New York Law Journal
MATRIMONIAL LAW
WWW.NYLJ.COM
An ALM Publication

MONDAY, JUNE 7, 2004

Technology and the Snooping Spouse

Law Struggles to Keep Pace With the Growing Trend of Using 'Adulteryware'

BY HELENE BREZINSKY AND ROBERT M. WALLACK

A RECENT decision from Westchester County reveals the many issues created by technologically savvy matrimonial clients. In *Berliner v. Berliner*,[1] the husband was accused of using his daughter to install a spyware[2] program on the wife's computer without her knowledge. He was accused of copying various confidential files belonging to the wife and of forwarding others via e-mail attachments to himself and his daughter. When the spyware was discovered and brought to the court's attention, the court took immediate steps to prevent spoliation. The court instructed the parties, their attorneys and computer consultants to proceed directly from the hearing to the husband's office to copy (without reading) the hard drives of the husband's computers and deposit them with the court.

The court further ordered that the husband not communicate with his office prior to the examination of the computers and that his cell phone, and that of his attorney, be held by a court officer during a break in the proceedings. Nevertheless, the husband thwarted the court's orders, contacted his office and daughter, and caused files to be erased before the computers could be inspected. Experts confirmed that files had been destroyed so there was no "smoking gun" revealing the wife's files on the husband's computers.

The decision cites no case law or statute that the husband violated by spying. The spying conduct is set forth as egregious, but lightly punished, as the husband was barred from further discovery and precluded from introducing at trial any evidence for which he could not establish a legitimate source. The major punishment imposed on the husband was for violating the court's order, and for this the court sentenced the husband to 10 days in jail. Did the court conclude that the husband's conduct was not unlawful?

'Adware' and 'Adulteryware'

The widespread use of spy software is a somewhat recent phenomenon and as a result, like with many emerging technologies, legislation defining lawful

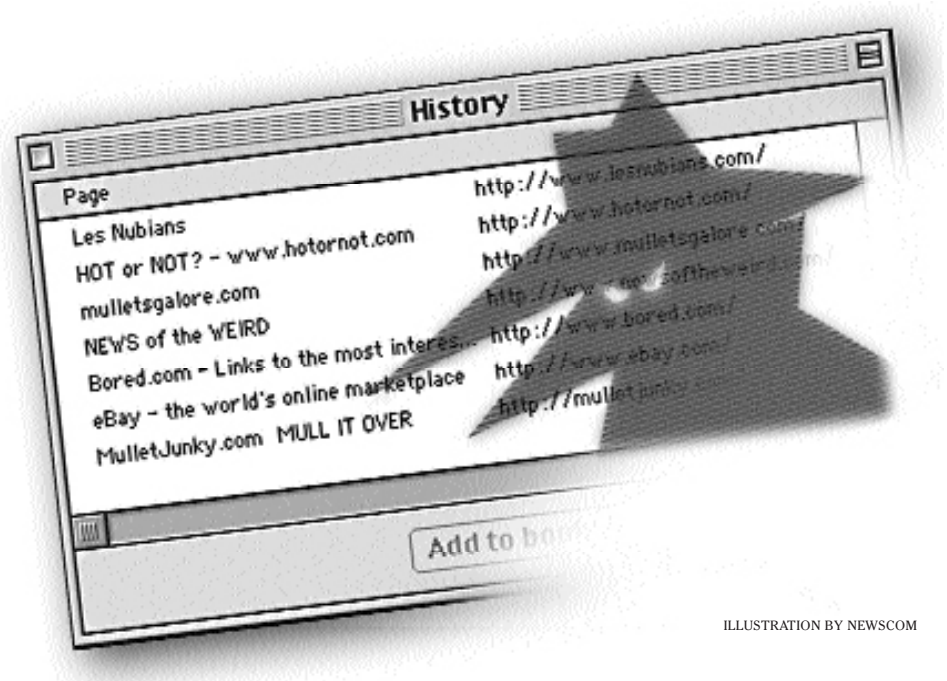

ILLUSTRATION BY NEWSCOM

Helene Brezinsky *is a partner and* **Robert M. Wallack** *is an associate at Kasowitz Benson Torres & Friedman.*

boundaries is struggling to keep pace. "Spyware" is a broad term used to define programs that are surreptitiously installed on a personal computer and which covertly gather user information without the user's knowledge or consent. Spyware is sometimes bundled as a hidden component of free file-sharing software and inadvertently downloaded from the Internet. It exists as an independent, executable program, and as a result, has the ability to monitor keystrokes, scan hard drive files and read a user's e-mail. The software then sends this information back to the spyware's home base or another specified computer, via the user's Internet connection.

There are different types of spyware. Advertiser spyware or "adware" consists of applications that are commonly used for advertising purposes and which utilize a user's information to display pop-up ads on their computer. Perhaps more insidious is computer-monitoring spyware which includes programs that are specifically designed to secretly track and record a computer user's activities. From downloading a hard drive to see what the computer user has saved, to installing software that records all of a user's keystrokes, snooping with "adulteryware," as it has come to be called, is a growing trend.

Companies are even advertising that their software can be useful for catching cheating spouses online. One company that develops and markets such software asks, "Is your spouse cheating on you? You have the RIGHT TO KNOW!" and "Knowing EVERYTHING They Do Online is as Easy as Checking Your Email." Such marketing has proven successful; approximately 50 percent of the company's sales are reportedly made to spouses monitoring other spouses.

One such program can be instantly downloaded and installed on a computer in minutes, and an option reportedly even allows a monitoring spouse to program the software on the target computer without physically gaining access to the computer. Once installed, the spyware records all incoming and outgoing e-mails, and instantly sends a copy to the e-mail address specified by the monitoring spouse. The program acts the moment an e-mail is sent or received and also works with Web- based e-mail services such as Hotmail, AOL and Yahoo!

In addition to the instant e-mail notification feature, the program is supposed to immediately record and forward both sides of chat room conversations and instant messages; record all Web sites visited; record every keystroke typed on the computer; record certain keywords or phrases when they appear on the computer; and record when the monitored computer logs on and logs off. All of this information is then sent to the monitoring spouse in the form of activity reports as frequently as every 30 minutes. The software is completely hidden and runs in stealth mode, and cannot be uninstalled without a password supplied by the monitoring spouse.

Are these computer-monitoring spyware programs legal? As to the intercepting of e-mails, in New York they are not legal.[3] Beyond intercepting and accessing e-mails, does spyware by its existence, installation or operation, violate federal or state law? This becomes grayer. One could reason that installation of such software on another person's computer without his or her permission would be illegal.[4] This raises an interesting question since the purpose of such software is to do just that, to spy on a user without his or her knowledge or consent. Courts will undoubtedly have to confront this and other issues in the future.

On March 23, 2004, Utah became the first state to enact legislation specifically targeting spyware. The law, known as the "Spyware Control Act,"[5] prohibits a person from installing or causing spyware to be installed on another person's computer and bans pop-up ads that interfere with a user's ability to view a Web site. The Utah statute was enacted primarily to deal with "adware," and while it provides for a private cause of action against any person who violates or causes a violation of the statute, a victim cannot bring a lawsuit. Only Web site owners, advertisers and copyright and trademark owners can sue under the act.

New York has also entered the spyware legislation fray. On April 19, 2004, Senator Michael Balboni introduced an act in the New York State Senate to amend the penal law by creating the crime of "Unlawful Dissemination of Spyware."[6] The proposed legislation provides, "A person is guilty of unlawful dissemination of spyware when having no right to do so, he or she uses an executable computer that employs a computer user's internet connection without the computer user's knowledge or explicit permission and such computer program gathers and transmits: (1) personal information or data of a computer user; or (2) data regarding the computer user's computer usage, including, but not limited to, the websites that are or have been visited by the computer user."

The legislation would also amend Penal Law §250.00 and expand eavesdropping to include information that is intercepted by the use of keylogging spyware computer programs. Keylogging computer programs are those "installed without the knowledge of the computer user that send electronic communications, that the computer user is unaware of, from the computer to an unauthorized user. Such communications are computer files that display all of the key strokes that a computer user makes."[7]

There are few, if any, reported decisions addressing the use of spy software in the snooping spouse context. Legislatures and the courts, confronted with these new technologies and seeing a burgeoning trend in this area, are beginning to tackle these issues. Only then will the line between permissible and unlawful conduct in this currently gray area, begin to become apparent.

The Internet and E-mail

The Internet and e-mail have changed the way we live our lives and the way the world communicates. As of September 2001, more than 143 million Americans, or about 54 percent of the population,

were using the Internet, and new users were adopting the technology at a rate of more than two million per month.[8] The number of person-to-person e-mails sent on an average day has dwarfed postal mail and is expected to exceed 36 billion worldwide in 2005.[9]

The prevalence and accessibility of the Internet and e-mail have also aided electronically snooping spouses. Spouses are obtaining information by intercepting and/or accessing the other spouse's e-mail messages. If a spouse uses or retrieves e-mail messages from a home computer to which both spouses have equal access, there is most likely no violation of the law. However, if the computer belongs to one spouse and is password protected or if e-mail messages are retrieved by hacking into a file on a shared computer, or by surreptitiously accessing a Web-based e-mail provider, the spouse who hacks into the computer or retrieves the messages may be subject to civil or criminal penalties.

Congress passed the Electronic Communications Protection Act of 1986 (ECPA) to update and clarify federal privacy protections "in light of dramatic changes in new computer and telecommunication technologies."[10] The ECPA amended Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (the original Wiretap Act), which prior to 1986, only prohibited the eavesdropping and wiretapping of wire and oral communications.[11] Title I of the ECPA (the new Federal Wiretap Act) extended the protection of the original Wiretap Act by prohibiting the "interception" of "electronic communications," and subjects violators to both criminal prosecution and civil penalties.[12] "Interception" as defined by the statute, is "the aural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device."[13] The legislative history surrounding the ECPA makes clear that such "electronic communications"include e-mail messages.[14]

Title II of the ECPA created the Stored Communications Act (the SCA), which protects against unauthorized "access" to "electronic communication while it is in electronic storage."[15] Electronic storage is defined as: "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication."[16] Access merely requires being in a position to obtain the contents of a communication. An individual would, therefore, be in violation of the SCA, simply by gaining unauthorized entry into another's e-mail system, even if that person never reads, prints or downloads a message.

The intersection of these two statutes "is a complex, often convoluted, area of the law,"[17] and "[c]ourts and scholars have struggled to determine the precise boundaries of and also the intended relationship between the [Federal] Wiretap Act and the [SCA]."[18] This discussion requires a basic understanding of how e-mail technology works.

The sending of e-mail is indirect, as all e-mail messages are stored at some point during the transmission process. After a message is sent, the electronic communication system stores the message in intermediate (or temporary) storage while another copy of the message is stored separately for backup protection. The transmission process is completed when the recipient retrieves the message from intermediate storage. After the message is retrieved, it is copied to a third type of storage known as post-transmission storage, where it can remain indefinitely.[19]

Since the passage of the ECPA, there has been discussion about when an "interception" occurs. Some federal courts have held that e-mail cannot be "intercepted" in violation of the Federal Wiretap Act unless the contents of the communication were acquired contemporaneously with the transmission.[20] Under this rationale, "there is only a narrow window during which e-mail interception may occur — the seconds or milliseconds before a newly composed message is saved to any temporary location following a send command. Therefore, unless some type of automatic routing software is used (for example, a duplicate of all … messages are automatically sent to … [another person]), interception of e-mail within the prohibition of the ECPA is virtually impossible."[21]

Likewise there has been debate over the "accessing" of e-mail in electronic storage in violation of the SCA. One view appears to be that "access" must take place before the e-mail reaches post-transmission storage,[22] while other federal courts have held that "access" applies to e-mails in backup storage, regardless of whether it is intermediate or post transmission.[23]

New York State Law

The "interception" or "access" of electronic communications also constitutes the crime of eavesdropping under New York state law. "A person is guilty of eavesdropping when he unlawfully engages in wiretapping, mechanical overhearing of a conversation, or intercepting or accessing of an electronic communication."[24] "Intercepting or accessing of an electronic communication" means "the intentional acquiring, receiving, collecting, overhearing, or recording of an electronic communication, without the consent of a sender or the intended receiver thereof, by means of any instrument, device or equipment…"[25]

While Penal Law §250.05 does not include a specific reference to e-mail, the practice commentary for the statute states that "electronic communication" includes "communications transmitted by ... computers (e.g. electronic mail)."[26] One should, therefore, reasonably conclude that e-mail messages are included, despite the lack of language specifically referencing "e-mail" and the dearth of reported case law interpreting the statute to include e-mail.

Although this statute does not provide a private cause of action, the contents of any intercepted communication, or evidence derived therefrom, which has been obtained through eavesdropping as defined by §250.05 of the penal law,

may not be received in evidence at any trial, hearing or proceeding.[27]

Unlike New Jersey, whose Wiretap Act is identical to the ECPA,[28] New York does not differentiate between the "intercepting" and "accessing" of an "electronic communication," making both actions equally culpable under Penal Law §250.05. Moreover, New York's statute does not contain an explicit contemporaneous transmission requirement and does not mention "electronic storage." While it appears that Penal Law §250.05 is more stringent than the ECPA in this context, it has not been extensively applied or interpreted as applicable to e-mail.

Additionally, Article 156 was added to the Penal Law in 1986 to "deal with the evolving and diversified forms of crimes involving computers."[29] Penal Law §156.05 provides that: "A person is guilty of unauthorized use of a computer when he knowingly uses or causes to be used a computer or computer service without authorization and the computer utilized is equipped or programmed with any device or coding system, a function of which is to prevent the unauthorized use of said computer or computer system."[30]

The statute on its face does not make criminal the mere use or accessing of a computer system without permission or authority. Instead, the Legislature added the additional requirement that the computer be equipped with a system designed to prevent the unauthorized use of the computer, such as a password requirement or a lock. This requirement was incorporated into the law to "encourage greater self-protection on the part of the computer industry."[31]

There exists a statutory defense to Penal Law §156.05 which permits individuals who act without authorization to be absolved from criminal liability if they had reasonable grounds to believe that they were authorized to use the computer.[32] Thus, it is important that constructive notice of a person's lack of authorization be given in the form of oral or written instructions, a posted written notice adjacent to the computer, or a notice displayed on, printed out on or announced by the computer.[33]

Attorneys beware. The Code of Professional Responsibility expressly prohibits a lawyer from counseling or assisting a client in conduct the lawyer knows to be illegal.[34] Remember that a person is criminally liable for the conduct of another, when, acting with the required mental culpability, he solicits, requests, commands, importunes, or intentionally aids such person to engage in such conduct.[35] In the exercise of caution, a lawyer should never advise a client to install spyware on a spouse's computer without the spouse's consent. Likewise, a lawyer should not counsel a client to furtively intercept or access a spouse's e-mail messages. If there are discovery requests for such material, further care is required.

If a client appears in a practitioner's office and reports that he or she has already done one or both of these things, the client may be in violation of federal or New York State law, and any evidence obtained by the client through eavesdropping will likely be suppressed. While the client will be angry that you refuse to use it, as *Berliner* reveals, the consequence of use may be worse.

•••••••••••••●●●•••••••••••••

1. NYLJ, May 11, 2004, pg. 19.

2. A computer-monitoring spyware program called "Home Key Logger," which recorded all keystrokes made on the computer, was installed on the wife's computer in the *Berliner* case.

3. See PL §250.05.

4. See www.spycop.org.

5. Utah Code 13-39-201, 2004 Ut. HB 323.

6. See New York State Bill S07141, April 19, 2004. The crime would be a Class A Misdemeanor.

7. See Id.

8. CNN, Feb. 6, 2002; see also Nielsen//NetRatings, April 29, 2004.

9. See "Email Mailboxes to Increase to 1.2 Billion Worldwide by 2005," CNN.com, Sept. 19, 2001.

10. Allan H. Zerman and Cary J. Mogerman, "Wiretapping and Divorce: A Survey and Analysis of the Federal and State Laws Relating to Electronic Eavesdropping and their Application in Matrimonial Cases," 12 J. Am. Acad. Matrim. Law. 227 (1994), quoting S. Rep. No. 541, 99th Cong., 2nd Sess. 5 (1986).

11. See 18 USC §2511(1)(a).

12. Id.

13. See 18 USC §2510(4).

14. See 1986 USCCAN 3555, 3568.

15. See 18 USC §2701.

16. 18 USC §2510(17)(A) & (B).

17. *U.S. v. Smith*, 155 F.3d 1051, 1055 (9th Cir. 1998).

18. *Fraser v. Nationwide Mutual Insurance Co.*, 135 F.Supp.2d 623, 633 (E.D. Pa. 2001), aff'd 352 F.3d 107 (3d Cir. 2003).

19. Id.

20. See e.g. Id.; *Steve Jackson Games, Inc. v. U.S. Secret Service*, 36 F.3d 457 (5th Cir. 1994).

21. Jarrod J. White, "Email@Work.com: Employer Monitoring of Employee E-Mail," 48 Ala.L.Rev. 1079, 1083 (1997).

22. See *Fraser*, 135 F.Supp.2d at 636.

23. See e.g. *Theofel v. Farey-Jones*, 341 F.3d 978 (9th Cir. 2003).

24. See PL §250.05.

25. See PL §250.05(6).

26. William C. Donnino, Practice Commentary for PL §250.05 (McKinney 2000) at 481.

27. See CPLR §4506(1).

28. See N.J. Stat. Ann. §§2A:156A-1 to -34; *White v. White*, 781 A.2d 85 (N.J.Super. 2001) (wife's retrieval of her husband's stored e-mail from the hard drive of a family computer for use in a custody dispute did not violate the New Jersey Wiretap Act since the messages were in post-transmission storage and thus were not "intercepted").

29. William C. Donnino, Practice Commentary for Article 156 of PL (McKinney 2000) at 281.

30. PL §156.05.

31. Id. at 284.

32. See PL §156.50(1).

33. See PL §156.00(6)(a),(b) & (c).

34. 22 NYCRR §1200.33 [DR 7-102].

35. See PL §20.00.