Journal of Civil Rights and Economic Development

Volume 16
Issue 3 *Volume 16, Fall 2002, Issue 3*

Article 2

September 2002

Is Email Privacy an Oxymoron? Meeting the Challenge of Formulating a Company Email Policy

Micalyn S. Harris

IS EMAIL PRIVACY AN OXYMORON?

MEETING THE CHALLENGE OF FORMULATING A COMPANY EMAIL POLICY

MICALYN S. HARRIS[1]

INTRODUCTION

Email is wonderful. Fast and effective, its low cost and ease of use have induced many of us to depend on it. We expect that it will be available and functional on demand, and rely on that functionality in conducting our business and personal relations.

Email feels like a telephone call - quick and casual - without the hassle of telephone tag. But however casual and friendly it feels, email creates a document, and that document is likely to be long-lived and may, depending upon the system and steps taken to protect availability, be widely accessible. In a business or other organization, email is likely to be discoverable in connection with litigation.[2] Producing it may be costly. Sheer

 Ms. Harris is Vice-President, Secretary and General Counsel of Winpro Inc., a software consulting and development company with offices in New Jersey and New York City, and a professional arbitrator and mediator. She currently serves on the Executive Committee of the New York State Bar Association's Business Law Section and chairs the Internet and Technology Law Committee, is a member of the Center for Professional Responsibility of the American Bar Association and also co-chairs its Business Law Sections' Subcommittee on Software Licensing, as well as being an elected member of the American Law Institute.

[1] *See e.g.* Micalyn S. Harris, *Email Privacy: An Oxymoron?*, 78 NEB. L. REV. 386 (1999) and materials cited therein.

[2] *See* Simon Waldman, *Beware the Mail Detectors*, THE GUARDIAN (UK), Apr. 29, 1999, at Features 4 (discussing how email has increasingly been used against individuals at trial including Bill Gates in Microsoft anti-trust case); *see also* U.S. v. Microsoft, 165 F.3d 952 (1999).

volume and the need to review and catalog it may have high financial costs, and the ease of proving its precise content may result in additional costs - financial and otherwise. Unlike a telephone conversation, which is ephemeral, subject to the vagaries of memory, and permits explanation in the light of hindsight, email can be reproduced exactly as communicated at the time and may have to be explained in the harsh light of a hostile courtroom. Thus, using email has risks that telephone conversations do not have.

ALL EMAIL IS NOT CREATED EQUAL

All email is not created equal. There may be intranets, which operate only within a company. Such intranets may be either limited to machines within the company and on company premises or they may permit access from outside company premises. If they permit access from outside the company, such access may or may not require messaging across the Internet. Where messages are sent within a single ISP (Internet Service Provider), they do not travel across the Internet. Where they are sent from one ISP to another, they may travel across the Internet. The distinction may be important, because messages moving across the Internet may be exposed to risks of loss of privacy that messages moving within an intranet are not. Use of other alternatives, such as modem-to-modem connections, dedicated lines, encryption, or secure sockets, can reduce the risk of potential loss of privacy. Thus, the characteristics of each system will impact the analysis of the risk of loss of privacy and the available means for reducing those risks.

RISKS AND POTENTIAL RISKS

High on the list of risks is the risk of required disclosure of email messages in response to a discovery request in connection with litigation, and use of email in the context of litigation to prove a case or impeach testimony.[3] Thus, email can, depending upon the point of view, be a gold mine or a land mine.

In either event, the risk runs from merely embarrassing to providing seriously damaging evidence. Email that has not been

[3] *See U. S. v. Microsoft*, 165 F.3d 952 (1999).

thoughtfully handled may be vulnerable to an assertion that it is not covered by the attorney-client privilege, although in New York, by statute, the mere use of email does not forfeit the attorney-client privilege.[4] To date, research discloses no court decisions holding that mere use of email forfeits the attorney-client privilege, but the issue has been raised and discussed, and is worthy of attention.[5]

Ethical issues may also be implicated. An attorney has an ethical obligation to protect client confidences.[6] The potential absence of privacy of email communications has been widely publicized, and some states require or recommend obtaining the informed consent of a client if email is to be used for confidential attorney-client communications.[7]

Also worthy of attention is the fact that the risk of actual disclosure of otherwise privileged or confidential information may be higher when using email than when using a telephone, letter in a sealed envelope or even a fax machine. For example, there is the so-called "oops" effect, when one sends an email to a group rather than one individual member of that group, or to the person below the intended recipient as their names appear on the sender's email address list. Such inadvertent disclosure may waive attorney-client and work product privileges,[8] forfeit trade

[4] *See* N.Y. C.P.L.R. 4548 (McKinney Supp 2001) (stating "[n]o communication privileged under this Article shall lose its privileged character for the sole reason that it is communicated by electronic means or because persons necessary for the delivery or facilitation of such electronic communication may have access to the content of the communication.").

[5] *See* Micalyn S. Harris, *Email Privacy: An Oxymoron?*, 78 NEB. L. REV. 386, 387 n.8 (1999) (noting that in *American Civil Liberties Union v. Reno*, the court stated email is not "sealed" mode of communication, although that court also indicated that use of a notice similar to those commonly found on facsimile messages would be adequate to meet confidentiality protection requirements); *see also* American Civil Liberties Union v. Reno, 929 F. Supp. 824 (E.D.Pa 1996).

[6] *See* MODEL RULES OF PROF'L CONDUCT Rule 1.6 (Lexis 2002).

[7] Ethics opinions in Arizona, Iowa and South Carolina require or suggest client consent in order to maintain attorney-client confidentiality for unencrypted emails. Rule 1.6 of the Model Rules of Professional Conduct also suggests discussion with clients is advisable. MODEL RULES OF PROF'L CONDUCT R. 1.6.

[8] *See e.g.*, Champion International Corp. v. International Paper, 486 F. Supp. 1328 (N.D.Ga. 1980) (finding privilege lost as to privileged documents inadvertently delivered during discovery, but denying right to demand additional documents); Subpoena Duces Tecum v. Fulbright & Jaworski, 738 F. 2d 1367 (D.C. Cir. 1984) (finding voluntary disclosure to SEC waived privilege); In re Sealed Case, 676 F. 2d 793 (D.C. Cir. 1982) (also finding voluntary disclosure to SEC waived privilege); Upjohn Co. v. United States, 449 U.S. 383, 389 (1981) (advising that communications between in-house counsel and corporate employees to secure legal advice from counsel concerning matters within scope of employee's corporate duties and considered "highly confidential" when made and kept

secret protection,[9] and may have adverse implications for attorney-client, employer-employee and other relationships.

Email is available to system administrators - not only the sender and receiver's system administrators, but also any intermediate administrators through whose systems the message may pass. Where messages remain within a single system or ISP, legal obligations of confidentiality are clear. Where, however, messages move through third party systems that may or may not be subject to the obligations imposed on commercial ISPs, obligations of confidentiality are less clear.

Other risks of loss of confidentiality include loss through hacking. Hacking is clearly "interception" and therefore loss of confidentiality resulting from hacking should not implicate either attorney-client privilege or attorney ethics. Hacking has recently been held to include entering a protected web site under false pretenses.[10] Regardless of whether or not hacking implicates attorney-client privilege or ethical rules (and it seems clear that it should not), hacking can result in actual loss of confidentiality, with whatever damages may result there from.

Another risk arises from the possibility of infection from computer viruses. Viruses can threaten not only loss of confidentiality, but also may result in the loss of information and destruction of data.

Use of email has also given rise to a number of human relations (social) issues. These include harassment, libel and creation of a hostile work environment. For example, pulling down suggestive pictures and displaying them on one's computer screen has been likened to putting pin-ups in locker room areas. At least one court has found that office displays of pornographic pictures did create an unacceptable work environment.[11]

Other questions have arisen regarding when and whether employees may use email for personal correspondence and whether employees have reasonable expectations of privacy with

confidential were privileged, with implication that disclosure beyond those who had "need to know" or failure to treat information as confidential had potential to waive privilege).

[9] *See e.g.,* Religious Technology Center et al. v. Netcom On-Line Communication Services, Inc., et al, 1995 U.S. Dist. LEXIS 16184 (N.D. Ca. Sept. 22, 1995).

[10] *See* Konop v. Hawaiian Airlines, Inc., 236 F. 3d 1035, 1042 (9th Cir. 2001), *reh.* Konop v. Hawaiian Airlines, Inc., 262 F.3d 972 (9th Cir. 2001).

[11] *See* Urofsky v. Gilmore, 216 F.3d 401, 431 (4th Cir. 2000) (noting that posting of pornographic material on web sites in state offices has led to workplace disruption and complaints that such sexually graphic matter contributes to hostile work environment).

regard to their email messages. The use of an employer's equipment for personal business may be a problem for employers not only because of harassment, libel and creation of a hostile work environment, but also for a variety of other reasons. For example, such use may decrease employee productivity, may give rise to employer liability for infringement, and may create practical problems by making bandwidth intended for company business unavailable for that purpose.

As a result, many companies monitor employee use of email and/or access to the Web. At this point in time, it is clear that organizations can monitor, especially if they disclose that they monitor or reserve the right to do so. The real question for most is not whether they can, but whether they wish to do so. Monitoring is not without risk. If a company knows about improper behavior, it probably has an obligation to do something about it. Monitoring may provide the company with information it would rather not have, because once it has the information, it may have an obligation to take action which it would rather not take.

Monitoring may also have an unacceptably adverse impact on employee morale and productivity. For example, a company might block certain kinds of use, e.g., Napster, to avoid copyright infringement or inordinate use of bandwidth, or certain sites to avoid social problems, e.g. porno sites or sites that promote Nazism. By so doing, however, a company may also block sites that might be useful to employees. Blocking access to game and shopping sites may prevent loss of employee productivity, but may also generate resentment, or even adversely impact attendance by forcing employees to take time off from work to accomplish tasks that can only done during regular business hours. Thus, while organizations probably have the right monitor and block, particularly if they advise they are doing so or reserve the right to do so, in formulating an email policy, the likely the effect on employee morale is an important consideration.

TAKING STEPS TO MINIMIZE RISKS

1. Educate Management - Disclosure, Good Faith and Fair Dealing

The first step in minimizing the risks of using email is to educate management on the essentials. Establishing email policies requires thought, and effective implementation requires support from the top. Whatever the policy, full disclosure, good faith and fair dealing with employees are essential requirements, and essential to achieving that goal is a clear articulation of email policies.[12]

2. Educate Employees - Hacking, Viruses, Bandwidth and Confidentiality

Employees, too, must be educated. Reducing the risks of hacking may rest primarily with the technical staff, but users can help. Most companies require passwords. Employees who are instructed on how to choose passwords (e.g., use uncommon words or combinations of numbers and words, and upper and lower cases, and avoid using one's own name or other obvious words) and reminded to keep them secret are more likely to enjoy the protection that passwords are intended to provide.

Virus-scanning software can be installed, and should be updated at least monthly. Because many viruses are transmitted via attachments, reminding employees that if they receive an attachment from an unknown person it should not be opened can reduce the risk of infection. Now, however, viruses are now increasingly sophisticated. Some can read an address book and send a message to everyone on it. Thus, as a further precaution, employees should be advised that if they receive a message with an attachment from a person they know but from whom they are not expecting a document, they should call and verify that the

[12] *See* Bourke v. Nissan Corp., YC 003979 (L.A.Super.Ct. 1994) (indicating proper email policy may shield corporation from liability); *see also* Shoars v. Epson America Inc., No. SWC 112749 (L.A.Super.Ct. Mar. 12, 1991).

apparent sender actually sent the message and attachment before opening. More generally, employees should be encouraged to think before opening a document. If a header seems somehow odd, check further before opening the message or any attachment to it. [13]

Employees may also need to be educated about bandwidth. Bandwidth is, essentially, a measure of capacity. Today's college graduates expect that large amounts of bandwidth are always available. Most companies have less bandwidth available than a major university, and if they do have that kind of bandwidth available, it's for business purposes.

Several years ago, the Christmas Tree email, a graphically impressive electronic Christmas card, was popular. Because the graphics were stunning, many people who received the "card" wanted to share it with friends, so the card "made the rounds". In one large law firm, many copies of the message were sent through the firm's email system in a short time. Senders saw the message as a goodwill gesture - and even arguably a business communication. One person sending the message would not have been a problem. Many people sending the message was a problem. The elaborate graphics took up so much bandwidth that the system simply couldn't handle it and continue to handle other business. As a result, a large law firm's email system was brought to a halt for six hours while the system sent out the Christmas card messages.

Experience indicates that users may inadvertently slow even a high-capacity system. For example, on investigating complaints by users of one high-capacity system that its email system had slowed to a crawl, it was discovered that many of its users, knowing that the system was "always on" at a flat rate, were using the system to listen to music via the Internet rather than listening to their radios. Again, no harm was intended. As far as anyone was aware, the additional cost to the organization was zero, because it paid a flat rate for unlimited Internet access.

Streaming audio, however, like heavy graphics, requires large amounts of bandwidth. Widespread use of bandwidth to carry streaming audio left little bandwidth for other communications.

[13] Recently, viruses have become more sophisticated. Under some circumstances, merely opening an email message, without opening the attachment, may cause a system to become infected.

When these users were told about bandwidth, they went back to using their radios. Having a rule or policy wasn't necessary; once they understood that the streaming audio was creating a problem, the problem disappeared.

Participation in chat rooms and bulletin board discussions has also given rise to employer concerns, even when such participation occurs on private equipment and away from the office. Employers are concerned about infringing on employees' First Amendment freedoms, but such concerns need not prevent employers from reminding employees about their obligations of confidentiality and loyalty. Employers, too, have obligations, including obligations of good faith and fair dealing with employees. In the recent case of *Konop v. Hawaiian Airlines*,[14] an employee pilot of Hawaiian used a personal web site to promote election of a competing union to represent Hawaiian's pilots. The web site was protected and entry limited to a list of Hawaiian pilots. Management wanted to find out what was being said on the web site. A management employee falsely identifying himself as a Hawaiian pilot gained entry to the web site on two occasions. One of the pilots whose name the manager used had given permission for its use; the other had not. The court said, in effect, that it did not matter, finding that in both instances, gaining access by falsely representing one's identity constituted "interception" and was therefore improper.[15] Good faith and fair dealing are required on both sides.

3. Provide Practical Suggestions

Providing practical suggestions can reduce risks. For example, one can avoid the "oops" effect by giving unique names to groups, rather than using the name of one member and "et al." Preventing individual and group names from appearing consecutively in an email address book reduces the risk that the group will receive a message intended for only one of its members.

Secure sockets can protect the confidentiality of Internet messages. Using encryption can make message contents unavailable to unintended recipients. Making secure sockets

[14] *See* Konop v. Hawaiian Airlines, Inc., 236 F.3d 1035, 1053 (2001).
[15] *See Konop*, 236 F.3d at 1047.

available and encryption easy to use encourages their use.

Establishing a written email policy can reduce risks by making it clear what, exactly, the company expects. Most company email policies state that company equipment belongs to the company and is to be used for company business, and also specify that email belongs to the company. Such policies should also remind people that email creates a document that is likely to be long-lived, discoverable, and may have to be explained in the harsh light of a hostile courtroom, so messages should be composed accordingly.[16] Advise people that email is monitored, if it is, and if not, that the company reserves the right to monitor.

Some organizations have determined that the risks and burdens of producing email in connection with litigation outweigh the advantages of permitting its use, and have instructed employees in certain areas, e.g. investment bankers, not to use email, period. Thus, a company may want to consider barring use of email altogether.

4. Monitoring

The right to monitor is well established, and monitoring has some advantages. It may have a prophylactic effect - if people know email is or may be monitored, they are less likely to send harassing, libelous, steamy or otherwise offensive messages. If email is monitored and that fact is publicized, it may also avoid claims that employees' privacy has been invaded. When employees have been advised that their email is monitored, or may be monitored, it is clear that employees cannot reasonably expect privacy.

Monitoring also has disadvantages however. Monitoring of attorney-client communications so as to protect assertion of attorney-client privilege may require some planning and restructuring to assure that appropriate attorneys review privileged communications.[17] Review by non-lawyers or lawyers acting in a non-legal capacity may give support to claims by

[16] *See U. S. v. Microsoft*, 165 F.3d 952 (1999) (asserting and showing that confronting key witness with his email messages was devastating at trial).

[17] Upjohn Co. v. United States, 449 U.S. 383, 391-95 (1984) provides a general discussion of the need to limit dissemination of attorney-client communications to assure successful assertion of privilege. *See* Micalyn S. Harris, *Email Privacy: An Oxymoron?*, 78 NEB. L. REV. 386 (1999).

opposing counsel that the email was not treated as attorney-client privileged communication and is therefore discoverable. Monitoring may also result in discovering otherwise unreported problems with which the company, on discovering them, has an obligation to deal. Thus, the advantages must be weighed against the potential disadvantages, and a policy formulated accordingly.

Email policies also need to include policies for document retention and destruction, including handling system back ups that include confidential information so as to protect confidentiality.

SUMMARY AND CHECKLISTS

The above can be summarized in checklists, which are also useful in Formulating and implementing email policies. The first list is focused on the challenge of organizing and establishing an email policy; the second is intended to assist users in developing good habits in connection with using email.

A. A Checklist for Organizing and Establishing an Email Policy

1. Understand how the email/computer system of the organization works. Does it have:

   An intranet for employee communications within the organization that is separate from the system that connects to third party systems, e.g. the Web?

   Facilities for creating password protected areas?

   Facilities for automatic encryption?

   Facilities for establishing secure sockets?

   Firewalls to protect against hackers, and if so, does providing access to employees from outside the system jeopardize the effectiveness of those firewalls?

2. Establish and publicize a written policy with standards for creating email messages.

Educate employee email users.

Explain the basics of the attorney-client and work product privileges and the need to take appropriate precautions to assure that email between attorney and client will qualify for protection from discovery pursuant to applicable rules of evidence.

Explain the basics of trade secret protection and the need to take appropriate precautions to assure that messages containing trade secrets are handled and stored appropriately.

Circulate reminders regularly; tell "horror stories." Merely making copies of policies and procedures available is unlikely to be sufficient.

Remind employees that email creates a document, that the document is likely to be regarded as a business record, and that the standards that apply to creating a paper document also apply to email.

Remind employees that company email is to be used for company business.

Remind employees that email belongs to the company.

Remind employees of the need to take precautions to assure confidentiality of attorney-client communications, communications involving trade secrets and other highly sensitive information.

Remind users that if email is discoverable and provided in connection with litigation, it may have to be explained in the environment of a hostile courtroom.

Advise employees that email is monitored, if it is, and if not, that the company reserves the right to monitor email.

Remind users that email may not remain private, and the

implications of that risk for individual users and for the organization.

3. Explain to employees that use of certain kinds of facilities may create problems for the organization, and therefore the company prohibits or places limitations on certain uses, and limitations on sending and receiving certain kinds of messages. For example:

> Streaming audio requires a lot of bandwidth, and bandwidth is limited. Accordingly, if one wishes to listen to music while working, it is appropriate to use a radio, not one's computer.
>
> Messages heavy with graphics require a lot of bandwidth. Accordingly, personal messages, if permitted, should be brief (to minimize productivity loss) and should avoid heavy use of graphics.
>
> Computer viruses are most often spread through email attachments. Accordingly, email attachments one does not expect should not be opened. If an email message appears to come from a known person but no attachment is expected and the attachment is not instantly identifiable as an expected document, check with the putative sender before opening it. Viruses often "infect" address books, with the result that the apparent sender is a known name.

4. Establish procedures for storing and retrieving email documents, including backup copies. Where confidential information is likely to be included in email, assure that backup copies are handled appropriately. Explain that these procedures are designed to maximize ease of use while minimizing the risks associated with that use, and deserve to (and will) be enforced. Establish procedures for overseeing implementation and ongoing enforcement.

5. Educate clients, customers and suppliers about the organization's email system with a view to reducing inadvertent abuse and assisting them in exercising good judgment regarding

when and how and for what purposes it is appropriate to use email and when, if at all, arrangements for using encryption or a secure socket or another method of communication are advisable.

6. Consider the advantages of encryption and of making it easily available, either by using a public-private key or other encryption scheme, or by using secure sockets for privileged and confidential communications.

7. Consider the advantages of installing a dedicated server for email, and of having a separate, dedicated server for the organization's web site. The cost of the equipment is relatively low, and there are distinct advantages. These include ease of management, the ability to implement security measures (both to protect privacy and to minimize the possibility of unauthorized entry into the system), and the ability to shut down the company's email system (e.g. to deal with a virus or "trojan horse" propagated via email) without bringing other computer-dependent operations to a halt.

B. A Checklist for Email Users

The fundamental principle to remember is that email creates a document. Therefore, the three basic reminders are:

Reread your message

Think before you send

This is a document.

The following more specific questions and reminders, which eventually become habitual, can focus thinking:

1. Is this a document I want to have available for unknown others to see now and into the indefinite future? If not, consider communicating by telephone. Voice conversations are ephemeral; email creates a more or less permanent record.
2. Is this a message that contains information sufficiently sensitive to warrant encryption?
3. Will encryption adequately protect the confidential aspects of the message? Or will the email, even if encrypted, provide

clues to a reader of information I regard as sensitive or confidential, *e.g.*, that possible merger partners are having "conversation"? If so, consider communicating by telephone. The connection by telephone is direct and simultaneous.

Note: Unintended discovery of the content of the telephone conversation would have to involve eavesdropping, via a wiretap, which is illegal in the absence of appropriate legal process.[18] Unencrypted email traveling across the Internet may be subject to legitimate review by unknown third parties if such review occurs when the message is "stored" en route on a system other than the addressee's system prior to being forwarded to the addressee.

4. Is this a document that contains time-sensitive information? If so, consider encryption.

5. To whom is the message being sent?

Have I properly coded the address so that only the intended recipient(s) are listed?

Double-check addressee to assure it is addressed to the intended recipient or group, and not a larger group of which the intended recipient is a member.

6. Is this a message regarding which I wish to be able to assert attorney-client privilege, trade secret status, or other status for which encryption is likely to provide evidence of an intention to handle the message as confidential information?

If so, have I included language, or provided for a password or encryption, or taken other steps to evidence that intention?

Even if the only reason to encrypt is to provide evidence of an intention to handle information as confidential information,

[18] The U.S.A. Patriot Act enacted after September 11, 2001, significantly expanded and eased requirements for obtaining warrants under a variety of laws. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. No. 107-56, §115 Stat. 272. (2001).

consider whether that is sufficient to warrant encryption.

What kind of a record am I building?

If encryption indicates an intention to maintain confidentiality, will my failure to encrypt indicate the opposite?

7. Cultivate consistent habits regarding treatment of confidential information.

CONCLUSION

Email is seductive, and justifiably so. Its speed, ease of use and low cost facilitate business communications. The advantages, however, are not without risks. Education and good email policies can reduce those risks, and assist an organization to make efficient and effective use of its email.