

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

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.

Section 1030(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

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.

INTERNET ISSUES



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 Shurgard. 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

