Prof. Corporations

Continued from preceding page

self-employment, which means practice net income in a given year reduced by the plan contribution itself. The employee of a corporation can base the contribution on the full amount of taxable compensation, without such reduction. This means that, even if the percentage limits appear to be the same, there are situations where a corporate employee can contribute more to a qualified plan than a self-employed person.

The professional corporation has a special advantage to the junior owners of a large law firm with centralized management. For example, the formality of the corporate records benefits those owners who aren't in control by subjecting those in control to more formal accountability. In addition, the shareholder of a C corporation doesn't have to pay income taxes on undistributed profits, so the "junior partner" doesn't have to worry about a management decision to withhold distribution of profits.

It should be noted that shareholders of an S corporation are similar to partners and L.L.C. members in this regard, and that undistributed profits are taxable to the owners, including those owners who did not take part in the decision to accumulate profits. However, undistributed profits in an S corporation will not be subject to FICA taxes, an advantage that could be a consideration for some professionals.

In the past, it seemed as though most professionals could benefit from the professional corporation, particularly the C corporation. Now, the question of whether the professional corporation is advantageous can only be answered on a case-by-case basis. For the lawyers who will still benefit from one or more of the characteristics of the corporation, in a firm that does not anticipate regular changes in its ownership, the professional corporation certainly should still be considered.

—❖—

WORKPLACE COMMUNICATIONS

Do Employees Have a Legitimate Expectation Of Privacy in Their E-Mail and Voice Mail Use?

By Lisa S. Burton and Melineh Blackwell

Today employees are more reliant and knowledgeable about the use of the World Wide Web, e-mail and voice mail systems in conducting their day-to-day tasks. Employees are using these technologies to communicate with customers, suppliers and colleagues. But along with business use comes personal use. Employees' usage of computers and telephones for personal business can range from chatting with friends and relatives to cybershopping. The employer of today must be cognizant of the risks and benefits associated with the use and misuse of these ever-expanding technologies.

The usefulness of these technologies is well known for employee access, use and dissemination of business information. Likewise, misuse of communication technologies can just as easily waste company time and resources as a result of employees:

- Spending too much time on personal e-mail messages,
- Taking part in extensive "chat room" dialogues,
- Misappropriating and disseminating company trade secrets,
- Copying and distributing intellectual property without authorization,
- Improperly posting company information on "bulletin boards," and
- Sending or downloading inappropriate, sexually hostile or harassing messages or graphic pictures that can expose companies to liability.

By establishing policies stating the company's expectations regarding e-mail and Internet access and use, employers can prevent misunderstandings and possible claims before they develop.

Do Employers Have the Right To Monitor Communications?

The federal law on employee privacy rights and e-mail is still developing. Congress enacted the Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510 et seq., which prohibits the interception of "electronic communications," including e-mail, to update older federal wire-tapping laws used to combat organized crime. The ECPA protects e-mail messages from interception and disclosure to third parties and also protects against unlawful access to stored e-mail communications. Communications receive varying degrees of protection depending on whether they are in the transmission phase or the storage phase. Sec. 2511 of the ECPA prohibits any person from "intentionally intercept[ing] or. . . disclos[ing]" the contents of wire, oral and electronic communications by any electronic, mechanical or other device. Sec. 2701 provides that a person who "intentionally accesses without authorization a facility through which an electronic communication is provided. . ..and thereby obtains access to an. . .electronic communication while it is in electronic storage . . .shall be punished as provided in subsection (b) of this section."[1] Exceptions within the ECPA, however, may exempt employers who monitor employee-provided e-mail systems in the ordinary course of business.

First, the ECPA allows access to electronic communications where one of the parties to the communication has given prior consent. In theory, employees could consent to their employer's accessing communications sent, received or stored on their employer's e-mail system. Second, employers could also likely use the "business extension exception" to intercept e-mails during their transmission phase or access stored e-mails. For the business exception to apply, an employer would likely need to show that its reason for monitoring is credible and not excessive. In such circumstances, the employer would argue that the interception or monitoring is necessary to prevent misconduct in the work environment, or that it justifiably suspects disclosure of

Continued on Page 8

Lisa S. Burton is a junior partner at Hale and Dorr LLP in Boston. e-mail: *lisa.burton@haledorr.com* **Melineh Blackwell** is an associate in the Washington, D.C. office. e-mail: *melineh.blackwell@haledorr.com.*

Employee Privacy

Continued from Page 7

confidential information. For the "provider" exception to apply, the employer would have to establish that it was a "provider" of the electronic communications system. To intercept e-mails in the transmission phase, the employer also would have to show that it was necessary to monitor e-mail to protect the rights and/or property of the employer.

Even if exempted from the ECPA, however, employers still must be wary of restrictions under state law counterparts to the ECPA, as well as possible common law claims that irate employees may bring on discovering that their e-mail was intercepted and read by their employers. Likewise, many states already have statutes creating a tort for invasion of privacy, and several states are considering enacting such statutes. For a list of states that have enacted privacy laws, go to *www.epic.com.* Employees may claim under existing state laws that their privacy has been improperly invaded when their employers review or monitor what the employees deem to be their "private," "nonbusiness-related" communications.

Massachusetts, for example, has a statute that protects every person in the commonwealth from unreasonable, substantial or serious interference with his or her privacy: the Massachusetts Privacy Statute, M.G.L. c. 214, § 1B. In *Smyth v. Pillsbury Co.*, 914 F. Supp. 97, 101 (E.D. Pa. 1996), a federal court interpreting Pennsylvania common law on privacy concluded that an employee has no reasonable expectation of privacy in his e-mail. The court stated that a reasonable person would not consider an employer's interception of e-mail communications to be a substantial and highly offensive invasion of privacy. The employer's interest in preventing inappropriate and unprofessional comments or even illegal activity over its e-mail was found to outweigh any privacy interest that the employee may have had.

Employee access to the Internet can also lead to potential employer liability. For example, employees who use an employer's internal access usually disclose the employer's name as the originator of the message. Thus, if the employee accesses or downloads copyrighted materials or engages in any other inappropriate conduct, a third party could argue that the employer had a duty to stop such conduct. Likewise, if during employment, the employee downloads and uses copyrighted information, the company likely will be liable for copyright infringement. Companies also need to make sure that employees are not improperly accessing and sending confidential information or trade secrets of the company over the Internet.

Don't Forget: E-Mail Is Evidence

E-mail also is becoming the proverbial "smoking gun" in litigation. Today smart attorneys are routinely requesting e-mail records as part of their general discovery requests.

Employers and employees must understand that e-mail is not a one-time, whispered exchange. E-mail messages can be retrieved, recreated and used as evidence, even if the sender or recipient believes that they have been deleted.

What Should Employers Do?

Every employer who provides e-mail and Internet access to its employees should create e-mail and Internet policies that explain the company's expectations and state that the company's e-mail, voice mail and computer systems are monitored. Policies should state that employees' e-mail and Internet access are the company's property. Employees should also be cautioned to commit to e-mail only what they would commit to paper, because e-mail continues to exist even after the delete button is pushed. To prevent e-mail from being recreated, companies should also implement electronic deletion procedures that will destroy all e-mail files on a regular basis. By doing so, companies may prevent embarrassing or damaging messages from being restored after deletion.

(1) Civil penalties for violation of the ECPA include preliminary and other declaratory and equitable relief, monetary damages, punitive damages, attorney fees, and costs. 18 U.S.C. § 2520(b). Criminal penalties include maximum imprisonment for not more than five years, fines, or both. 18 U.S.C. § 2511(4)(c).

—❖—

Crisis Spurs Settlement

With America under attack by terrorists, lawyers involved in the trial of a bitter, highly personal fee fight have agreed the dispute was trivial in the wake of the horror and tragedy of the events of Sept. 11, and they resolved their disagreement.

Houston plaintiffs' lawyer John O'Quinn and former associate Kendall Montgomery agreed to settle the suit that Mr. Montgomery filed against Mr. O'Quinn seeking $105 million in unpaid fees and punitive damages.

Terms aren't confidential, but Mr. O'Quinn and two of Mr. Montgomery's lawyers, Joseph Jamail and Ronald Krist, declined to talk about them.

Mr. Jamail said that a heartfelt comment by Mr. Krist on the morning of Sept. 11, shortly after lawyers on both sides agreed to let the jurors go home for the day because of the unfolding tragedy, prompted them to think hard about what's important. The American crisis was undeniably the catalyst that ended the dispute, Mr. Krist said. He said that no one was thinking settlement before then.

The trial was attracting great interest in Houston's legal community, not only because of the amount of money at stake, but because it promised to reveal details of how Mr. O'Quinn runs his highly successful plaintiffs' firm, O'Quinn & Laminack. Mr. Montgomery, who worked for Mr. O'Quinn from 1991 to 1999, alleged that Mr. O'Quinn owed him at least $105 million in fees, based on a 25 percent share of the firm's net fees from several large suits, including the $17 billion settlement in Texas' tobacco litigation.

Mr. O'Quinn said that he agreed to pay Mr. Montgomery a $110,000 yearly salary, but bonuses were at his discretion. His lawyers also filed a counterclaim against Mr. Montgomery, alleging that the associate breached his fiduciary duty to the firm by failing to disclose his investment in Christian Hill & Associates, a firm in Houston that primarily handles workers' compensation work.

—Brenda Sapino Jeffreys

