

Watch Your Language: The Risks of E-mail

Contributed by Victor O. Schinnerer & Company Inc.

Revised February 2007

The AIA collects and disseminates Best Practices as a service to AIA members without endorsement or recommendation. Appropriate use of the information provided is the responsibility of the reader.

CONSULT YOUR ATTORNEY

The information herein should not be regarded as a substitute for legal advice. Readers are strongly advised to consult an attorney for advice regarding any matter related to electronic communications.

SUMMARY

Email creates an electronic paper trail that can have serious consequences. Below, the consequences and risks of email are outlined and strategies to mitigate that risk are presented.

YOU HAVE MAIL

E-mail often is used in place of carefully worded, well-considered statements or formal written communication to clients or contractors. Too often, e-mail messages are perceived as instantaneous and ephemeral communication. E-mail messages are distributed—and often redistributed by the recipient—without the sensible review that should precede any professional communication. Even when the authors compose and edit their e-mail with care, they rarely preserve the messages properly. More often, e-mail is preserved in an unintended and unmanaged way.

Liability lurks in other ways as well. Employers have been held liable for employee misuse of e-mail in situations ranging from sexual harassment to copyright infringement, even when the employer had no prior knowledge of the employee's conduct.

E-MAIL IS FOREVER

While e-mail messages often are stored haphazardly and can be difficult to retrieve when needed, they are likely to reappear in the possession of others in a way that can become a prolonged source of cost and agony for professional service firms in disputes ranging from unfair employment practices to professional liability claims.

Redundant backup systems and storage media on mail servers may preserve messages far beyond anyone's memory on media outside the control of either the author or the recipient of the message.

The absence of systematic and verifiable storage and retrieval methods and systems, combined with the mere fact that particular e-mail messages may exist, may give opponents sufficient cause in a legal proceeding to demand, and be granted, access to the complete e-mail archive of an organization.

Among the many types of information stored electronically that could be discoverable in a legal proceeding, e-mail messages are often of the greatest concern. Too often, e-mail authors may be trying to cover their tracks with a casual, transient message. Instead, they are creating an electronic paper trail—date- and time-stamped—that can have serious consequences. Such messages are often the most incriminating.

THE CONSEQUENCES OF UNDIFFERENTIATED STORAGE

Although few professional liability cases are litigated in federal court, an expansion of federal discovery rules that went into effect on December 1, 2001, may require firms to make all intentional and unmanaged electronic records available to aggrieved parties automatically, whether or not the documents are relevant to the dispute. Federal district courts must comply with a 1993 amendment to the Federal Rules of Civil Procedure that requires litigants to turn over all materials relevant to a dispute—including e-mail and other electronic documents—whether or not a discovery request has been made for specific documents.

Simply producing and conveying this electronic documentation could be agonizing to defendants because of the large number of documents that are stored electronically. A firm's entire archive of electronically stored data could be subject to discovery—including project management files, billing records, preliminary calculations, report drafts, and calendars—simply because it is impossible to quickly determine which documents might be relevant.

Trade secrets and other privileged data unrelated to a dispute may also be at risk of exposure because

this information may be stored on the same media as discoverable information.

For a plaintiff, the task of carefully searching the defendant's electronic records for relevant documents may seem overwhelming. But because few defendant firms can examine every electronic document stored electronically to determine its relevance to a dispute before conveying the information to the opposition, the plaintiff has an advantage: access to the entire body of knowledge stored electronically by the defendant and the ability to mine it for information to support additional claims or to discover the defendant's trade secrets.

The simple awareness of this fact by both parties favors the plaintiff because it gives the plaintiff a coercive negotiating tool to extract a favorable settlement that spares the defendant from giving the plaintiff access to the defendant's information.

Overwhelmed by the sheer volume of electronic data, some lawyers may agree with their opponents not to ask for each other's e-mail during discovery. Alternatively, some courts may allow attorneys to stipulate what would be produced. Nonetheless, the threat of a plaintiff's access to unmanaged documentation, exercised or not, is too great a risk for most defendants. It is far better for firms to educate all personnel in the careful and rational management of electronic communication.

SPOLIATION OF EVIDENCE

The intentional destruction of evidence related to a legal proceeding can lead to sanctions or the inference by a jury that the evidence must have been unfavorable to the party who destroyed it. No defense counsel—and no defendant—wants to be regarded as having improperly destroyed electronic data that harmed a plaintiff's case. Such action might lead a judge to impose sanctions or provide a jury with instructions related to "bad faith."

MANAGING THE RISK

Establishing, implementing, and enforcing a records retention and document management policy greatly reduces the risk of unintentional disclosure of confidential electronic information that would not otherwise be subject to discovery. In addition, such a policy minimizes the risk of liability for the intentional destruction of evidence related to a dispute. An effective document management and destruction policy might include, but is not necessarily limited to, the following elements:

- An organized electronic filing system that segregates electronic records by type and

segregates record documents from drafts or other documents that the firm would not otherwise retain

- A policy on what types of electronic records are to be destroyed regularly and on what schedule
- A policy that establishes how electronic records are to be destroyed, including—for archival material—destruction of the physical storage media (tape, CD-ROM, or other media) used to archive e-mail messages or electronic documents that are no longer needed
- A written employee policy regarding the proper use of electronic communication by employees, with a particular emphasis on the risk posed by the casual nature of most e-mail
- Helpful reminders that flash on employees' computer screens at log-in

INCREASING EMPLOYEE AWARENESS

The use of project-specific Web sites, e-mail-based project documentation systems, and Internet research capabilities will continue to increase. Successful firms will create policies and procedures that help employees take advantage of electronic communication to enhance productivity and increase firm profitability without generating needless liabilities.

A written employee policy on the proper use of electronic communication is a good first step. But policies are only effective to the extent that employees' habits and the culture of electronic communication are consistent with the policy. The following employee advisory information, while not intended to be comprehensive, may help achieve these ends:

- Electronic transmissions are NOT private. Courts have ruled that e-mail is an inherently public means of communication in which users lack any reasonable expectation of privacy.
- E-mail use may (or will) be subject to monitoring. Although the intentional interception of electronic communications is a felony, the monitoring of employees' electronic messages has been held not to violate the federal statute.
- Only company-related use is authorized; personal use, or any use for illegal or unethical purposes, is prohibited.
- Unauthorized e-mail use may result in disciplinary action, up to and including discharge.

RESOURCES

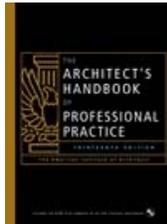
More Best Practices

The following AIA Best Practices provide additional information related to this topic

- 10.01.06 Fundamentals of Record Retention
- 10.02.01 Electronic Data Transfer:
Sample Disclaimer Notice
- 10.02.02 Electronic Data Transfer: A Guide To
Managing Opportunities and Risks

For More Information on This Topic

See also “Information Management,” by Elena Marcheso Moreno, *The Architect’s Handbook of Professional Practice*, 13th edition, Chapter 13, page 380.



See also the 14th edition of the *Handbook*, which can be ordered from the AIA Bookstore by calling 800-242-3837 (option 4) or by email at bookstore@aia.org



Feedback

The AIA welcomes member feedback on Best Practice articles. To provide feedback on this article, please contact: bestpractices@aia.org

Key Terms

- Practice
- Business planning
- Quality control programs
- Risk management



Two Wisconsin Circle
Chevy Chase, MD 20815-7022
(301) 951-9746
www.planetAEC.com

Portions of this Best Practice are a contribution of Victor O. Schinnerer & Company, program administrators of the AIA Commended Professional Liability Insurance Program.