

**FORC QUARTERLY JOURNAL
OF
INSURANCE LAW AND REGULATION**

Spring 1999 March 14, 1999 Vol. XI, Edition I

THE DANGERS OF E-MAIL: DEFENSIVE DRIVING ON THE INFORMATION SUPERHIGHWAY,

Charles T. Richardson, Esq.
(317) 237-1209

As I get older, I am becoming more and more frustrated with the lawyer's "balance," the tendency to see both pros and cons, with the constant weighing of the benefits and risks to the point where advice which started out as clear direction gets burdened with a litany of footnotes and warnings. Such be the case with my own recent advice to clients over the dangers of e-mail. How could anything so wonderful as e-mail have a dark side? How could any lawyer --- i.e., me and thousands of others who are supposed to keep companies and individuals out of trouble --- turn the decade's most popular communication device, which has revolutionized how we work (and literally created telecommuting), into a demon?

Well, demon it can be if you are a company which finds itself on the receiving end of a subpoena for old computer records in a serious piece of litigation or, worse yet, of a complaint by a disgruntled employee who claims she or he was the victim of a hostile work environment where the best evidence is sexually explicit or racist messages sent by e-mail by other employees. Consider what we have seen and heard recently. Does anyone doubt that the star of the Microsoft antitrust trial was e-mail? Day after day we heard about old e-mails coming back to haunt the witnesses, with messages that no one at the time (least of all Bill Gates) thought would have a shelf life longer than a few days. And, don't forget that the Iran-Contra scandal that so tarnished the Reagan administration was uncovered from supposedly deleted White House computer records.

Shoot From the Hip Risks and Issues

Americans send roughly 400 million electronic messages a day, from both home and office. And you can bet that a high percentage of that number — even the pure business ones — represent communications sent with less than careful reflection. There is an amazing tendency to shoot from the hip and to substitute fast communication for thorough, reflective communication. E-mail messages frequently are sent without full consideration of the impact on the recipient and with virtually no regard to the implications if the messages get into the wrong hands years later. People are only slowly coming to realize that e-mail messages can stay in a computer system for years and provide inflammatory evidence in legal disputes ranging from antitrust to employment practices to breach of contract. The very attributes that have made e-mail so popular — chief among them its tendency to induce off-the-cuff candor and immediate access to the top bananas in business and government — are driving employers to conclude that the unfettered use of e-mail has to be reined in.

For lawyers, these concerns have special relevance as we move from routine electronic messages to communications that contain garden variety legal advice, the confidentiality of which must be protected.

communications that contain garden variety legal advice, the confidentiality of which must be protected. The informality of e-mail and the dangers of unencrypted messages can produce liability problems for lawyers who are not careful.

In the endnotes, I have put a bevy of cases, articles and secondary authorities on legal issues that are dominating the discussion of how dangerous e-mail can be, and what all of us — as counselors to businesses and as managers of our own businesses — should be considering as we move from the carbon paper footpath to the information highway. These include:

- Discoverability of computer records¹
- Protecting the attorney-client privilege and security issues²
- Employee privacy³
- Message retention and destruction⁴
- Employer liability for employee actions⁵

Most of those who have discovered e-mail are infatuated with its power and potential. However, with that power comes responsibility and a plethora of unexplored legal issues. Companies that anticipate these problems and guard against them with proactive policies and processes will be in a much better position to protect themselves in the event of future litigation by ensuring that there are no "e-mail messages from hell" lurking on the company's network. For we members of the FORC who advise and industry that is as information dependent and as computer driven as any, here are several suggestions to keep our clients out of electronic hot water and limit potential corporate losses and liability from employee improper use.

A Higher Level of Employee Consciousness

Establish an e-mail policy for your employees, with a clear explanation of expectations about business v. personal use, rules regarding purging/deletion/retention, access to the Internet, monitoring by management, etc. One key strategy is to ensure that employees understand, believe, and act as if the information they enter into their computers is *public* information. Employees should be told up front how that information can be used, that it may be subpoenaed as evidence in a legal proceeding, and the dire consequences for disclosure of inappropriate or illegal statements. When assigning e-mail passwords or user IDs, make sure recipients know they are not the only persons with access to their files, that information exists on a wide variety of back-ups or is otherwise electronically encrypted. Immediately destroy any "illusion of privacy" that employees have regarding e-mail messages.

If You Wouldn't Say It to Your Grandmother, Don't Send It Via E-Mail

The real question for employers is not whether to invade or not to invade the privacy of employees, or whether, when, how, and where to monitor electronic communications. The challenge, and the more effective strategy, is to modify employee behavior so that such messages are *never sent* in the first place. Whether an employer is attempting to avoid liability or prevent employee misconduct or both, managers must educate employees on how to avoid using hostile or discriminatory language and take precautions to safeguard electronic documents that can be used as evidence.

There is an interesting and unexplained phenomenon on the electronic highway that surrounds the sending of e-mail messages. For whatever reason, people tend to regard e-mail as an ephemeral verbal message and accordingly, say things they would never (and should never) write in a memo. Some

message and accordingly, say things they would never (and should never) write in a memo. Some employees are either unaware or in denial about the fact that e-mail messages are just as permanent — in many cases *more* permanent — than hard copy communications. Other employees, feeling invulnerable, shielded by the distance and anonymity of electronic communication, may say things they would not normally say, in a way and with an intensity they would not normally use to express themselves. This is a sort of electronic analog to the adrenaline that prompts motorists, their bravado bolstered by a shield of safety glass and guarantee of a quick getaway, to make obscene gestures at other drivers who have frustrated or angered them. Those same drivers would likely not do the same thing if they were face-to-face with the other driver, *mano a mano*. Similarly, e-mail messages of even mild-mannered employees tend to be more intense and emotional than what that same person would be comfortable saying over the phone, in a memo or letter, or in any communication that has a greater aura of permanence.

Most e-mail users take great liberty with their language — and their opinions — because they incorrectly assume that no one else will ever read their messages or are falsely confident that the messages are destroyed with a simple click of the "delete" key. (Most employees do not comprehend that deleting a message merely eliminates it from their e-mail in-box, but that the message lurks in the company's system indefinitely.) This propensity of employees to "flame" and vent and harangue and defame and argue electronically can cost an employer dearly. Such intensity creates graphic and incriminating evidence that may provide an employee in a discrimination or wrongful discharge suit with valuable ammunition, particularly effective in front of an easily embarrassed or quickly outraged jury.

Employers whose e-mail systems integrate internal and external users on the same electronic address lists should be even more concerned. Although convenient, this set-up allows a demeaning, defamatory, discriminatory, or demoralizing message intended for an employee's officemate to be inadvertently transmitted to every manager in the firm, or to the desk of your best client or customer.

Don't Be an E-Mail Pack Rat

Employers should ensure that e-mail is kept no longer than necessary by avoiding the archiving of back-up tapes on which e-mail messages are filed. Employers are advised to leave such files on the system only for limited periods of time, for example, 30 days. Employees who want or need to save messages for a longer period can do so, by printing out a hard copy or by saving the contents of the message as a word processing document.

What to Do When an Employee Leaves

Employees come and go, but computer files stay, sometimes much too long. Although in some instances an employee's personal files may be useful if an employer later sues an employee for disclosure of trade secrets, patent infringement, or purchasing improprieties, routinely purging unnecessary files of departed employees will reduce the proliferation of data and protect the employer from surprises later on. In most cases it is best to err on the side of eliminating, rather than retaining, messages created by employees who are long gone. The less information available, the less chance the information will later "boomerang" to harm you.

Conclusion

E-mail has become so popular that my issuance of all these endnotes and warnings seems downright wimpy. But all you need is one misstep on a computer screen or buried in a server to convince you that this is no small matter. In fact, to be on the safe side, I've eliminated my e-mail address, unplugged my computer and begun wiping off all door knobs with a handkerchief before entering (and leaving) any room.

Endnotes

1. Discoverability of computer records.

Federal Rules of Civil Procedure, Rule 34. "Any party may serve on any other party a request (1) to produce and permit the party making the request, or someone acting on the requestor's behalf, to inspect and copy, any designated documents (including writings, drawings, graphs, charts, photographs, phonorecords, and other data compilations from which information can be obtained, translated, if necessary, by the respondent through detection devices into reasonably usable form.)"

U.S. vs. Microsoft Corporation, 1998 WL 614485 (D.D.C.). E-mails of Microsoft executives were discoverable and provided substantial evidence in the government's case that Microsoft executives colluded to cement Microsoft's hold on the internet provider segment of the marketplace.

Crown Life Insurance v. Craig, 995 F.2d 1376 (7th Cir. 1993). Data stored in raw form on Crown's computer system was found to be discoverable and when Crown did not turn over data, Crown was sanctioned.

2. Protecting the attorney-client privilege and security issues.

The Electronic Communications Privacy Act of 1986, 18 USC 2510-2711, prohibits unauthorized interception and access of electronically stored data; and also provides for prosecution of fraud and threats *via* e-mail.

State of West Virginia ex rel. United State Fidelity and Guaranty Company and Tim Linsky, Relators, v. Honorable Herman C. Canady, Jr., Judge of the Circuit Court of Kanawha County, and Robert M. Lovell, Respondents, 460 S.E.2d at 689. E-mail message transmitting copy of letter protected by attorney-client privilege was held to be attorney-client privilege.

Heidelberg Harris, Inc., v. Mitsubishi Heavy Industries, Ltd. and MLP U.S.A., Inc., 1996 732522(N.D. Ill.). Finds portion of e-mail to be covered by attorney-client privilege.

National Employment Service Corporation v. Liberty Mutual Insurance Company, 1994 WL 878920 (Mass. Super.), holds that 32 e-mails are protected by the attorney-client privilege.

O'Neil, Thomas F., III, Kevin P. Gallagher and Jonathon L. Nevett, *Detours on the Information Superhighway: The Erosion of Evidentiary Privileges in Cyberspace and Beyond*, 1997 Stan. Tech. L. Rev. 3 (1997). Discussion of method of transmission of e-mail; misunderstanding by state ethics committees of e-mail transmission has led to short-sighted findings that restrict the use of e-mail by attorneys.

American Civil Liberties Union v. Reno, 929 F. Supp. 824 at 834 (E.D. Pa. 1996). "Simple e-mail generally is not 'sealed' or secure . . . (unless the message is encrypted)."

U.S. v. Petersen, 98 F. 3d. 502. Defines hacking as "the ability to bypass computer security protocols and gain access to computer systems."

3. Employee privacy.

Smith v. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa. 1996). An employee who made threatening remarks on e-mail did not have reasonable expectation of privacy.

Bohach v. City of Reno, 932 F. Supp. 1232 (D. Nev. 1996). City did not violate ECPA by reading stored electronic messages of officers facing internal affairs investigation; court rules the city "was free to access the stored messages as it pleased." At 1237.

Kenneth R. Shear, *What You Don't Know Can Hurt You: E-Mail Privacy Claims Under the Federal Electronic Communications Privacy Act*, Louisiana Bar Journal, February 1996. Companies that monitor employees' e-mail without permission could be liable for damages.

Kevin J. Baum, *E-Mail in the Workplace and the Right of Privacy*, 42 Vill. L. Rev. 1011. Employee has limited rights to privacy.

4. Message retention and destruction.

Ronald L. Plessner and Emilio W. Cividanés, "Discovery and Other Problems Related to Electronically Stored Data and Privacy," Practising Law Institute, Patents, Copyrights, Trademarks, and Literary Property Course Handbook Series, September, 1995. Archived or backed up computer records which are deleted can still be retrieved.

Siemens Solar Indus. v. Atlantic Richfield Co., 93 Civ. 1126. 1994 U.S. Dist. LEXIS 3026; Fed. Sec. L. Rep. (CCH)(1994). E-mail messages retrieved from back-up tapes showed that ARCO knew of serious flaws with main product of subsidiary at the time of the sale of subsidiary to Siemens.

5. Employer liability for employee action.

Strauss v. Microsoft Corp., 814 F. Supp. 1186 (S.D.N.Y. 1993). Employer held liable for sexual discrimination based on e-mail.

Owen v. Morgan Stanley & Co., Inc., 1997 WL 403454. Two black employees sued Morgan Stanley for racial discrimination based on e-mail containing racist jokes and

Morgan Stanley for racial discrimination based on e-mail containing racist jokes and circulated among white employees.

Kelley v. Airborne Freight Corp., 140 F. 3d. 335. Age discrimination claim supported by e-mails between supervisors.