THE NATIONAL
LAW JOURNAL
DAILY UPDATES ON WWW.NLJ.COM THE WEEKLY NEWSPAPER FOR THE LEGAL PROFESSION MONDAY, JANUARY 14, 2008 ALM

IN FOCUS

LABOR & EMPLOYMENT

Ownership of e-mail is not clear

Employees retain some rights over confidential writing sent from work.

By Elise M. Bloom
SPECIAL TO THE NATIONAL LAW JOURNAL

"YOU'VE GOT MAIL." Three little words that everyone loves to hear. But in today's society, where more time is spent at work or working remotely than anywhere else, one has to wonder "Whose mail is it anyway?" From online shopping to e-vites, almost every employee has used his or her corporate e-mail to send personal communications to friends and family despite the company's clear policy to the contrary. In the current, litigious environment, what happens when an employee sends personal, allegedly confidential communications from work to his or her attorney or spouse? Can the employer lawfully access those e-mails, or do the attorney-client and marital privileges prohibit the employer from doing so? In answering this question, the key inquiry is always whether the employee had a reasonable expectation of privacy in the e-mails at issue.

The attorney-client privilege has long protected communications between an attorney and his or her client, provided that they are made in confidence and for the purpose of seeking legal advice. Fed. R. Evid. 501; *Knepp v. United Stone Veneer*, No. 4:06-CV-1018, 2007 U.S. Dist. Lexis 65423 (M.D. Pa. Sept. 5, 2007). The privilege was devised to ensure free and open communication between attorneys and clients. Likewise, the marital confidential communications privilege protects confidential communications made by one spouse to another during marriage and exists beyond divorce. Id. It promotes open and honest communication between spouses, which, in turn, aims to facilitate marital harmony. In 2006, the Federal Rules of Civil Procedure were amended to include the phrase "electronically stored information," and, since then, courts have made it clear that the mode of communication does not destroy privilege. *Scott v. Beth Israel Med. Center Inc.*, 17 Misc. 3d 934, (New York Co., N.Y., Sup. Ct. 2007). On the contrary, privilege extends to e-mails and other forms of electronic communication.

So when an employee uses the corporate server or an employer-provided computer to send communications to an attorney or spouse, how do courts determine whether privilege has been waived so that the employer can have free access to those communications? Does it matter if the employee uses a personal e-mail account or personal computer?

In determining the parties' respective rights to communications sent from work, the few courts to consider the issue have generally employed a balancing test, which primarily considers the following factors: Does the employer have an e-mail policy? How are employees made aware of the policy? Is the policy uniformly applied? What precautions, if any, did the employee take to protect the confidentiality of the communication?

Notably, whether the employer pays for the e-mail account is not dispositive, because an employer does not necessarily "own" e-mails merely because it pays for the account from which they were sent. *Rozell v. Ross-Holst*, No. 05 Civ. 2936, 2006 U.S. Dist. Lexis 2277 (S.D.N.Y. Jan. 20, 2006), summary judgment granted in part, denied in part, and objection overruled by 2007 U.S. Dist. Lexis 46450 (S.D.N.Y. June 21, 2007).

Clear and well-communicated

The first factor that courts consider when determining whether privilege has been waived is whether the employer had a clear and well-communicated e-mail policy in place. *In re Asia Global Crossing Ltd.*, 322 B.R. 247 (S.D.N.Y. 2005). As illustrated in *Nat'l Econ. Research Assocs. Inc. v. Evans*, No. 04-2618-BLS2, 2006 WL 2440008 (Suffolk Co., Mass., Super. Ct. Aug. 3, 2006), the exact wording of the policy is possibly the most influential factor in a waiver-of-privilege analysis. There, the court's conclusion that the employee had not waived privilege as to e-mails sent to his attorney from a personal Yahoo! account while at work or on his work computer hinged on the exact wording of his employer's policy.

The court explained: "Based on the warnings furnished in the Manual, Evans could not reasonably expect to communicate in confidence with his private attorney if Evans e-mailed his attorney using his NERA [the employer] e-mail address through the NERA Intranet, because the Manual plainly warned Evans that e-mails on the network could be read by NERA network administrators. The Manual, however, did not expressly declare that it would monitor the content of Internet communications....[T]he Manual did not expressly declare, or even implicitly suggest, that NERA would monitor the content of e-mail communications made from an employee's personal e-mail account via the Internet whenever those communications were viewed on a NERA-issued computer. Nor did NERA warn its employees that the content of such Internet e-mail communications is stored on the hard disk of a NERA–issued computer and therefore capable of being read by NERA." Id. at *3.

Under the reasoning of *Nat'l Econ. Research Assocs.*, to ensure access to employee e-mails, employers need to draft broad use-and-monitoring policies that limit personal use of e-mail and other electronic means of communication, and to state that all communications transmitted by, received from, created and/or stored in the corporate server are employer property in which employees have no right of privacy. In drafting these policies, companies should strongly consider including restrictions

Elise M. Bloom is a partner in the labor and employment department at New York-based Proskauer Rose. Abigail L. Perdue, a law clerk at the firm, contributed to this article.

on Internet blogging and message board posting.

Implementing a clear e-mail policy is not enough. Employers also must take steps to ensure that their employees are aware of the policy. See *In re Asia Global Crossing* and *Nat'l Econ. Research Assocs*. Only if employees know of the policy will it diminish any expectation of confidentiality. See *Scott v. Beth Israel Med. Center Inc.* Although some courts presume that employees in supervisory positions are on notice of their employers' policies, if an employer desires full access to employee e-mails, even those sent to spouses or attorneys, it should notify all employees that all e-mails are stored on their employer-provided computers and expressly reserve the right to retrieve and read those communications. See *Nat'l Econ. Research Assocs.* An employer can better ensure that its employees have notice of its policy by posting it in conspicuous workplace locations, including it in the handbook, and frequently reminding employees of its existence.

Because the consistency and frequency of the policy's enforcement is indicative of whether employees are aware of the policy and thus have no reasonable expectation of privacy in the e-mails at issue, employers should consistently enforce and uniformly apply their e-mail policies. Inconsistent or sporadic enforcement will leave employees with insufficient notice and perhaps lull them into a false sense of security. *Curto v. Med. World Communications Inc.*, No. 03CV6327, 2006 U.S. Dist. Lexis 29387 (E.D.N.Y. May 15, 2006), objection overruled by, objection sustained by, in part, remanded by, 2007 U.S. Dist. Lexis 35464 (E.D.N.Y. May 15, 2007). In *Curto*, an employee used employer-provided laptops to work from a home office. She claimed that before returning her laptops, she always deleted personal e-mails from them, including attorney-client communications regarding a subsequent suit against the employer. The employer only monitored employee e-mail use in limited instances, such as downloading pornography and playing online poker. Therefore, despite the fact that the employee signed an employee handbook that contained her employer's e-mail policy, the court ultimately concluded that the employer's inconsistent enforcement of the policy was insufficient to destroy the employee's reasonable expectation of privacy as to the e-mails at issue.

Most recently, some courts have held that even when an employer implements, consistently enforces and makes employees aware of its clear e-mail policy, public policy concerns may trump those factors in the waiver-of-privilege analysis. As the court in *Sims v. Lakeside School,* No. C06-1412RSM, 2007 WL 2745367 (W.D. Wash. Sept. 20, 2007), explained, public policy dictates that communications to one's attorney or spouse be protected "to preserve the sanctity of communications made in confidence." Id. at *2. There, the court held that the clear phrasing of the employer's e-mail policy, which stated that user accounts were school property and to be used solely for academic and administrative purposes, destroyed the employee's expectation of privacy. However, because public policy concerns factored more heavily in its analysis, it still held that the employee had not waived privilege.

Waiver of privilege

Finally, the waiver-of-privilege analysis often turns on the reasonable precautions that an employee takes to protect the confidential nature of the communication. Sometimes these precautions actually outweigh other factors in the analysis, such as the existence and wording of an e-mail policy. Not surprisingly, this factor has become especially relevant in recent years, as employees have become increasingly tech-savvy. In fact, the greater the measures that an employee takes to segregate and secure personal e-mails and files, the likelier the court is to find that the employee did not waive privilege as to those materials.

Sending personal e-mails via a personal, rather than corporate, account illustrates the type of reasonable precaution often sufficient to preserve privilege. See *Nat'l Econ. Research Assocs*. Similarly, not forwarding personal e-mails to a corporate e-mail address, not saving or storing them in the "My Documents" folder on an employer-issued computer or laptop and deleting personal files from and running a "disk defragmenter" on employer-issued laptops before returning them have also been deemed sufficient to preserve privilege. Id.

However, not all seemingly reasonable precautions are sufficient to preserve privilege. For instance, employees who think that sending e-mails from a personal home computer or laptop will always protect their privacy should think again. Recently, some courts have permitted forensic imaging of employees' home computers, even over objections that doing so invades the privacy of the employee and his or her family. In *Ball v. Versar Inc.*, for instance, the court granted access to "all work and home computer systems known to have been used by [plaintiff Roy O.] Ball from 1996 to September 2004 for inspection and analysis by [defendant] Versar's technical consultant." 2005 U.S. Dist. Lexis 24351 (S.D. Ind. Sept. 23, 2005); motions ruled upon by 2005 U.S. Dist. Lexis 42995 (S.D. Ind. Nov. 23, 2005); partial summary judgment granted in part, denied in part, and motion denied by 2006 U.S. Dist. Lexis 63358 (S.D. Ind. 2006).

The heart of the case

Other courts deny unfettered access to a party's personal computer, unless the computer's contents go to the "heart of the case." *Hedenburg v. Aramark Am. Food Servs.*, No. C06-5267, 2007 U.S. Dist. Lexis 3443 (W.D. Wash. Jan. 17, 2007), summary judgment granted by, motion to strike denied by, claim dismissed by 2007 U.S. Dist. Lexis 14415 (W.D. Wash. March 1, 2007). For example, the court in *Hedenburg* denied an employer's motion to compel production of an employee's home computer because the employee's personal e-mails with unnamed third parties might reveal discrepancies in her testimony. The court said that the company's request was nothing more than an improper attempt to troll for impeachment evidence. As the court explained, the computer's contents did not go to the "heart of the case," and the employer's central claims were wholly unrelated to the contents of the employee's computer. Similarly, in *Benton v. Dlorah*, No. 06-CV-2488, 2007 WL 2225946 (D. Kan. Aug. 1, 2007), the employer claimed that the employee's failure to produce any e-mails beyond February 2007 led it to suspect that she had been deleting relevant e-mails since then. The court denied the employer's motion to compel production of the employee's personal computer to facilitate recovery of allegedly deleted relevant e-mails because it found "nothing to lead to such an inference, beyond speculation." Id. Compare *Benton*, No. 06-CV-2488, 2007 U.S. Dist. Lexis 80503 (D. Kan. Oct. 30, 2007) (ordering the plaintiff to produce certain specific e-mails likely relevant to the case—and if the e-mails had been deleted, then to produce for inspection her computer hard drive from which the e-mails had been sent).

Employee e-mail can provide good information in defending employment-related claims. To maximize their ability to access such e-mails, employers should take steps to diminish employees' expectations of privacy in their electronic communications. Given that employees are increasingly tech-savvy and thereby likelier to take reasonable precautions sufficient to preserve privilege, tipping the court's balancing of interests in employers' favor is increasingly challenging. In this environment, the stronger and clearer the message that all employee e-mails sent from work or through the employer's server are employer property, despite whatever measures employees take to preserve privilege, the greater is the likelihood that when courts are asked the increasingly common question, "Whose mail is it anyway?" the answer will be "The employer's." NLJ