

THE ISON LAW GROUP
Workplace Law
3220 "M" Street
Sacramento, California 95816-5231
Telephone: (916) 492-6555
Facsimile: (916) 492-6556

**EMPLOYEES MAY BE LIABLE UNDER FEDERAL LAW
FOR DELETION OF COMPUTER FILES**

Recently, a Federal Court of Appeals in a 3-0 decision written by Judge Richard Posner held that an employee who permanently deletes company data on a computer provided by the employer may be liable under the federal Computer Fraud and Abuse Act (CFAA), 18 U.S.C. §§ 1030 et seq.

The Seventh Circuit's decision in *International Airport Centers, L.L.C. v. Citrin* Case No. 05-1522, 2006 U.S.App.LEXIS 577 (7th Cir. March 8, 2006) provides employers with a means to go after employees who leave employment with an intent to damage the employer and provides protection to employer's computers and electronic information.

Employee Deletes Critical Company Files

In this case, International Airport Centers (IAC), engaged in the real-estate business, hired Jacob Citrin to help it identify properties that IAC might want to acquire. IAC lent Citrin a laptop "to record data" that he collected in the course of identifying potential acquisition targets.

While still employed, Citrin, in breach of his employment contract, "decided to quit and go into business for himself." Before returning the laptop to IAC, he deleted all the data in it - - not only the data that he collected, but also data that would have revealed to IAC improper conduct on Citrin's part prior to his resignation. Citrin did not simply delete the files by pressing the "delete" key on his computer. Instead, he used a "secure eraser program" to permanently delete the files and prevent their recovery.

Permanently Deleting Files Through Secure Eraser Programs

Citrin used a trace remover program or tool often referred to as a "secure eraser program." These programs are also sometimes referred to as "disk wipes." They permanently delete files from a computer and prevent them from being recovered.

Secure eraser programs are frequently used for their security and privacy benefits. These programs allow an individual or company to, for instance, transfer a computer or storage media to another user without revealing any confidential files. They are also used to limit the loss of confidential data if a computer is improperly accessed.

Computer Fraud and Abuse Act Applied To Employee

IAC sued Citrin alleging, in part, that he had violated the CFAA. The CFAA is an “anti-hacker” law that was designed to punish computer hackers. It punishes those who distribute damaging software, such as viruses and worms, and punishes unauthorized access to computer systems.

CFAA imposes liability on an individual who “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.” 18 U.S.C. §1030(a)(5)(A)(1).

The main issue in the case was whether there was a “transmission” within the meaning of the law. Citrin argued that erasing a file from a computer does not constitute a “transmission.” He argued that he had not used a virus, worm, or any other kind of attack on the computer system.

The Seventh Circuit disagreed holding that the secure eraser program was transmitted to the computer, under the meaning of CFFA, regardless of whether it was downloaded from the Internet or inserted through a disk into the computer’s disk drive. The court found the distinction irrelevant, noting that “[i]n neither the Internet download or the disk insertion, a program intended to cause damage ... is transmitted to the computer electronically.” Citrin had clearly caused damage to the computer.

The court did agree with Citrin that “it might be stretching the statute too far” to consider any deletion to be a transmission under the statute. “ Pressing a delete or erase key in fact transmits a command, but it might be stretching the statute too far (especially since it provides criminal, as well as civil sanctions for its violation) to consider any typing on a computer keyboard to be a form of "transmission" just because it transmits a command to the computer.”

However, Citrin’s conduct went beyond this by either downloading a secure eraser program from the Internet or inserting the program from a disk. In either case, a program intended to cause damage is transmitted to the computer electronically.

Congress Concerned With Preventing Attacks On Company’s Data

The Seventh Circuit noted that in enacting the CFAA, Congress intended to protect from the type of attack committed by Citrin.

“Congress was concerned with both kinds of attack: attacks by virus and worm writers on the one hand, which come mainly from the outside, and attacks by disgruntled programmers who decide to trash the employer’s data system on the way out (or threaten to do so in order to extort payments) on the other,” the ruling held. “If the statue is to reach a disgruntled programmer, which Congress intended ... it can’t make any

difference that the destructive program comes on a physical medium, such as a floppy disk or CD.”

Employee did Not Have Authorization To Destroy Data

Under the CFAA, liability only exists if the individual causes damage “without authorization.” The perpetrator must also have engaged in "unauthorized access" of the computer in question. A provision in Citrin’s employment contract allowed him to return or destroy data on the laptop when his employment ended. Citrin argued that he was authorized to destroy the data.

However, the court found that it was unlikely that the provision in his employment agreement was intended to authorize him to destroy data that he knew the company had no duplicates of and would have wanted to have—“if only to nail Citrin for misconduct”. Instead, the purpose of the provision may have simply been to avoid overloading the company with returned data of no further value, which the employee should simply have deleted or to remind the employee that confidential information was not to be disseminated after employment was terminated.

Moreover, the court held that Citrin's "... authorization to access the laptop terminated when, having already engaged in misconduct and decided to quit IAC 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 imposes on an employee." *Id.* The Seventh Circuit is the first circuit court to hold that "unauthorized access" is established when an employee accesses a computer for a purpose that is disloyal or adverse to his employer.

The court held that Citrin violated the CFAA.

Statute Provides Criminal And Civil Penalties

This decision sends a warning to employees considering trashing a company’s computer files, and provides a means for employers to take on disgruntled employees who delete their data.

The decision is from the Seventh Circuit, not the Ninth Circuit. However, it interprets a federal law and was written by Judge Richard Posner, a highly influential jurist.

Employers who suffer damage or loss due to an employee’s violation of CFAA may maintain a civil action against the employee to obtain compensatory damages and injunctive relief. Some courts have also allowed claims under the CFAA for misappropriation of trade secrets.

The statute also provides for criminal penalties and injunctive remedies.

Tips for Employers

Employers should:

- Review and revise their policies and procedures regarding use of all electronic resources, including company computers;
- Ensure that company policies and procedures address data security, authorization and access, and preservation of records and privacy;
- Keep in mind the CFAA when departing employees cause damage by deleting files.

Elizabeth R. Ison is a principal with THE ISON LAW GROUP, a law firm specializing in all aspects of workplace law. Among other specialties, Ms. Ison conducts neutral workplace investigations, acts as an expert witness with respect to human resource compliance issues and conducts all forms of corporate training. Call (916) 492-6555, or e-mail Ms. Ison at eison@theisonlawgroup.com.