionally causes damage without authorization." To qualify under the act, the damage must exceed $5,000 in value.

Thus, after the 1994 amendment, the CFAA was no longer limited to protecting computers deemed necessary for national security and the national economy, but instead covered all computer data involved in interstate and foreign commerce while also providing a civil enforcement mechanism.

Early Employment Decisions

After the 1994 and 1996 amendments to the CFAA, there were few reported cases in the employment context. In early 2000, however, three cases were decided that created renewed employer interest in the CFAA.

United States v. Middleton[4] involved a government prosecution for a computer-related crime. The defendant argued that the phrase "one or more individuals" in the operative CFAA provision meant that corporations such as his former employer were not within the act's reach. He argued that Congress would have used the term "persons" as opposed to "individuals" if it had intended the CFAA to cover damages to a corporation.

The U.S. Court of Appeals for the Ninth Circuit rejected this idea, stating that Congress could not have intended to protect computers used in interstate and foreign commerce yet limit the act only to computers owned by natural persons. Though Congress replaced the word "individuals" with "persons" in its 2001 amendment to the CFAA, thereby eliminating the issue addressed in *Middleton*, the case remained helpful to employers because it shed light on the CFAA's $5,000 damage requirement.

The court held that this threshold could be satisfied by evidence showing the hourly rate of consultants hired to investigate and fix the damage done by the defendant and the cost of new software installed to prevent reoccurrence.

Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.[5] also arose in an employment context. Several former Shurgard employees used the company's computer network to send trade secrets to Safeguard, their future employer and a Shurgard competitor. The employees argued that they retained authority to access the plaintiff's computer system as long as they remained employees of Shurguard. The court dismissed their argument, applying traditional agency principles, and noting that any authority evaporated when the employees in question began serving the interests of the new employer. The district court also rejected the proposition that the CFAA was inapplicable to employees because it only applied to outsiders or "hackers."

Also in 2000, in *YourNetDating, Inc. v. Mitchell*,[6] the court held that an Internet dating service was entitled to a temporary restraining order prohibiting a former programmer from hacking its Web site and diverting its clients to a pornography site. Importantly, the court held that damage to the goodwill of the

Peter J. Pizzi *is chair of Connell Foley's Internet and information law practice and chair of the Internet and Litigation Committee of the New York State Bar Association's Commercial and Federal Litigation Section.* **M. Trevor Lyons,** *an associate in the firm's employment law group, assisted in the preparation of this article.*

plaintiff's services and its customers constituted irreparable harm within the scope of the CFAA.

Middleton, *Shurgard* and *YourNetDating* together established that the CFAA was not limited to traditional "hacker" activity but applied to the workplace and to unfair competition disputes.

An employer need only show that the system was accessed without authorization and caused at least $5,000 in losses. CFAA thus supplements an employer's arsenal but does not replace traditional causes of action.

An Emerging Standard

The portion of the CFAA most applicable in the employment context is §1030 (a)(5)(B)(i), which requires a "loss to 1 or more persons during any 1-year period...aggregating at least $5,000 in value." Though each section of the act imposes a slightly different prima facie case, courts have generally required proof that a defendant (1) intentionally accessed (2) a protected computer (3) without authorization, and (4) as a result of such conduct, (5) intentionally, recklessly or otherwise caused (6) damage.[7] Because several provisions of the CFAA relate solely to the protection of computers deemed necessary for national defense and the economy, however, employers typically allege only violations of §1030 (a)(2)(c), (a)(4) and (a) (5) of the act.

There are, however, several important issues that are emerging as employers seek to apply the CFAA to employee misconduct.

First, there is the question of what constitutes a "transmission" under §1030(a)(5)(a)(i). Specifically, §1030(a)(5)(a)(i) states that it is a violation of the CFAA if a former employee:

> knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer...

In *Airport Centers LLC v. Citrin*,[8] Judge Richard Posner addressed the situation in which a former employee used a secure erasure program, ostensibly downloaded from either the Internet or a CD, to delete data that he had been hired by his former employer to compile as well as e-mails showing that he had sought and secured employment with a competitor in violation of his employment contract.

The employee argued that his misconduct was not a transmission within the meaning of 18 U.S.C. 1030 (a)(5)(A)(i). Judge Posner rejected this argument, holding that Congress must have intended the use of a CD would fall within the reach of the act:

> If the statute is to reach the disgruntled programmer, which Congress intended by providing that whoever 'intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage' violates the Act, 18 U.S.C. §1030(a)(5)(A)(ii), it can't make any difference that the destructive program comes on a physical medium, such as a floppy disk or CD.

As noted, the "authorization" issue has also arisen in CFAA employment cases. Specifically, §1030(a)(4) makes it a violation to knowingly, and with intent to defraud, access a protected computer "without authorization" or to "exceed[] authorized access" to commit fraud and obtain something of value.

Shurgard and *Citrin* applied traditional agency principles, embodied by Restatement (Second) of Agency, §112, which provides that "the authority of the agent terminates, if, without knowledge of the principal, he acquires adverse interests or if he is otherwise guilty of a serious breach of the duty of loyalty to the principal."

This interpretation of the term "unauthorized access" means that anytime an employee acts other than in his employer's best interest in accessing an employer's computer system, such access is "without authorization" and therefore covered by the CFAA, assuming all other elements are present.

In his August 2006 decision in *Lockheed Martin Corp. v. Speed*, Judge Gregory A. Presnell declined to follow the *Shurgard* and *Citrin* use of agency law to interpret the term "authorization." The court considered the Restatement "extrinsic materials" to which courts are not to resort for purposes of statutory construction unless the language is ambiguous.

Judge Presnell held that the concept of "authorization" is not ambiguous because the employees involved clearly were given access by their employer. He also noted that, as a criminal statute, the CFAA was subject to the "rule of lenity," a principle of statutory construction requiring that criminal statutes be given a narrow, restrained interpretation.

Judges generally have held that the employee's "authorization" ceased or was "exceeded" when the employee engaged in conduct intended to benefit a new employer.

Based on this reasoning, Judge Presnell ruled that an employee who copied computer files before departing for a rival firm was neither "without authorization" nor "exceeding authorization" as those terms are contemplated by the CFAA because such access occurred while the employee still enjoyed access privileges to the company's computer system.

If *Lockheed* is sustained on appeal, the Eleventh Circuit would split with the First[9] and Seventh circuits on the scope of the CFAA as applied to disloyal employees, possibly setting the stage for a petition to the U.S. Supreme Court.

Judge Presnell's opinion raises at least two additional issues for further exploration.

First, should the civil remedy available to employers under the CFAA be read narrowly to avoid the possibility of criminalizing workplace misconduct? And, second, in response to *Lockheed*, can employers limit the "authorization" enjoyed by employees by redrafting computer use policies to proscribe use of the network for purpose adverse to the interests of the employer?

In *EF Cultural Travel BV. v. Explorica, Inc.*,[10] the First Circuit answered the latter question in the affirmative, holding that the employee lacked the requisite "authorization" because a confidentiality agreement he signed prohibited disclosure of information "which might reasonably be construed to be contrary to the [employer's] interests..."

Act's Benefits

The Computer Fraud and Abuse Act offers employers many advantages. It gives them a choice of forum because the statute bestows federal question jurisdiction. In addition, it can provide a remedy against the competing former employee that may be unavailable under state law in jurisdictions such as California which, except in limited circumstances, refrain from enforcing employee non-compete agreements.

The employer's burden is also relatively light due to the CFAA's focus on the abuse of a computer system, as opposed to the quality or character of information or data taken.

Thus, employers can bring CFAA claims without having to prove that the information wrongfully accessed was a trade secret, constituted confidential or proprietary information or breached an employment contract, confidentiality agreement or non-compete agreement.

The employer need only show that the system was accessed without authorization and caused at least $5,000 in losses. CFAA thus supplements an employer's arsenal but does not replace traditional causes of action.

In addition, employers must have in place effective computer use policies and appropriate restrictive covenants, where enforceable.

1. 6:05-cv-1580-Orl-31KRS (M.D. Fla., Aug. 1, 2006).

2. 18 U.S.C. §1030(g) provides:

> Any 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. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in clause (i), (ii), (iii), (iv), or (v) of subsection (a)(5)(B). Damages for a violation involving only conduct described in subsection (a)(5)(B)(i) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.

3. See Senate Rep. No. 104-357, §IV(1)(E) (1996 WL 492169).

4. 231 F.3d 1207 (9th Cir. 2000).

5. 119 F. Supp.2d 1121 (W.D.Wash. 2000).

6. 88 F.Supp. 2d 870 (N.D. Ill. 2000).

7. *ViChip Corp. v. Lee*, 2006 WL 1626706 (N.D.Cal., June 9, 2006).

8. 440 F.3d 420 (7th Cir. 2006).

9. 274 F.3d 377 (1st Cir. 2001).

10. See note 9.