

The Computer Fraud and Abuse Act

Holding Employees Accountable for Computer Fraud

By Christopher Hitchcock and Amber W. Locklear

In a recent decision written by Judge Richard Posner, The United States Court of Appeals for the Seventh Circuit determined that the Computer Fraud and Abuse Act (CFAA) may be used to bring a private cause of action against a former employee who permanently erased confidential data from his company-issued laptop before returning it to the company. *International Airport Centers, L.L.C. v. Citrin*, (Slip Op.) No. 05-1522 (7th Cir. March 8, 2006). In so holding, the Seventh Circuit has joined the current tide of federal courts that have permitted companies to use the CFAA as a means with which to defend themselves against the malicious and competitive acts of departing employees.

Since passing the CFAA in 1984 to

Christopher B. Hitchcock, a partner at Ohrenstein & Brown, LLP, concentrates his practice in business litigation and professional liability with a focus on employment issues, trade secret disputes, insurance coverage matters, shareholder claims and breach of contract actions. **Amber W. Locklear**, an associate with the firm, focuses her practice in commercial litigation.

criminalize “classic” attacks on government computer databases by hackers, Congress has expanded its scope to include a private right of action covering not only government-owned computers, but also “protected computers” used in interstate commerce. (According to the CFAA’s express terms, a “protected computer” is defined as one that “is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States.” 18 U.S.C. § 1030(e)(2)(B).) As a result, individuals and companies may now bring civil claims alleging violations of the CFAA to seek compensatory damages, injunctive and other equitable relief.

The CFAA’s scope has also been extended beyond computer hacking activities to encompass all manner of sins. Plaintiffs have sued individuals under the CFAA for placing “cookies” on a business’s computers in order to gather personal and confidential information, *see, eg, In re Doubleclick Privacy Litig.*, 154 F. Supp. 2d 497 (S.D.N.Y. 2001), for infecting a business’s e-mail network with unsolicited commercial bulk

e-mails (*ie*, “spam”); *America Online, Inc. v. National Health Care Discount, Inc.*, 121 F. Supp. 2d 1255, 1267 (D. Iowa 2000) and for taking confidential and proprietary information from a former employer’s computers for delivery to their new employers, *see, eg, Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*, 199 F. Supp. 2d 1121 (W.D. Wash. 2000).

FOUR ELEMENTS OF PRIVATE RIGHT OF ACTION

To bring a civil claim under § 1030(a) of the CFAA, a party must establish that:

- the defendant intentionally accessed a protected computer,
- without authorization or in excess of their authorization,
- to commit one of the enumerated categories of misconduct:
- theft of computer data;
- unauthorized access of a protected computer with the intent to defraud;
- unauthorized access of a computer resulting in damage to that computer;
- trafficking in computer passwords;
- extorting any money or other thing of value by threatening to cause damage to

- a protected computer; and
- the conduct resulted in at least \$5000 in damages within a 1-year period

MAKING THE CASE

In *International Airport Centers*, IAC hired Jacob Citrin to identify potential real estate properties for the company and to assist it in acquiring those properties. In order to collect data on prospective properties, IAC lent Citrin a laptop computer to use in the course of his employment. After working for IAC for several years, Citrin decided to quit his job in order to start a competing business, in breach of his employment contract with IAC. Before returning the laptop to IAC, Citrin loaded a secure-erasure program, and permanently erased all of the data on it — including the data he had collected in the course of his employment, and presumably, evidence of his disloyalty in planning a competing business while still working for IAC. In this case, the Sixth Circuit simply assumed without discussion that the company-issued laptop IAC loaned to Citrin was a “protected computer” within the meaning of the CFAA.

In deciding on Citrin’s use of the protected computer to be “without authorization or exceeding authorization,” Judge Posner noted that Citrin’s authority to access the laptop was based solely on his employment relationship as an agent of IAC. Accordingly,

when he uploaded the secure erasure program onto his company-issued laptop for the purpose of deleting his employer’s confidential information, his agency relationship terminated, and he was completely “without authorization” to access the information stored on the company’s computer.

In proving Citrin’s misconduct, the IAC relied on the CFAA provision that deals with unauthorized access of a computer resulting in damage to that computer, specifically, “whoever 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.” The court noted that Citrin’s transmission of “a program intended to cause damage” to a computer’s files met the CFAA requirement of damage which includes “any impairment to the integrity or availability of data, a program a system or information.”

Finally, in addition to the elements listed above, a plaintiff must also prove that defendant’s misconduct resulted in at least \$5000 in damages within a 1-year period. Under the statute, “loss” is defined as “any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program system, or information to its condition prior to the offense, and any

revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.” 18 U.S.C. 1020(e)(11). It is important to note that while the \$5000 jurisdictional threshold is met in a majority of cases, lost revenue is a “loss” as defined by the CFAA only when the revenue is lost as a result of an interruption of service — for example, when a company’s network is damaged or impaired. *Nexans Wires SA v. Sark-USA, Inc.*, 2006 U.S. App. LEXIS 3619 (2d Cir. 2006).

PROTECTION UNDER THE LAW

Individuals and companies can look to the expansive reading of the CFAA by the Seventh Circuit as welcome news in the defense against computer crimes by known and unknown attackers. As companies rely more and more on computers to create and store intellectual property and proprietary work product, the CFAA offers protection to safeguard the information on which business is built.



This article is reprinted with permission from the September 2006 edition of the LAW JOURNAL NEWSLETTERS - EMPLOYMENT LAW STRATEGIST. © 2006 ALM Properties, Inc. All rights reserved. Further duplication without permission is prohibited. For information, contact ALM Reprint Department at 800-888-8300 x6111 or visit www.almreprints.com. #055081-09-06-0003

OHRENSTEIN & BROWN

www.oandb.com