

Discovery Unplugged: Should Internal E-mails Be Privileged Confidential Communications?

The concept of appropriate discovery should keep pace with modern communications technology and protect intra-company e-mail

By Ralph Streza

MOST PEOPLE are more comfortable with old problems than new solutions. That notwithstanding, this article argues for the creation of a new communications privilege based on privacy and business policy: An organization's internal e-mail communications related to advancing the goals of the organization should not be discoverable in litigation, provided the organization takes the steps necessary to preserve the privacy of these communications.

DISCOVERING E-MAIL

Generally speaking, corporations, lawyers who represent corporations, lawyers who assert claims against corporations and judges who manage discovery issues related to litigation involving corporations have not questioned the propriety of allowing discovery of a company's e-mail database. It seems natural and logical for the litigation professionals to accept the discoverability of a preserved record of an individual's thoughts, or a group of individuals' exchanged thoughts, within a corporation and related to the advancement of corporate goals.

A search of the Lexis national case law database for federal and state decisions from January 1990 to the summer of 2002 uncovered no decision in which a court considered creating a privilege for internal corporate e-mail. A search of the profes-

IADC member Ralph Streza is a member of Porter Wright Morris & Arthur L.L.P. in the firm's Cleveland office. He is a graduate of Miami University (B.A. 1978) and Cleveland Marshall College of Law (J.D. 1982).

sional journal article database covering 900 leading legal and business journals was similarly unavailing. No effort was evident in pending or abandoned federal legislation.

The evolution of computer technology in the corporate world and in society has contributed to the mindset that e-mail should be discoverable. The decisions sustaining the discoverability of e-mail, however, occurred before the practical effects of allowing that discovery were foreseen, or possibly even appreciated. The time may be ripe to rethink the propriety of invading these communications.

Responding to a discovery request for a corporation's internal e-mail sounds simple until the task begins. A corporation served with a request to produce these electronic communications will soon learn that compliance can be time consuming and very expensive. For instance, President Clinton's chief of staff, John Podesta, in October 2000 estimated that the cost of the effort to reconstruct, retrieve and analyze lost e-mail related to the Monica Lewinsky scandal would exceed \$11 million. The court ordered the defendant to pay the not "undue" estimated cost in excess of \$1 million to retrieve electronic data in civil litigation discovery.¹

In addition to collecting and analyzing e-mail, the production can generate extensive

1. See 1 *Digital Discovery & e-Evidence* at 16 (December 2000). See also *Linnen v. A.H. Robins Co.*, 1999 WL 462015 (Mass.Super.).

spin-off discovery in an effort to leave no stone unturned. An internal information technology staff can be tied up for days or even weeks, according to some treatises. If the IT staff is insufficient, the corporation must outsource the collection and analysis.² The e-mail may pull otherwise unknowledgeable witnesses into the litigation. They may add little, if anything, to the merits of the claims or defenses, yet they are corralled, interrogated and distracted from otherwise productive duties. Instead of uncovering truly relevant facts, e-mail productions prolong and sidetrack the search for truth, and sometimes it may even develop untruth. Some written communications found in e-mail just aren't accurate.

However, apart from these litigation-related costs, which many people argue are simply a cost of doing business, one must ask whether the true social intent, benefit and purpose of e-mail within companies, are advanced or suppressed by its use in civil litigation.

BASIS OF LEGAL PRIVILEGE

Concepts of legal privilege are grounded in private, confidential relationships. Communications made in confidence in these relationships are not protected from disclosure merely because of the confidentiality of the communication, but because of a strong public policy or a public concern that underlies the communication.³ Privileges not to testify create narrow exceptions to the principle that the truth should be ascertained by all rational means.

Scores of articles discuss the new privacy concerns that have arisen with the advent of electronic communications. Most

have centered on the privacy interests of the individual—particularly as people surf the Internet or send their encrypted message into cyberspace expecting it to land in another Internet user's mailbox. But little attention has been devoted to an organization's privacy as it relates to an intra-company e-mail network.

Legal privilege is regulated by Rule 501 of the Federal Rules of Evidence, which provides in pertinent part that the "privilege of a witness, person, government, state, or political subdivision thereof shall be governed by the principles of the common law as they may be interpreted by the courts of the United States in the light of reason and experience."⁴ This rule has not been amended since its adoption in 1972.

When originally submitted to Congress, Article V of the proposed Federal Rules of Evidence, of which Rule 501 is a part, listed 13 specific rules. Nine defined specific non-constitutional privileges, one expressly excluded all privileges not enumerated in Article V, and three addressed waiver issues. Ultimately, Rule 501 was adopted with the view, according to the Advisory Committee Notes, that not only were existing privileges to be applied, but that privileges would continue to develop, in light of reason and experience, and that "the recognition of a privilege based on a confidential relationship and other privileges should be determined on a case-by-case basis."

It seems settled that an organization has a reasonable expectation of privacy in its closed e-mail system implemented to exclude third parties to allow its employees to communicate.⁵ It also is undisputed that

2. *Digital Discovery & e-Evidence*, *supra* note 1, at 4.

3. 81 AM. JUR. 2D *Witnesses* § 286 (1992) states: "It must appear that the element of confidentiality is essential to the full and satisfactory maintenance of the relation between the parties, the relation must be one which in the opinion of the community ought to be sedulously fostered, and the injury that would inure to the relation by the disclosure of the communication must be greater than the benefit thereby gained for the correct disposal of litigation."

4. Many states have adopted the "reason and experience" guideline of Rule 501. Twenty-six states have adopted this rationale, a rule patterned after Article V or similar provisions. 23 CHARLES ALAN WRIGHT & KENNETH W. GRAHAM, JR., *FEDERAL PRACTICE AND PROCEDURE: EVIDENCE* § 5421 (2d ed. 1982 & Supp. 2002).

5. See *Dow Chem. Co. v. United States*, 476 U.S. 227, 236 (1986), *aff'd* 749 F.2d 307 (6th Cir. 1984) (well settled that business that undertakes extensive effort to protect interior of its business from un-

the closed e-mail network belongs to the corporation and not to the employees who use it.⁶ At least one court has determined that the expectation of privacy related to e-mail is linked to the type of e-mail involved and the intended recipient. By negative inference from that decision, the users of a closed network have a much greater privacy right in a closed network.⁷

APPLICATION TO E-MAIL

Accepting the premise that communications given in the closed network are confidential and private, one must remember the goals of e-mail. E-mail is a shorthand way of expressing a thought with the added benefit that the other side of the communication does not need to be present for the thought to be sent or received. E-mail often is a fleeting thought, unintentionally memorialized. While there sometimes is ample time to alter the thought, there is seldom corrective follow-up or retraction.⁸

In a very real sense, an e-mail is, at most, half of a conversation, and its reliability for the truth of its content is suspect for many reasons. For example, in a conversation, there is give and take, feedback in the form of questions, and pauses and voice inflections that provide personal cues to the interpretation of the message. Ideas are often modified or discarded during the conversation. By contrast, in an exchange of e-mail thoughts, when an idea is changed, there is not always a written acknowledgment of that change.

E-mail users often communicate in an informal and casual manner, not taking the care usually invested when writing a formal business document. Users often believe that once a message is communicated and deleted, it disappears forever, much like a telephone call when the communication has ended. As a result, a discovering party may find a variety of candid statements made about company strategies and secrets that would never have been presented on paper.⁹

Even if deleted, e-mail still can be recovered, and if deleted e-mail is requested and produced, consideration must be given to the reason for the deletion. It is quite possible that the person deleting the e-mail changed his or her mind about the content of the e-mail. Yet, an after-the-fact explanation may not be convincing.

Despite its compromised reliability in litigation, intra-company e-mail networks are useful to a corporation. One court has recognized that companies not only incur enormous expense in implementing the technology to stay competitive, they then face substantial expense to produce the data based on a concept of "litigation fairness."¹⁰ E-mail has become as basic to most companies as the telephone, and in most settings has overtaken the telephone as the preferred method to communicate.

Although e-mail discovery has been allowed in civil cases, it is ironic that the same invasion into the content of private conversations—with or without a telephone—generally has not been allowed,

wanted intrusions from public or competitors "has a reasonable, legitimate and objective expectation of privacy within the interior of its covered buildings, and it is equally clear that expectation is one society is prepared to observe").

6. See *Smith v. Pillsbury Co.*, 914 F.Supp. 97 (E.D. Pa. 1996) (company-owned e-mail system belongs to company, not to employees using system, thereby distinguishing situations that involve employees who claim invasion of their privacy when company disciplines or discharges employee for abusing or misusing company e-mail system).

7. See *United States v. Maxwell*, 45 M.J. 406 (C.A.A.F. 1996). In this case, the court analyzed the scope of privacy related to e-mail transmitted via an Internet online service provider (AOL) in a criminal case of distributing child pornography by the defend-

dant under an anonymous screen name.

8. See Connie W. Crook & Rosemary Booth, *Building Rapport in Electronic Mail Using Accommodation Theory*, SOC'Y FOR ADVANCEMENT OF MANAGEMENT J., Winter 1997, at 4: "In electronic communication, the rapidity of response, the jargon and symbols used, and the informality of the message give additional meaning to the communication. Thus, to communicate effectively the author must accommodate the message to the reader by adjusting it to reflect the reader's communication style."

9. Armen Artinyan, *Legal Impediments to Discovery and Destruction of E-mail*, 2 J. LEGAL ADVOC. & PRAC. 95, 96 (2000).

10. In re *Brand Name Prescription Drugs Antitrust Litig.*, 1995 WL 360526 (N.D. Ill.).

and evidence based on that invasion generally is not admissible.¹¹ It is unlawful for anyone to intercept the conversation of third parties with wiretaps or listening devices, unbeknownst to those talking. Such conduct otherwise might give rise to a private cause of action for damages as an invasion of privacy, and in some jurisdictions it is a criminal offense. The "fruit" of a subpoena or request for production of e-mail is fundamentally the same as the fruit of a wiretap or the illegal capture of conversation.

Courts have declined to admit illegally obtained evidence by way of wiretap in civil litigation.¹² Even where the wiretap was authorized by law in the context of a criminal investigation, courts have refrained from allowing civil litigants from discovering the recorded conversation.¹³ No case could be found in which a court issued a wiretap order to help civil litigants discover their claims or prepare their defenses.

NEVERTHELESS, PRODUCTION ORDERED

Despite these issues, corporations have been required and presumably will continue to be required to produce e-mail. The presumption that e-mail should be discoverable and admissible has developed a business mindset that discovery is a factor in a company's decision to employ an internal e-mail communication system: "Technology should be easily adaptable once litigation has begun and discovery or-

ders have been issued. Wise technology decisions may make compliance with discovery smooth and affordable; poor strategic planning can make it onerous and expensive."¹⁴

The production of deleted computerized information is also part of the expense.¹⁵ This has generated extensive efforts to ensure that corporations responsibly manage internal e-mail and other computerized data so that when a discovery request arrives, the company will not have to sift through millions of pages of disorganized data to determine the content of the data. Spoliation of evidence has generated million dollar fines when a company failed to preserve electronic data that harmed a claimant's ability to establish its claims.¹⁶

CONCLUSION

This article is intended to catalyze continued discussions on the benefits and burdens of intra-company e-mail productions. Underlying this rethinking is the question whether our concept of appropriate discovery has kept pace with this communication technology. The search for truth in the civil discovery process existed for many years before the advent of e-mail. The costs and burdens on companies, as well as the arguable defeated purpose of e-mail generally, might outweigh the benefits to have been gained by discovery into intra-company e-mail. If that is the case, then this may require a fundamental rethinking of whether intra-company e-mail should not be included in the litigation process.

11. See *Katz v. United States*, 389 U.S. 347, 353 (1967), *rev'g* 369 F.2d 130 (9th Cir. 1966) (use of eavesdropping devices without warrant violates Fourth Amendment when speaker has reasonable expectation of privacy).

12. See, e.g., *Filosa v. Filosa*, 1991 WL 180392 (E.D. N.Y.). The court relied on the prohibition in 18 U.S.C. § 2515 on the use of illegally obtained wiretap evidence or evidence derived therefrom in "any trial, hearing, or other proceeding in or before any court." See also *United States v. Wuliger*, 981 F.2d 1497 (6th Cir. 1992) (declining to recognize impeachment exception to 18 U.S.C. § 2515 to allow use of illegally obtained wiretap in civil proceedings between private parties).

13. See *In re Motion to Unseal Electronic Surveillance Evidence*, 990 F.2d 1015, (8th Cir. 1993)

(18 U.S.C. § 2517 does not authorize pretrial disclosure of wiretap evidence to private civil litigants). See also *Nat'l Broadcasting Co. v. U.S. Dep't of Justice*, 735 F.2d 51 (2d Cir. 1984) (finding lack of authority to compel government to release recorded tapes to private litigant pursuing civil matter).

14. William DeCoste, *Sender Beware: The Discoverability and Admissibility of E-mail*, 2 VAND. J. ENT. L. & PRAC. 79, 84 (2000).

15. See Gregory I. Rasin & Joseph P. Moan, *Fitting a Square Peg into a Round Hole: The Application of Traditional Rules of Law to Modern Technological Advancements in the Workplace*, 66 MO. L. REV. 793, 799 (2001).

16. See *In re Prudential Ins. Co. Sales Practices Litig.*, 169 F.R.D. 598, 617 (D. N.J. 1997).