LJN LAW JOURNAL NEWSLETTERS

LJN'S
Product Liability
Law & Strategy®

Volume 24, Number 9 • March 2006 ALM

Think Twice, Click Once: E-mail Guidelines

By Ronald J. Levine and Susan Swatski-Lebson

Document retention, and the host of related e-discovery issues, have been front and center for product liability attorneys for a number of years. Nevertheless, even with the best document retention program and the most sophisticated e-discovery system, companies and their attorneys are still going to have to deal with the documents themselves. As many trial lawyers have learned, it can take only one bad document to bring down the house. With respect to the increased use of e-mails as evidence in litigation, companies need to educate their employees on what constitutes appropriate online communication. We recommend that companies focus on training their employees to "think twice and click once."

Why are e-mails such a major issue? E-mails have become the primary form of communication. Millions of e-mails are exchanged between employees daily. E-mails are considered to be informal. Nevertheless, in one brief, seemingly informal e-mail, an employee can render an opinion on liability, falsely implicate fellow employees in wrongdoing, and make a binding admission — all without the employer even knowing such a "paper trail" exists. When writing e-mails, many employees may not understand that their informal e-mail comments can be twisted and taken out of context.

For example, a product engineer may write an e-mail explaining that the company's product is not safe for a particular use, but neglect to specify the conditions under which it would not be safe because the engineer thought that the recipient understood that information. The absence of such important qualifiers could render that e-mail a "smoking gun" if it surfaced during e-discovery.

Hundreds of "good" e-mails will not matter if that one "bad" e-mail is sitting around, waiting to be discovered during the course of pretrial discovery. An e-mail is not going to evaporate after it has been sent; e-mails may reside permanently on hard drives, servers and backup tapes. Unlike a paper draft, the e-mail may be around forever. That "bad" e-mail may eventually prove to be extremely costly for the company.

Corporate counsel — both inside and outside — should take the lead in educating employees that when they click on their keyboard, no matter how casual the situation, they must keep in mind the following assumptions:

- All e-mails may well be read by an adversary one day;
- Any e-mail can and will be used against its author and the author's employer;
- The language used in the e-mail may be taken out of context; and
- If litigation ensues, the e-mail will be viewed in the light most favorable to the plaintiff.

We have employed a few techniques in trying to educate clients' employees about e-mails, which in turn put clients in the best position to limit their risk of the unintended "bad" e-mail. We have assisted in drafting e-mail policies, delivered lectures to employees, prepared online training courses, and have even developed a mouse pad with a warning concerning e-mail drafting.

A helpful resource in drafting an e-mail policy can be found in the ANSI/ARMA 9-2004 Standard: "Requirements for Managing Electronic Messages as Records." The Standard emphasizes that an e-mail policy must address, among other things, security issues, appropriate use of the system, confidentiality, the company's obligations, if any, to protect individual privacy and the need to use encryption. In Section 8.1 of the Standard, it emphasizes that any policy should of course also address the appropriate content of messages.

Once a company has developed an e-mail policy, some employers have adopted a compliance strategy that includes randomly monitoring the content of all e-mails, while other employers have adopted a more elaborate strategy by implementing a computer program that has real-time content analysis capabilities to prevent delivery of e-mails with noncompliant content. With respect to these strategies, employers have advised employees that they have no expectation of privacy to their e-mails and that their e-mails may be monitored. Such strategies may help to reduce the cavalier use of e-mails and safeguard potentially confidential business information.

With respect to educating employees about e-mail content, we have tried to follow the "KISS" Principle — Keep It Simple, Stupid. If an employee can be trained to observe the following eight simple rules, the company will be well served.

1) Try not to write anything you would not want to see on the front page of the newspaper. Indeed, as some companies have learned the hard way, e-mails can wind up on page one of *The Wall Street Journal* or *The New York Times*.

continued on page 2

Ronald J. Levine is a partner in and co-chair of the Litigation Department of Herrick, Feinstein, LLP, a law firm with offices in New York; Princeton, NJ; and Newark, NJ. **Susan Swatski-Lebson** is a litigation associate with the firm.

E-mail

continued from page 5

2) Send e-mails to as few people as possible. Too many employees "cc the world" when they transmit e-mails. Recipients should be limited to those who need to know. The more people who know about an e-mail alleging, for example, a defect in a company product, the more people who can be charged with failure to act to remedy that defect regardless of whether any action was reasonable. With respect to this point, employees should be asked, "Do you want to be responsible for making everyone who receives your e-mail a potential witness at a trial?" Indeed, if an employee replies to an e-mail from counsel and copies people outside the company, an otherwise privileged communication could lose its privilege.

3) Avoid e-mails where a phone call or a meeting would be more appropriate. Employees should ask themselves the following question before they peck out a message: "Should I commit this to writing?" In the new world of Instant Messaging ("IM"), the telephone has been replaced by the keyboard. Employees need to be reminded that an instant message may create a permanent record, which is not the case with an oral conversation. Employers should weigh the pros and cons of the use of IM technology in their workplace. If the value of an instant message is minimal, some employers lock out IM platforms; or, if the value is substantial, some employers limit employee use and or monitor IM on an internal server.

4) Try to avoid expressing an opinion on liability unless you have been asked to do so. Employees must be told that they should avoid playing judge and jury concerning their company. Words such as "liability," "dangerous" and "defect" are very powerful, and should not be used lightly. Further, if an e-mail is going to be sent documenting a problem, the employee should be advised to note the steps that have been taken to resolve it.

5) Make every effort to be accurate when writing e-mails. E-mails are all too often written while in a hurry. Employees should be urged to avoid speculation, and to reflect before committing information to writing. Employees need to be reminded that an e-mail "off the top of the head" can be turned into the "gospel" by an adversary in a litigation.

6) Assume that ambiguities will be construed against the company. Employees may not realize that the e-mail can be deemed to be an admission on behalf of the entire company, not just by the employee. Similarly, e-mails should not be a vehicle for "venting." A company should of course have a quality control protocol and should be pursuing any performance-related issues. An employee, however, may be totally off base in his or her comments, or may rush to judgment. The unfortunate company may never get a chance to clear up the e-mail at trial.

7) Do not put on the "lawyer" hat if you are not a lawyer. Employees should be instructed to drop the following phrase from their e-mails: "I am no lawyer but … "

8) Mark e-mails as privileged when appropriate, but do not assume that the e-mail will only be read by your counsel. Employees should be marking communications that are protected by the attorney-client privilege with the designation of "Privileged and Confidential." However, they should not mark every e-mail that goes to a lawyer as privileged. For example, if employees use the privilege designation when it is not appropriate, and those e-mails are added to a privilege log, the judge may lose confidence in the log if and when it is reviewed by the court. An e-mail to the general counsel setting up a golf game is probably not a good candidate for "Attorney-Client Privilege." In addition, employees should not assume that an otherwise privileged e-mail will never see the light of day. Even a privileged e-mail may be read by the court, or worse, deemed not to be privileged by the court. Indeed, corporate counsel would be well advised to limit negative comments concerning the court. It is entirely possible that the judge may someday read those comments.

CONCLUSION

An effective e-mail training program can pay huge dividends, not only in avoiding "bad" documents in product liability cases, but in many other areas of potential risk, including employment discrimination and antitrust. As with any policy, it is important that it is communicated to all employees and supported by the company, from top to bottom. Moreover, the policy must be enforced consistently. Companies should deal with violators before their e-mails bring down the house.