LEGAL BYTES

E-MAIL AT THE WORKPLACE: I SPY, SHOULD I?

LORI LESSER
SIMPSON THACHER & BARTLETT LLP

MARCH 15, 1998

To snoop or not to snoop, that is the question when it comes to dealing with electronic mail in the workplace. For some employers, it may seem distasteful or an invasion of privacy to monitor employees' electronic mail. Yet as company employees send thousands of e-mails a day to colleagues, vendors, clients, (you hope not) competitors, Internet bulletin boards and cyber-friends, many employers are learning to snoop reasonably to avoid even greater liability by inaction.

How can an employee e-mail communication -- sent from a lone personal computer in a private office or cubicle -- create large-scale liability for a company? Many potential problems spring immediately to mind, and you probably have personal anecdotes to add to the list.

The Problems

The company calling card -- leave home without it. If employees send e-mail from the workplace to any outside party, the on-line world may perceive their comments as having a company endorsement. Workplace e-mail addresses usually include the company's exact name or an easily recognizable acronym or derivative. So if an employee unfairly attacks a vendor or competitor on a bulletin board -- or if a private slam sent to a chat-room denizen later gets circulated and posted -- the world knows the author first and foremost as a certain company's employee. Employees do not necessarily abandon all hope of free speech by entering the office door, but look at it this way: if you can't wax poetic on O.J. Simpson or bash Microsoft on company letterhead, you shouldn't do the same with a corporate e-mail address. This is why at-home AOL accounts exist.

Your honor, it was just a joke. By now, most readers have probably heard of one e-mail gaffe or misdirection that prompts more cringing than your driver's license photo. If nothing has come of this transgression by now, consider the perpetrator lucky. As for the future, do not allow workplace e-mails to be written, replied to, or forwarded along that you don't want read by (i) a dissatisfied employee, (ii) a dissatisfied ex-employee, or (iii) the lawyer for (i) or (ii) (who are by now the same person).

Last December, a blue-chip New York investment bank was sued by African American employees who alleged that their colleagues had circulated a racist joke on the company's e-mail system. The employees charged that the e-mail created a "hostile work environment" for African-Americans at the bank, in violation of federal law. Under federal civil rights law, a company can be held liable if its employees create an "intimidating, hostile or offensive environment" to members of a particular race, religion, national origin, or gender. (This term, the Supreme Court will consider whether to add sexual orientation to the list.) The employees' suit was later dismissed, but the investment bank would have saved immense time and resources had the allegedly racist e-mail never circulated. Plus, the mere fact of the lawsuit created unfavorable publicity, perhaps hurting minority recruiting and some business development. At least two other large financial companies have been sued for huge sums on e-mail related charges. In a more expensive result, a major U.S. energy company settled a sex discrimination case in 1995 for more than $2 million, after female employees alleged that the company e-mail system had circulated a sexually explicit, offensive joke about women.

Of course, the employer can argue that, like Oswald, the individual employees acted alone, and on a limited basis. Yet, the employee (or ex-employee's) lawyer will argue that the company (i) hired and retained the harassers, (ii) did not properly discipline the harassers after the employee complained; or (iii) tacitly encouraged the harassment, because the office atmosphere led the harassers to believe such behavior would not be punished. Further, from an ethical perspective, even if your company is not dragged into court for offensive e-mails, should it ignore statements that harm office morale or disregard a company policy favoring mutual respect and equal opportunity?

Your honor, I was exaggerating. Even for serious e-mail, there is a range of sensitive topics that employees would never "write down" the old-fashioned way, such as whether the company might be at fault in a brouhaha with vendors, clients and the like. Maybe the company did receive that invoice and it was misrouted interoffice. Maybe the company sales rep didn't leave the room when competitors improperly discussed pricing strategy. Maybe some executive suspected that a product would not be ready for market before the last stock offering. If you don't want to be asked about a statement in court, do not put it in an e-mail.

Even if the e-mail *subject* is appropriate, language trouble can still arise. Most employees compose e-mail with the presumption that it's informal chatter. In a future lawsuit or government investigation, however, lawyers and judges will read all firm e-mail quite literally, as formal corporate communication. Fortunately, in old-fashioned print correspondence, the English language has wonderful euphemisms to replace tempting e-mail words such as "disaster" (event), "mistake" (decision), "incompetent idiot" (insert name of colleague) and "absolute worst ever" (potentially not optimal). Employees should be encouraged to use protective language in all communications, including e-mail.

The best things in life are (not always) free. Current Internet manners among many digerati consider copying and forwarding of good e-mail humor and wisdom to be *de rigueur*.

One's closest friends and colleagues would be offended not to be sent instantly the latest Dilbert-ism, Top Ten list, or reasons why men and women view haircuts differently. The authors of such e-mail humor and wisdom may disagree, and sufficiently loudly and expensively so as to create a company problem.

In general, to copy, distribute, create derivative works based upon, or publicly perform or display an author's original expressive content requires that author's permission. Otherwise, such actions create liability for copyright infringement. Widespread downloading and forwarding of Internet content is risky -- it is unauthorized copying and distribution and the damages easily mount. For example, in a few days, a single e-mail that transcribes a magazine article can be forwarded to thousands of people who would otherwise have paid $3.95 to buy the magazine as a legitimate source of the article. In addition, if the creative e-mail humorist edits, splices or dices the Internet content, seasons it with other text or graphics, or chops off the author's original credit before forwarding the final e-mail masterpiece, the original Internet author may also have a case for unfair competition or under certain foreign laws protecting authors' "moral rights."

Sticks and stones . . . Every day, your employees are inspired to express strong opinions on a variety of topics. This can be a good thing in some areas, but not on the company's e-mail system. In general, liability for defamation will arise if one makes a false statement about a living person or corporation that tends to cause shame, ridicule or financial injury. While "pure" personal opinion is constitutionally protected, such "purity" is compromised if a personal opinion implies damaging facts. For example, an MIS person's statement that "I tried Company X's new computer product, and it's a loser!" implies a factual basis for the product's "loserhood" and should not be posted to a bulletin board.

(Almost) nothing lasts forever. Funny e-mail, serious e-mail, sensitive e-mail, the worst part about company e-mail transgressions is that, like death and taxes, the evidence is certain. The e-mail "delete" button functions less like a shredder than like an instant records cart taking your e-mail to a subterranean company warehouse. (That's a little too much fine print for a delete button, so "delete" alone is left to give the wrong impression.) Depending on the company's system of backing up e-mail, and whether or how often these records are purged, some digital archive probably exists of much company e-mail. If the company faces a lawsuit or government investigation, it will likely be forced to hand over all the existing, archived e-mail and all the e-mail it is technologically capable of reviving with the most advanced equipment available.

The Solutions

Now that the potential damage of office e-mail is evident, what is to be done? As Hamlet almost mused, is it nobler for employers to suffer the slings and arrows of outrageous fortune, or to take arms against a sea of troubles? It is a far, far better thing to have a written office electronic mail policy for employees to review and acknowledge. At best, the policy may prevent employees from creating e-mail-based liability. At worst, if an employee violates the

policy, the company can better argue that the individual acted alone, since the company had made clear from day one its views on proper e-mail etiquette.

What are the components of a proper in-house e-mail policy? A good policy requires coordinated input from the company's legal, technical and human resources managers, and should address the following questions:

(1) Can employees send e-mail from the workplace to outside third parties? In many cases this is desirable, or even necessary, to communicate effectively with vendors, customers and clients. Yet acceptable parameters for outside contact should be spelled out, such as appropriate work-related correspondents, and whether supervisors should approve or at least know of them. (Virus control is another issue that may warrant disclosure in this area.) Perhaps not all social correspondents are created equal -- family members and friends' private boxes may be treated differently from joining Internet chat rooms or posting to bulletin boards.

(2) Can the company monitor employees' e-mail, and under what circumstances? Most companies probably lack the desire or resources for routine, wide-scale monitoring of employee e-mail. In addition, comprehensive monitoring of employee e-mail without good cause may be against federal wiretapping laws, which allow employers to intercept employee e-mail, either (i) with their consent or (ii) in the ordinary course of business, if the employer has a legitimate business purpose to monitor the e-mail and minimizes any intrusion on employee privacy. Legitimate business purposes might include responding to a colleague's harassment complaint, investigating a data leak, checking the quality of the computer system, or responding to a government request for documents.

Notwithstanding the federal law, many state privacy laws protect employees from unreasonable intrusions on their personal privacy at the workplace.

Against this backdrop, company e-mail policy should be written and should make clear if and when employees can consider their workplace e-mail to be "private property," and if and when e-mail is not private, who may review employees' e-mail, and under what circumstances. To protect against employees' pleading non-consent or unreasonable monitoring, all employees should formally acknowledge the policy -- either by signing a personnel form in the stack for new employees on day one, or by clicking agreement when they first access the company's e-mail system. Recently, after an employee sued his California employer for reading his e-mail and firing him for sending sexual e-mails on the company system, the court ruled in favor of the employer. The court noted that the employee's privacy was not violated, because company employees had signed acknowledgments that the company would monitor employees' e-mail on an *ad hoc* basis.

(3) Does the company want to back-up or purge e-mail on a regular basis? The technical considerations include the human and network cost for continuous back-ups and deletions. Legally, a consistent purging policy is prudent, because it is often unethical and/or illegal to delete e-mail, just as with shredding paper documents, only when a lawsuit or

government investigation may be imminent. Conversely, retaining e-mail could later help the company -- *e.g.*, to help prove that a defecting employee leaked confidential data to a rival, because he had shopped his resumé months before his departure and while staffing a top-secret project. If the company already has a written policy on document retention and destruction, rethink electronic mail into the framework.

Your mother is always right (but when in doubt, get a lawyer). As a final note, for all the specific e-mail policy issues not addressed here, a little common sense goes a long way. If employees generally refrain from authoring or transmitting any communication that would not make the company proud, in terms of the company's overall mission statement, customers, regulators, potential recruits and the general public, then the company will probably evade trouble. A must-read company e-mail policy should, however, set the stage for appropriate e-mail conduct even before employees touch their keyboards.

Lori Lesser (l_lesser@stblaw.com) is an intellectual property associate in the New York office of Simpson Thacher & Bartlett. This article is intended to provide a general discussion of the topic and should not be relied upon as legal advice for any specific problem.