

PROTECTING YOURSELF WHILE PROTECTING YOUR COMPUTER DATA: TWO LAWS MAKE IT MORE IMPORTANT THAN EVER

NICK AKERMAN

In the not too distant past, industrial espionage consisted of photocopying and carting out files; and identity theft, a rare crime until recent years, happened when someone lost his or her wallet to a pickpocket. The computer and the Internet have dramatically changed the playing field. Now, customer lists, marketing and strategic plans, and financial information can be passed to the competition with a simple click of the mouse, and a high-school hacker can break into computers that store a wealth of personal information.

Two laws — one passed earlier this year and the other just being discovered as a deterrent to computer theft — when taken together, not only require organizations to be responsible custodians of personal data stored in their computers, but also make the theft of data from a computer a federal crime that can be vindicated through a civil lawsuit.

In response to these two laws, companies should take a number of prudent measures to make certain they can comply with the laws and also take advantage of them should they be the victim of computer theft.

THE CALIFORNIA IDENTITY THEFT STATUTE

The new California identity theft statute,¹ effective since July 1, 2003, requires businesses operating in California to notify individuals when they have reason to believe an individual's personal information — social security number, driver's license number, etc. — maintained as computer data has been stolen. Specifically, the statute provides that any business or person that "maintains computerized data that includes personal information that the person or business does not own ... [to] notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably

IN THIS ISSUE

- **Protecting Yourself While Protecting Your Computer Data: Two Laws Make It More Important Than Ever**
- **Who Guards the Computer Security Guards?**
- **Information Security Governance Reporting**
- **Is Wild Larry Now Crazy Larry?**
- **Of Interest**

Editor
PETER T. DAVIS, CISA, CISSP

Editor Emeritus
BELDEN MENKUS, CISA



believed to have been, acquired by an *unauthorized person*.”² [emphasis added]

Nowhere in the statute is “unauthorized person” defined. The statute also expressly provides that individuals who are damaged by the failure to provide the notice required by the law have the right to bring damage suits to recover for any losses caused by the failure to provide the required notifications. Violations of the statute can also result in class action lawsuits and injunctive relief.³

The purpose behind the California statute is to provide sufficient notice to individuals whose personal information has been stolen by an unauthorized person so they can take the appropriate steps to prevent the information from being used by data thieves. In enacting this statute, the California Legislature recognized that “[i]dentity theft is one of the fastest growing crimes committed in California” and that “[c]riminals who steal personal information such as social security numbers use the information to open credit card accounts, write bad checks, buy cars, and commit other financial crimes with other people’s identities.”

While the jurisdiction covered by this statute is limited to California, the statute’s implications extend far beyond that state’s borders. The statute does not just apply to businesses located in California but to any business “that conducts business in California.”⁴ Indeed, there are few major businesses in the United States that do not have customers or conduct business relations in California. In addition, California’s Senator Diane Feinstein has introduced a bill in Congress to make the requirements of this California statute national law.

THE FEDERAL COMPUTER FRAUD AND ABUSE ACT

In contrast, the Computer Fraud and Abuse Act (CFAA), rather than imposing obligations on the custodians of computer data, is a federal criminal statute designed to protect computer data from theft. Enacted in 1984, the CFAA began as an exclusively criminal statute, designed to protect classified

THE STATUTE DOES NOT JUST
APPLY TO BUSINESSES
LOCATED IN CALIFORNIA BUT
TO ANY BUSINESS “THAT
CONDUCTS BUSINESS IN
CALIFORNIA.”

If you have information of interest to EDPACS, contact Richard O’Hanley, Publisher, Auerbach Publications, 29 W. 35th Street, 7th Floor, New York, NY 10001 (ro’hanley@crcpress.com). EDPACS (ISSN 0736-6981) is published monthly by Auerbach Publications, CRC Press LLC, 2000 NW Corporate Blvd., Boca Raton, FL 33431. Periodicals postage is paid at Boca Raton and additional mailing offices. The subscription rate is \$245/year in the U.S. Prices elsewhere vary. Printed in USA. Copyright 2003 EDPACS is a registered trademark owned by CRC Press LLC. All rights reserved. No part of this newsletter may be reproduced in any form — by microfilm, xerography, or otherwise — or incorporated into any information retrieval system without the written permission of the copyright owner. Requests to publish material or to incorporate material into computerized databases or any other electronic form, or for other than individual or internal distribution, should be addressed to Auerbach Publications, Editorial Services, 2000 NW Corporate Blvd., Boca Raton, FL 33431. All rights, including translation into other languages, reserved by the publisher in the U.S., Great Britain, Mexico, and all countries participating in the International Copyright Convention and the Pan American Copyright Convention. Authorization to photocopy items for internal or personal use, or the personal or internal use of specific clients may be granted by CRC Press LLC, provided that \$20.00 per article photocopied is paid directly to Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923 USA. The fee code for users of the Transactional Reporting Service is ISSN 0736-6981/03/\$20.00+\$0.00. The fee is subject to change without notice. For organizations that have been granted a photocopy license by the CCC, a separate system of payment has been arranged. Product or corporate names may be trademarks or registered trademarks, and are only used for identification and explanation, without intent to infringe. POSTMASTER: Send address change to EDPACS, Auerbach Publications, CRC Press LLC, 2000 NW Corporate Blvd., Boca Raton, FL 33431.

information maintained on government computers and financial records or credit information maintained on financial institution computers. In 1994 and 1996, the U.S. Congress amended this act, broadening it to cover all computers used in interstate commerce. At the same time, Congress provided for private civil actions to help anyone injured by the criminal activity this statute prohibits. In October 2001, Congress broadened the CFAA to include any computer “located outside the United States that is used in a manner that affects interstate or foreign commerce or communication in the United States.”

The effectiveness of the CFAA as a broad device to protect computer data is because it embraces multiple civil causes of action, which fall into four main categories: (1) obtaining information from a computer through unauthorized access, (2) trafficking in a computer password that can be used to access a computer, (3) transmitting junk mail known as *spam*, and (4) damaging computer data. The CFAA allows a company victimized by the theft and destruction of computer data to seek injunctive relief from the courts to obtain the return of the stolen data and to prevent the stolen data from being used against it in competition in the marketplace. Despite the fact that the CFAA has provided for civil relief since 1994, it was not until recently that federal courts around the country have relied upon the CFAA to uphold the right of businesses to protect their business information from competitors.

Like the California identity theft statute, the CFAA is predicated on “unauthorized” access to computers and data.⁵ The definitions contained in the act provide little guidance as to the meaning of “authorization” other than to define the term “exceeds authorized access” to mean “to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter.”⁶

FEDERAL COURT INTERPRETATION OF AUTHORIZATION

However, because the CFAA has been on the books far longer than the California identity theft statute, the federal courts have interpreted the CFAA in a number of significant cases to give breadth and meaning to what is and is not illegal “unauthorized” access to computer data. These precedents are likely to be adopted by the California courts in interpreting the new anti-identity theft statute and will most certainly be followed by the federal courts in interpreting the proposed Feinstein legislation mirroring the California statute, if it is enacted into national law.

These court interpretations present opportunities and challenges to companies that must comply with the California law. This article examines those interpretations, the implications of these court interpretations for complying with the new California statute, and what proactive steps a company can take

*IT WAS NOT UNTIL RECENTLY
THAT FEDERAL COURTS
AROUND THE COUNTRY HAVE
RELIED UPON THE CFAA TO
UPHOLD THE RIGHT OF
BUSINESSES TO PROTECT
THEIR BUSINESS
INFORMATION FROM
COMPETITORS.*

to comply with the California statute and simultaneously position itself to take advantage of the powerful remedies offered by the CFAA to protect its valuable computer data.

In interpreting the CFAA, the federal courts have recognized two categories of unauthorized conduct: (1) those inherent in common law principal/agency relationships and (2) those explicitly established and published by the owner of the computer data. The lack of authorization based on the common law of agency involves the factual scenario that almost every business has at some point confronted — an employee sending valuable company information through the Internet immediately before the employee terminates his or her employment with the company to assume a new position with a competitor.

For example, in *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*,⁷ employees sent trade secret information via e-mail from a Shurgard computer to their new employer, a direct competitor of Shurgard. The defendant competitor argued to the federal district court that the CFAA was inapplicable because, as employees, they had the right to access the company's computer and, as a result, could not have exceeded authorized access, as the CFAA requires. The district court did not agree. Relying on the common law rules of agency, the district court held that the employees' authority ended when they acquired "adverse interests" or committed "a serious breach of loyalty" to their employer. Thus, the court found that these employees "lost their authorization and were 'without authorization' when they allegedly obtained and sent the proprietary information to the defendant via e-mail."

This past summer, the District Court for the District of Columbia rejected an identical attack on a complaint brought under the CFAA in which an employee sent confidential and proprietary company data to his personal Yahoo e-mail account to be used in his new position with a direct competitor and then destroyed the data. [*Deloitte & Touche, LLP v. Pesin*, Civ. Action No. 03-675 (RBW) (D.DC July 7, 2003).]

While this legal precedent is good news for companies that can use the CFAA to retrieve their stolen computer data from disloyal employees who join competitors and enjoin them from using the stolen data to compete against them, it has the opposite effect with respect to the California identity theft statute, in which the company is responsible for notifications if the personal information is taken by an unauthorized person who is one of its own employees. Indeed, the California statute, by its terms, explicitly recognizes that a company employee is not "unauthorized" when he or she is not acting in "good faith." The simplest way to avoid the problem of the disloyal employee under the California statute, and to avoid liability under the statute altogether, is to encrypt all such personal data, scrambling the data systematically and permitting it to be opened strictly through a password. By its terms, the new

THE COURTS HAVE
RECOGNIZED TWO
CATEGORIES OF
UNAUTHORIZED CONDUCT:
(1) THOSE INHERENT IN
COMMON LAW
PRINCIPAL/AGENCY
RELATIONSHIPS AND
(2) THOSE EXPLICITLY
ESTABLISHED AND
PUBLISHED BY THE OWNER OF
THE COMPUTER DATA.

California statute only applies to “unencrypted personal information.”

The federal courts have also found access to be “unauthorized” when rules established and promulgated by the employer or owner of the computer data have been violated. [*US Greenfiber v. Brooks*.⁸] In *Brooks*, the defendant, who was the plaintiff’s former quality control manager, “removed from the computer assigned to her all documents, e-mail files, and Microsoft Office, including the Outlook e-mail program.” In entering the preliminary injunction against the defendant under the CFAA, the court found that the defendant’s taking of the computer data was unauthorized by virtue of the company’s work rules and procedures established to protect the confidentiality of its computer data.

In addition to determining what is unauthorized in the corporate workplace, the federal courts have also opined on what is authorized activity with respect to taking data from public Web sites. An express rule on the Web site prohibiting the use of an automatic robot to download data from the Web site was used by the federal district court in *Register.Com, Inc. v. Verio, Inc.*⁹ to find that the downloading by the defendant lacked authorization and was illegal under the CFAA and justified the entry of a preliminary injunction enjoining such future downloading.

In *Register.com*, the data at issue was customer contact information for domain names registered by Register.com. As an accredited domain-name registrar, Register.com is required to permit online access to names and contact information for its customers “to provide necessary information in the event of domain-name disputes, such as those arising from cybersquatting or trademark infringement.” The database is set up to “allow the user to collect registrant contact information for one domain name at a time by entering the domain name into the provided search engine.”

The defendant, a direct competitor of Register.com, built “an automated software program or ‘robot’” and periodically downloaded all of Register.com’s customer-contact information, so the defendant could solicit those customers for the same Internet services offered by Register.com. The robot’s automatic downloading allowed the defendant to contact Register.com’s customers “within the first several days after their registration,” when they were most likely primed and ready to purchase the related services. In *Register.com*, the district court found that the automated search robot was not “authorized” by the Web site’s terms of use, holding that even if the defendant’s “means of access” to the database would otherwise be authorized, “that access would be rendered unauthorized *ab initio* by virtue of the fact that prior to entry ... [the defendant] knows that the data obtained will be used later for an unauthorized purpose.”

Another case addressing authorization to download data from a public Web site, *EF Cultural Travel BV v. Explorica, Inc.*,¹⁰

THE FEDERAL COURTS HAVE
ALSO OPINED ON WHAT IS
AUTHORIZED ACTIVITY WITH
RESPECT TO TAKING DATA
FROM PUBLIC WEB SITES.

A MORE PRACTICAL WAY TO
PROTECT THE COMPUTER
DATA IS TO ENCRYPT THE
DATA.

relied upon a confidentiality agreement between the employer and a former employee to find lack of authorization in upholding a preliminary injunction under the CFAA prohibiting the use of an automatic robot to gather public pricing data. The data at issue in *EF Cultural Travel* consisted of approximately 154,293 prices for high-school educational tours. The court found that the defendants downloaded and used this pricing data to “gain a substantial advantage over all other student tour companies, and especially EF, by undercutting EF’s already competitive prices on student tours.” In *EF Cultural Travel*, the First Circuit court relied on the confidentiality agreement between the plaintiff and one of the defendants to find that the defendants exceeded authorized access by using the plaintiff’s confidential information to build the robot so it could effectively download all of the plaintiff’s prices.

A number of practical lessons can be drawn from these cases to assist companies in complying both with the new California identity theft statute and in taking advantage of the remedies offered by the CFAA. These cases suggest a proactive program — establishing who is “authorized” to access and use the company’s computer data. Authorizations can be embedded in the computer network and can be promulgated as company rules delineating which employees are authorized or not authorized to access certain sets of data and under what circumstances the data can and should be accessed. These cases also illustrate the importance of being able to prove the unauthorized access of the computer data.

PROTECTIONS BUILT INTO THE COMPUTER NETWORK

First, rules concerning who can and cannot use certain data can be built into the computer network. Password protection, for example, can facilitate a “need-to-know” policy that restricts access to those who need to use particular information in the performance of their jobs. Password restrictions, however, become meaningless when computer data can be copied to a floppy disk or printed in unlimited hardcopies. To avoid these issues, a company might consider instituting a document application that can be adjusted to prohibit printing. However, in most business environments, prohibiting copying is not a practical solution.

Similarly, the copying of information to floppy disks can be prevented by simply disabling and prohibiting the use of floppy drives in the workplace, but this does not stop someone from downloading information to a USB key ring. Of course, another more practical way to protect the computer data, mentioned above and encouraged by the California law, is to encrypt the data.

There are also software solutions now on the market that can assist companies in creating authorizations over specific data in the computer network. For example, Liquid Machines, a company that provides information security management

software and is located in Lexington, Massachusetts, has recently released a product that not only encrypts data, but also regulates from a central point in the company who in the company can access particular data and records while tracking the flow of a document through the network, providing an evidentiary trail of which user accessed, printed, or e-mailed a particular document. Those rights can be revoked at any time, preventing former employees access to sensitive information once they leave the company. This software not only complies with the encryption requirement of the California law, but also provides the evidentiary basis for proving a case under the CFAA or determining whether security has been breached on personal computers that would necessitate the notifications required under the California statute.

COMPANY POLICIES AND PROCEDURES

Companies have enormous options to establish the rules by which employees under various circumstances are entitled to access the company's computer data — for example, work rules, employee handbooks, and compliance policies. As with the restrictions built into the network, the key overriding principle is to limit data to those with a legitimate need to use the information to perform their job functions.

In addition to restricting physical access, rules should be established recognizing that computer data can be easily removed from the workplace by sending it via e-mail through the Internet or copying data to floppy disks. Thus, a business must decide what rules will govern concerning the removal of computer data from the workplace. If company personnel are permitted to work at home, should they be permitted to e-mail work home over the Internet? Will employees be allowed to work on their home computers, over which the company has no control, or will work be limited to company laptops? In many instances, certain company personnel, such as sales people, need to take company data on the road. The answer to these questions is to determine what steps can reasonably be undertaken to protect the data within the confines and demands of the business.

Employee training is a critical part of this process. It is important not only in conveying the rules to the workforce concerning who is entitled to access which computer data and under what circumstances, but also in emphasizing the importance of being vigilant for thefts of personal data so that notices, as the California statute requires, can be provided on a timely basis and appropriate action can be taken to retrieve the stolen data — either through the CFAA or by reporting the theft to law enforcement. With respect to the California identify theft law, employee training is necessary for no other reason than to avoid punitive damages under the CFAA so that a company can show that it acted responsibly and alerted its employees to the company's responsibilities under the act.

*A BUSINESS MUST DECIDE
WHAT RULES WILL GOVERN
CONCERNING THE REMOVAL
OF COMPUTER DATA FROM
THE WORKPLACE.*

THE PROBLEM WITH MANY COMPANYWIDE NETWORKS IS THAT IF THEY CAN DETECT AN INTRUSION INTO THE SYSTEM, THEY DO NOT NECESSARILY HAVE THE ABILITY TO KNOW FOR SURE WHETHER DATA HAS BEEN COPIED FROM THE NETWORK.

As the previously discussed cases also demonstrate, posting rules on a public Web site is important to protect the unauthorized use of a company's data that can be reached through its Web site. For example, in *Register.com, Inc. v. Verio*, the federal district court enjoined the defendant Verio, a competitor of Register.com in Web-based services, from using an automatic robot to download public information about Register.com's customers because the use of such automated robots was expressly forbidden by the terms of use for the Web site. Equally important, as reflected by the *EF Cultural* decision, is a policy requiring all key employees to sign confidentiality agreements that forbid the use of confidential information — most of which is today maintained in computer data — to compete against the employer after employment ends.

PROVING ILLEGAL ACCESS TO THE DATA

Finally, an integral component of any sound data protection program is being able to prove that unauthorized access has occurred and what data was taken, by whom, and when. This is important under the California law because having reason to believe that the personal data has been acquired by an unauthorized person triggers the notification requirement. A company is not going to want to give notice, particularly to customers, when in fact there is no theft of personal information. The problem with many companywide networks is that if they can detect an intrusion into the system, they do not necessarily have the ability to know for sure whether data has been copied from the network. The software mentioned above from Liquid Machines, for example, can definitively answer that question; but, obviously, if it is installed on the network to track personal information, there is no reason not to use the same software to track all the company's valuable computer data to provide the admissible evidence of data thefts that is necessary if a company should decide to take advantage of the civil remedies offered by the CFAA.

In short, most companies right now probably could not comply with the new California statute, nor could they successfully mount a legal challenge to confidential data taken from their computers. The prudent IT executive, working with the general counsel and the company's human resources professional, should address these needs sooner rather than later if they want to protect both their employers and their employer's confidential information. ■

Notes

1. § 1798.82, et seq. of the California Civil Code.
2. § 1798.82b.
3. § 1798.82 (a)(b)(c).
4. § 1798.82 (a).
5. Title 18, U.S.C. § 1030.
6. Title 18, U.S.C. § 1030(e)(6).

7. 119 F. Supp. 2d 1121 (W.D. Washington, 2000).
8. No. Civ. A. 02-2215, 2002 WL 31834009, at *3 (W.D. La. Oct. 25, 2002).
9. 126 F. Supp. 2d 238 (S.D.N.Y. 2000).
10. 274 F.3d 577(1st Cir. 2001).

Nick Akerman, a partner at Dorsey & Whitney in New York City, is an attorney who is an expert in computer fraud and the protection of trade secrets and intellectual property.

WHO GUARDS THE COMPUTER SECURITY GUARDS?

BEN ROTHKE

How do we know we can have confidence in senior staff who are empowered to maintain security? Organizations must have more checks and balances in place to ensure that the guards are not only guarding, but that they are cognizant of what is being guarded and how to appropriately guard it. Computer security is far too valuable to take lightly. Computer security is like insurance — make sure you are covered.

Juvenal's famous quote of *quis custodiet custodes* translates to *who guards the guards?* This is an important question for anyone involved with information systems and network security. A more meaningful question might be: How do we know we can trust the internal infosecurity guards?

Of even greater significance is where senior security and audit staff decide to institute policies and procedures without fully comprehending their implications. If senior staff are not correct with their security paradigm, a false sense of security can exist for the company and the company is then protected behind a false wall of security. Let me explain this concept by sharing an event that transpired at a major international bank in New York City.

A senior audit and compliance manager became nearly obsessed by the fact that members of the technical team could use a protocol analyzer to perform protocol decodes at the data layer. They could, if so desired, capture passwords. It was explained to the compliance manager that if a password is sent over the wire in an unencrypted form, then that password could easily be seen by anyone with a protocol analyzer. It is a well-known problem that applications such as Telnet