andrews
Employment
LITIGATION REPORTER
Volume 17, Issue 17
April 1, 2003

Commentary:

Does Your Company E-Mail Policy Need A Makeover?

By David R. Singer

Not surprisingly, today's businesses have become increasingly dependent on e-mail. The same holds true for today's employment lawyers, who often rely on e-mail records to paint a picture of the events surrounding employment disputes.

Golden nuggets of evidence are often embedded deep in a company's e-mails just waiting to be discovered. But retrieving old e-mails can be difficult, especially for companies that routinely purge expired e-mails every few months. In those cases, lawyers follow the e-mail trail to employees' home or laptop computers, or to the computers and networks of the e-mail recipients where copies of workplace e-mails may still exist.

The Basics of Privacy Concerns

Because of privacy issues, retrieving employee e-mails from a third-party's records requires some legal wrangling. To succeed in the modern e-mail hunt, employers should prepare themselves by following three basic rules: lower expectations of privacy that employees may have in their e-mails; prepare e-mail usage policies that are easy to understand but technical enough to cover the latest e-mail technology; and have employees read and sign the usage policies.

E-mail privacy issues frequently arise during discovery, when attorneys gather the evidence. Our firm was recently involved with a case that put the issue of e-mail privacy to the ultimate test. One of our clients (the company, in this case), subpoenaed e-mails exchanged between the plaintiff, a former employee, and her husband, who worked for the company's competitor.

Our client no longer had its own records of the plaintiff's e-mails and the plaintiff had deleted all copies of her e-mails from the laptop computer the company lent her. The plaintiff opposed the subpoena, claiming that her "work e-mails" to her husband constituted privileged spousal communications (an absolute privilege like the attorney-client privilege) and were protected by her constitutional right to privacy.

To prevent a prohibited invasion of privacy, the objecting party has the burden of establishing a reasonable expectation of privacy in the circumstances. Similarly, in order to assert the confidential spousal communication privilege, the claimant must prove that she intended the communication to be confidential, and that she had a reasonable expectation of privacy. In this case, the issue before the court was whether the plaintiff had a reasonable expectation of privacy in the e-mails she sent to her husband from work.

Under California law, two factors determine whether there is a reasonable expectation of privacy in work e-mail: accepted community norms, and whether the employee had an advance opportunity to consent or reject the thing that constitutes the invasion.

The Community Norms of Workplace E-Mail

In recent years, the use of e-mail in the workplace has gone from cutting-edge technology to basic necessity. In determining whether an employee has a legitimate expectation of privacy in her work e-mails, courts look to the modern day customs of e-mail usage in the context of the "21st-Century computer dependent business." One appellate court has already noted that in 2001, "more than three-quarters of this country's major firms monitor, record, and review employee communications and activities on the job, including their ...e-mails, Internet connections, and computer files."

Employers seeking access to an employee's e-mails must demonstrate to the court how today's community norms rebut any claimed expectation of privacy. This is fairly easy because, unlike the days when e-mail was a novelty, most employees understand that their work e-mail is just that – work e-mail. Many employees are savvy computer users or Web surfers and increasingly understand that "John" in the "IT Department" can access all of the company's e-mails or other computer usage information.

In this case, the company was able to salvage a few of the plaintiff's e-mails. One of them contained a great example of "community norms" for workplace e-mails. The plaintiff sent an e-mail to a co-worker containing inappropriate comments about her supervisor. At the end of the rude e-mail, she included the statement: "If anyone is reading my e-mails, I hope they are enjoying them."

When confronted with this e-mail at her deposition, the plaintiff reluctantly admitted her understanding that the company could review and monitor her e-mail traffic. The court denied the plaintiff's motion for a protective order and we were able to obtain all of the plaintiff's workplace e-mails to her husband.

Make Sure You Have a Written E-Mail Usage Policy

The reasonableness of an employee's claimed expectation of privacy also depends on whether the employer gave advance notice that workplace e-mails were not private, and whether the employee signed the policy. These e-mail usage policies play a critical role in showing that there is no reasonable expectation of privacy in workplace e-mails.

E-mail usage policies do not need to be long and should contain a clear and concise statement of the policy such as "Electronic communications are to be used solely for company business, and the company reserves the right to monitor or access all employee Internet or e-mail usage." The policy should be written in a manner that is simple enough for all employees to understand. One e-mail usage policy warns employees not to send any e-mails from work that "you wouldn't want to see in the *Los Angeles Times* headlines." Although somewhat extreme, it makes the point.

E-mail usage policies should not be oversimplified. They must be technical enough to specify the types of data, files, and communications that are covered by the policy. The policy should explicitly cover employee usage of work computers as well as home computers used to access the company's network. More thorough policies should also cover information on work-related peripheral devices such as a BlackBerry wireless handheld device, and should include Internet access and usage provisions. The overall policy should make clear that any information that "passes through" any of the company's computer equipment is "company property" and fair game for the company to review or subpoena from recipient third parties.

In the example case, the company provided the plaintiff with software and Internet access allowing her to connect to the company's server remotely. The plaintiff used the company's Internet access to send and receive e-mails from her Yahoo! account when she worked at home. Our subpoena sought the plaintiff's e-mails to her husband sent from her Yahoo! e-mail address – not her work e-mail address – while using her home computer.

We argued that because the plaintiff was connected to the Internet via the company's network, and because all of the plaintiff's communications were literally "traveling through" the company's equipment, the plaintiff waived any reasonable expectation of privacy in those e-mails too. Indeed, we specifically called to the court's attention the fact that the company's information technology staff could "eavesdrop" on the plaintiff's Internet activity if they wanted to. The court agreed, and the company succeeded in obtaining the plaintiff's e-mails to her husband. The court noted that the outcome would be entirely different if the plaintiff had used her own Internet service provider to access her Yahoo! e-mail account and send e-mail to her husband.

E-mail usage policies can also be used to set forth other company guidelines dealing with inappropriate Internet use, racial and sexual harassment, or other company policies that might be affected by computer, e-mail, and Internet use.

Sign on the Dotted Line

In addition to having a well-written e-mail usage policy, obtaining employee signatures is the only way to ensure its effectiveness. One appeals court has held that that notice, combined with an employee's written consent defeats a claim of reasonable expectation of privacy: "His signature shows that he read the company's policy, understood it, and agreed to adhere to it." Thanks to favorable and clear legal precedent, California employers can protect against expensive privacy battles by following a few simple steps.

At least two federal courts have addressed situations where there was no signed e-mail usage policy. In *Smyth v. Pillsbury* (E.D. Pa. 1996), a plaintiff employee accused his employer of violating his privacy rights by reviewing his e-mail messages sent to a supervisor over the company's network. The employer in *Smyth* never circulated an e-mail usage policy to be signed by its employees. In fact, the employer affirmatively "assured its employees, including plaintiff, that all e-mail communications would remain confidential and privileged."

Despite these assurances, the court rejected the plaintiff's privacy claims. According to the court, "[O]nce plaintiff communicated the alleged unprofessional comments to a second person ... over an e-mail system which was apparently utilized by the entire company, any reasonable expectation of privacy was lost."

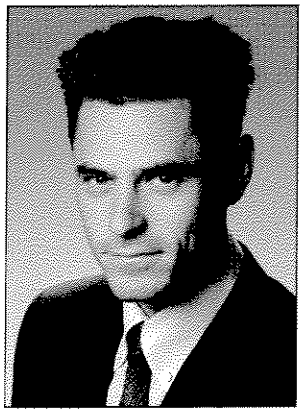
In a more recent federal case, the plaintiff and her daughter were fired for violating the company's e-mail policy based on sexually explicit content e-mailed to them from the plaintiff's husband. The employer's email usage policy was not distributed to employees but merely posted on the company's intranet Web site which, according to the plaintiff, was confusing and difficult to access. Nonetheless, the district court found no reasonable expectation of privacy in the plaintiff's work e-mails.

California employers should not rely too heavily on these federal cases, however, because the state's constitution guarantees some of the most expansive privacy rights in the nation. E-mail and computer usage policies can be drafted and signed without much cost to the company, and the potential payout is immeasurable.

Keeping Up with Technology ... and the Law

Modern tools of the workplace like e-mail, desktop or laptop computers, personal digital assistants, and Internet access are undeniably efficient and productive. Offering these tools to employees allows employers to create a web of company-owned devices over which critical information can flow. While benefiting from these advancements, employers must also take advantage of the laws that permit the employer to maintain control over this information.

And unlike some traditional areas of law, cases addressing e-mail usage are quickly adapting to keep pace with technology. If your company or client is using an outdated e-mail usage policy, it's probably time for a makeover. With a little luck, a combination of high-tech gadgets and high-tech lawyering might one day lead your company to an old-fashioned smoking gun.



David Singer is an attorney in the Los Angeles office of Hogan & Hartson and is a member of the firm's litigation group. Singer works on a broad range of litigation matters, including complex business litigation, sexual harassment, race discrimination, unfair competition, and entertainment litigation. He has represented clients in numerous industries including computer software, television production, fashion and apparel, telecommunications, and real estate.