LJN LAW JOURNAL NEWSLETTERS

Employment Law Strategist™

Volume 11, Number 1 • May 2003

Electronic Media: The Dark Side

Combating Employee Infiltration of Workplace Systems

By James A. Burstein and William F. Dugan

The proliferation of electronic media in the workplace has greatly transformed business, enabling employees to communicate almost instantly with one another, and with vendors, clients and customers. The fantastic business advantages gained through advanced electronic media, however, can also negatively impact the workplace. Indeed, individuals may use electronic media improperly to infiltrate employer systems — obtaining confidential, proprietary and sensitive information.

The Stored Communications Act

Employers have a variety of legal weapons at their disposal to combat such situations. One avenue they often overlook, however, is the Stored Communications Act. In 1986, Congress passed the Electronic Communications Privacy (ECPA), 18 U.S.S. Sections 2510-2521, which substantially amended Title III of the Omnibus Crime Control and Safe Streets Act of 1968. These provisions are commonly known as the "Wiretap Act." In 1988, Congress further expanded the protections of the ECPA by passing the Stored Communications Act, 18 U.S.C. Sections 2701-2711. The Act provides the following in Section 2701(a):

"Except as provided in subsection (c) of this section, whoever — intentionally accesses without authorization a facility through which an electronic communication service is provided; or intentionally exceeds authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be [subject to civil liability]."

In other words, a person violates the Stored Communications Act by "intentionally *access[ing]* without authorization a facility through which an electronic communication is provided … and thereby obtains … access to a wire or electronic communication while it is in electronic storage in such system." 18 U.S.C. Section 2701(a)(1) (emphasis added).

United States v. Smith, 155 F.3d 1051 (9th Cir. 1998) concerns Richard Smith, who served as Vice President of North American Sales for PDA Engineering, Inc. In his executive position, Smith had access to sensitive information that could directly affect the price of PDA stock. In a series of transactions in June 1993, Smith liquidated his position at PDA. He left voice-mail messages for two co-workers in which he informed them that there was a seven-figure mistake in the PDA budget that would decrease the stock price as soon as the mistake became public knowledge. He also informed these co-workers that he had liquidated all of his stock and that he was going to "short the stock." And, in July 1993, he indeed "sold short" several shares of the company.

Unbeknownst to Smith, another PDA employee, Linda Alexander Grove, had guessed the password to one of the voice mailboxes. Grove accessed the co-worker's voice mail, played the message and then forwarded it to her own voice mailbox. She then called her voice mailbox from home and recorded Smith's message by holding a handheld audiotape recorder to the telephone receiver. Grove disclosed the contents of the audiotape to her PDA superiors. The audiotape was eventually secured by the FBI and used to prosecute Smith for a variety of securities violations.

Smith moved to suppress the contents of the audiotape pursuant to Section 2515 of the Wiretap Act, which provides that "[w]henever any wire … communication has been intercepted, no parts of the contents of such communication and no evidence derived there from may be received into evidence at trial." The United States argued in opposition that the Stored Communications Act applied rather than the Wiretap Act, because the message

continued on page 2

Electronic Media

continued from page 1

was recorded while in storage in the co-worker's voice mail (the Stored Communications Act does not have a suppression provision). The court held, among other things, that "Grove might have violated the Stored Communications Act's prohibition in "access[ing]" by simply making unauthorized use of the [co-worker's] voice-mail password and roaming about PDA's automated voice-mail system, even had she never recorded or otherwise "intercepted" the contents of any given message." *Smith*, 155 F.3d at 1058. (On October 26, 2001, USA Patriot Act, Pub. L. No. 107-56, 115 Stat. 272, amended the Wiretap Act and the Stored Communications Act. The amendments, however, do not affect the *Smith* holding as addressed here.)

In *Giddens v. S & A Restaurant Corp., et al.,* Case No. 97 C 3101, United States District Court for the Northern District of Illinois, the authors were able to effectively utilize the development of the law under the Stored Communications Act to obtain a judgment against a former employee, Rommel Giddens, who accessed S&A's voice-mail system without authorization after his termination. Specifically, Giddens used a confidential code to access S&A's voice-mail system, listened to various voice-mail messages, and recorded selected messages by holding a dictaphone next to his telephone receiver. The recorded messages contained confidential and proprietary S&A information.

Upon receiving the audiotapes in discovery, S&A (and one individual defendant) filed counterclaims against Giddens pursuant to the Wiretap Act and the Stored Communications Act. The court found, among other things, that Giddens violated the Stored Communications Act by accessing and roaming through S&A's voice-mail system without authorization. The District Court awarded S&A and the individual mandatory statutory damages. The Stored Communications Act also provides for punitive damages and reasonable attorneys' fees and costs, which were not sought.

It is clear the Stored Communications Act permits a cause of action against individuals who access employers' electronic systems without authorization. With the increasing frequency of "hacking" electronic systems by former employees and others, employers must be aware that they have a cause of action against infiltrators even if an infiltrator does not read the e-mail or listen to the voice mail. In other words, by accessing the system alone, an infiltrator has violated the Stored Communications Act. Of course, in the case of employees, it is essential that employers have policies and procedures that clearly delineate employees' authority to utilize voice mail and/or electronic mail systems. Without such policies the employer may have no cause action under the Stored Communications Act, as it may be difficult to prove an individual did not have the authority to access the electronic system.

James A. Burstein is of counsel in the labor and employment department of Seyfarth, Shaw's Chicago offices. **William F. Dugan** is an associate in that department.

Employment Law Strategist™

PUBLISHER ..... Marjorie A. Weiner
ASSOCIATE PUBLISHER ..... Sofia Pables
EDITOR-IN-CHIEF ..... Stephen L. Sheinfeld, Winston & Strawn, New York
ASSOCIATE EDITOR ..... Mark A. Konkel, Winston & Strawn
MANAGING EDITOR ..... Wendy Kaplan Ampolsk
MARKETING DIRECTOR ..... Gina S. Waserstein
ART DIRECTOR ..... Claire C. O'Neill-Burke
GRAPHIC DESIGNER ..... Louis F. Bartella

BOARD OF EDITORS

GIL A. ABRAMSON ..... Hogan & Hartson LLP, Baltimore
FRED W. ALVAREZ ..... Wilson Sonsini Goodrich & Rosati, Palo Alto, CA
BARBARA BERISH BROWN ..... Paul, Hastings, Janofsky & Walker LLP, Washington, DC
FRANK CUMMINGS ..... LeBoeuf, Lamb, Greene & MacRae, LLP, Washington, DC
MARK S. DICHTER ..... Morgan, Lewis & Bockius LLP, Philadelphia
ROBERT B. FITZPATRICK. ..... Fitzpatrick & Associates, Washington, DC
DAVID K FRAM ..... National Employment Law Institute (NELI), Washington, DC
BARRY A. HARTSTEIN ..... Vedder, Price, Kaufman & Kammholtz, PC, Chicago
KATHRYN M. HINDMAN ..... Bullard Smith Jerhstedt Wilson, Portland, OR
DOUGLAS B. HURON ..... Heller, Huron, Chertkof, Lerner & Saltzman, Washington, DC
JEFFREY S. KLEIN ..... Weil, Gotshal & Manges, LLP, New York City
WENDY L. KORNREICH ..... PricewaterhouseCoopers LLP, New York City
LANCE LIEBMAN ..... Columbia University School of Law, New York City
MICHAEL G. McQUEENEY. ..... The Coca-Cola Company, Atlanta
CORNELIUS J. MOYNIHAN, JR. ..... Nixon Peabody LLP, Boston
WAYNE N. OUTTEN ..... Outten & Golden LLP, New York City
RUSSELL L. PERISHO ..... Perkins Coie LLP, Seattle
MARK N. REINHARZ ..... Rains & Pogrebin, PC, Mineola, NY
DAVID B. RITTER ..... Altheimer & Gray, Chicago
GUY T. SAPERSTEIN ..... Saperstein, Goldstein, Demchak & Baller, Oakland, CA
LEWIS M. STEEL ..... Steel Bellman Ritz & Clark, PC, New York City
STEPHEN E. TALLENT ..... Gibson, Dunn & Crutcher LLP, Los Angeles
JUDITH P. VLADECK ..... Vladeck Waldman, Elias & Engelhard, PC, New York City

Employment Law Strategist™ (ISSN 1069-3741) is published by Law Journal Newsletters, a division of American Lawyer Media.Telephone: (800) 999-1916 • Editorial e-mail: wendya@palawnet.com • Circulation e-mail: subs@palawnet.com

Employment Law Strategist P0000-232
Periodicals Postage Pending at Philadelphia, PA
POSTMASTER: Send address changes to :
American Lawyer Media
1617 JFK Blvd.,Suite 1750, Philadelphia, PA 19103
Annual Subscription: $269

Published by:
Law Journal Newsletters
1617 JFK Boulevard, Suite 1750, Philadelphia, Pa 19103