PHILADELPHIA, FRIDAY, APRIL 3, 2009

The Legal Intelligencer

THE OLDEST LAW JOURNAL IN THE UNITED STATES

An incisivemedia publication

PROFESSIONAL CONDUCT

# When Clients Conduct E-Discovery, Can You Use What They Find?

**BY ELLEN C. BROTMAN AND MICHAEL B. HAYES**
*Special to the Legal*

E-mail has made it easier to communicate with more people, more quickly and more informally than ever before. We find ourselves in e-mail "conversations" divulging information that we used to reveal only in-person and under the strictest confidence. We incorrectly believe that we're in a private space and, as a former senator recently learned, when that private space becomes public, it can be more than embarrassing. Our clients' access to information through review of an opposing party's e-mails is the subject of our column this month.

Let's get right to our hypothetical: A suspicious wife accesses her husband's personal e-mail account on their mutually owned computer by using a password he created for some of their other accounts. Her review of the e-mails proves that he has not been the faithful husband she thought he was. Wife files for divorce and forwards e-mails to you, her lawyer.

Can you use those e-mails as proof in your case, or should you be worried about possible criminal charges for you or your client? How about possible disciplinary charges for you? Is the answer different if the password is not one they both used before but a secret password that the wife successfully guessed? Is it different if the computer is in his home office? Is it different if his home office computer is used for family bills? Is it different if it's his laptop and not the home computer?

BROTMAN HAYES

**ELLEN C. BROTMAN** *is a partner with Montgomery McCracken Walker & Rhoads and a member of its white-collar crime and government investigations group and chairwoman of its professional responsibility group, after several years of being a principal in the firm of Carroll & Brotman. Brotman is also a former assistant federal defender with the Philadelphia Community Defenders Organization.*

**MICHAEL B. HAYES** *is a partner with the firm and is a member of the firm's professional responsibility practice group. Prior to joining the firm, Hayes served as a law clerk to Justice Russell Nigro of the Pennsylvania Supreme Court.*

Let's talk about the Rules of Professional Conduct that are implicated by these scenarios. It's clear that you have an ethical obligation under Rule 4.4(b) of the Rules of Professional Conduct (Respect for Rights of Third Persons) to avoid using any "methods of obtaining evidence that violate the legal rights" of others. Therefore, you cannot use anything that was obtained in violation of either a criminal or civil law.

If you conclude that the evidence was illegally obtained, Rule 3.3 (Candor Toward the Tribunal) provides that: "A lawyer who represents a client in an adjudicative proceeding and who knows that a person … has engaged in criminal or fraudulent conduct related to the proceeding shall take reasonable remedial measures, including, if necessary, disclosure to the tribunal." In an extreme case, your duties under Rule 3.3, can even trump the client confidentiality protections afforded under Rule 1.6. However, "reasonable remedial measures" are easily taken by persuading your client not to use the wrongfully obtained e-mails.

Rule 4.1 (Truthfulness in Statements to Others) may also be at issue. This rule requires lawyers to disclose material facts to third persons in connection with a representation whenever necessary to "avoid aiding and abetting a criminal or fraudulent act by a client, unless disclosure is prohibited by Rule 1.6." Of note, Rule 1.6(c)(2) does not prohibit the disclosure of information relating to the representation of a client that the lawyer reasonably believes is necessary in order to "prevent the client from committing a criminal act that the lawyer believes is likely to result in substantial injury to the financial interests or property of another." Is violation of privacy a "substantial injury"? We believe it could be, if the violation of privacy proximately causes substantial economic harm.

Now the question is: Has your client violated the law? It's probably clear from the hypothetical and its suggested permutations that we think the answer is "definitely maybe."

The Electronic Communications and Privacy Act, or ECPA, makes it a crime when someone "intentionally accesses without authorization a facility through which an electronic communication service is provided;

or intentionally exceeds an 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." Title II of the act is the Stored Communications Act, which regulates the intentional access of stored electronic communications and records. (Unlike the Wiretap Act, the Stored Communications Act does not provide for exclusion of evidence obtained in violation of the act.)

In Pennsylvania, similar felony offenses are found at 18 Pa. C.S. §§ 7611 (Unlawful Use of Computer); 7613 (Computer Theft); 7614 (Unlawful Duplication); and 7615 (Computer Trespass) — each of which constitutes a felony of the third degree. These state statutes make it a crime to knowingly access without authorization a computer, computer network, telecommunications device or Web site to obtain, alter, delete or copy confidential information, passwords or other data.

The answers to the questions raised by our hypothetical are entirely fact dependent, but we think you'll be able to spot the issues with a simple "gut check." Consider the court's analysis in a relatively early case in New Jersey: *White v. White*. In *White*, the court interpreted the New Jersey Wiretapping and Electronic Surveillance Control Act, N.J.S.A. 2A:156A-1 et seq., and New Jersey's common law right of privacy against intrusion on seclusion. (The New Jersey act is identical to the federal act.)

Defendant wife used an investigator to duplicate and analyze the files from the family computer's hard drive, which was kept in a commonly used room in the home. Among those files were stored files of the plaintiff's e-mails. The court noted that plaintiff had failed to password protect his files and that the e-mails were stored on the home server, not intercepted, or stored on a remote Web server. Based on these factors, and the fact that the computer was not accessed "without authorization," the court concluded that New Jersey's Wiretap Statute was not violated.

As to the right of privacy claim, the court found that New Jersey law requires that the intrusion be "highly offensive" to a reasonable person's expectation of privacy. The court concluded that this expectation did not exist when plaintiff used a computer in a common room in the family home and that both the room and the computer were accessible by everyone in the house. (For a more thorough discussion of these issues that goes well beyond our word limit, see "Marital Cybertorts: The Limits Of Privacy In The Family Computer," published in the *Journal of the American Academy of Matrimonial Lawyers* in 2007.)

While writing this column we received an e-mail from a colleague that we think should be shared publicly. Patricia T. Brennan, a matrimonial lawyer in Chester County, wrote to us about her perspective on these issues: "The bright line for me is that a client should not access any private information on the family computer that they didn't have access to before the separation. I always ask the client about the circumstances under which the private information was found and I strongly discourage my clients from taking steps that will inflame passions and make settlement less likely, or if we need to litigate, will tarnish our credibility before the court."

We couldn't have said it better ourselves! •