

► **Privacy of Privileged Communications on Personal, Password-Protected E-mail Accounts**

Peter J. Gallagher



By now, nearly all companies have adopted policies governing the use of company computers by their employees. The advice most often given when developing these policies is to make sure that they are thorough, well crafted, and widely distributed so that the company is protected against, among other things, any suggestion that they improperly reviewed an employee's communications.

While this advice is undeniably sound, questions still exist regarding whether even the most comprehensive policy can permit a company to review e-mails between employees and their counsel on private, password-protected e-mail accounts. In New Jersey, the answer to this question is almost certainly no. However, in several other states, including New York, such a policy might permit employers to monitor e-mails on private accounts, even e-mails between the employee and counsel. Whether New Jersey is at the forefront of a change in the law or stands outside of the mainstream on this issue remains to be seen. Nonetheless, it is important for companies with employees and computers in multiple locations across the country to be aware of the different standards that currently apply in different jurisdictions and structure their policies accordingly.

As noted above, whether employers in New Jersey can monitor attorney-client communications on private, password-protected e-mail accounts appears well settled. In *Stengart v. Loving Care Agency, Inc.*, 201 N.J. 300 (2010), the Supreme Court ruled that employees have a reasonable expectation of privacy when using company-owned computers to communicate with counsel, at least when such communications are made using a private, password-protected e-mail account as opposed to the employee's company account. The Supreme Court held that, by using a private e-mail account, an employee takes reasonable steps to keep these communications confidential, and thus maintains a reasonable expectation of privacy in the employee's e-mails with counsel.

The internet usage policy at issue in *Loving Care* permitted the "occasional personal use" of e-mails and did not indicate whether the contents of e-mails sent via personal accounts could be retrieved by the company. The New Jersey Supreme Court ruled that this policy "created doubt about whether those e-mails are company or private property." *Id.* at 322. However, the Supreme Court was quick to point out that a more restrictive policy – one that purported to render attorney-client communications, wherever made, fair game for review by the company – would not be permitted:

Because of the important public policy concerns underlying the attorney-client privilege, even a more clearly written company manual – that is, a policy that banned all personal computer use and provided unambiguous notice that an employer could retrieve and read an employee's attorney-client communications, if accessed on a personal, password-protected e-mail account using the company's computer system – would not be enforceable.

*Id.* at 325. Thus the New Jersey Supreme Court went beyond the narrow issue presented by the case before it to announce a bright-line rule that employers cannot read attorney-client e-mails exchanged by their employees on personal password-protected accounts.

In other jurisdictions, however, including right across the river in New York, the extent to which an employer may review its employees' e-mails, sent on company computers but using a private password-protected account, is not so clear. For example, the U.S. District Court for the Southern District of New York held that e-mails sent by an employee to counsel on a company computer using the employee's private, password-protected account were not privileged because the employer's computer use policy prohibited personal use and permitted employer review of all data "flowing through its system." *Long v. Marubeni America Corp.*, 2006 WL 2998671 (S.D.N.Y. Oct. 19, 2006).

However, the U.S. District Court for the Eastern District of New York concluded that an employee had a reasonable expectation of privacy in e-mails that she sent through her personal e-mail account, which did not go through her employer's server, particularly because the employer failed to enforce its computer usage policy. *Curto v. Medical World Communications, Inc.*, 2006 WL 1318387 (E.D.N.Y. May 15, 2006); see also *National Economic Research Associates, Inc. v. Evans*, 2006 WL 2440008 (Aug. 3, 2006 Mass. Superior Court) (holding that employer was not permitted to review

attorney-client communications sent via a private password-protected e-mail account and stored in a temporary file because, among other things, the company did not notify the employee that such files were stored by the employer and subject to retrieval and review). Accordingly, in jurisdictions like New York, the question of whether an employer can review e-mails sent by its own employees to their private counsel on company computers, but using password-protected e-mail accounts, remains unsettled.

To be clear, the uncertainty arises only in connection with e-mails sent using personal, private, password-protected e-mail accounts, not company e-mail accounts. The law in most jurisdictions is settled that, provided an employer has a comprehensive and well-publicized computer usage policy, all e-mails sent using the employer's e-mail account, including e-mails to counsel, are not privileged and are subject to review by the employer. One New York court ruled that the effect of comprehensive computer usage policies is "to have the employer looking over your shoulder each time you send an e-mail," a situation that would obviously negate any claim of privilege. *Scott v. Beth Israel Medical Center*, 17 Misc. 3d 934, 938 (Sup. Ct. 2007). Similarly, a California court held that, in the face of a computer usage policy that indicated that all company e-mails were subject to review, an employee's e-mails with counsel over her employer's e-mail system were "akin to consulting her lawyer in her employer's conference room, in a loud voice, with the door open, so that any reasonable person would expect that their discussion of her complaints about her employer would be overheard by him." *Holmes v. Petrovich Dev. Co., LLC*, 191 Cal. App. 4th 1047, 1051 (Cal. Ct. App. 3d Dist. 2011).

Finally, the American Bar Association recently issued an ethics opinion on the obligations of in-house counsel who discover communications between an employee and the employee's private counsel (*Opinion 11-460*). The ABA concluded that there was no ethical obligation under Model Rule of Professional Conduct 4.4(b) to notify an employee's lawyer when the employer discovers the employee's private communications with counsel "in the employee's business e-mail file or on the employee's workplace computer or other device." The ABA reasoned that Rule 4.4(b) deals only with documents that are "inadvertently sent," which is not the case when documents are "retrieved by a third person from a public or private place where it is stored or left." However, even without an obligation to notify opposing counsel, the ABA noted that it would "often [] be in the [employer's] best interest to give notice and obtain a judicial ruling as to the admissibility of the employee's attorney-client communications before attempting to use them," because this "minimizes the risk of disqualification or other sanction if the court ultimately concludes that the opposing party's communications with counsel are privileged and admissible."

A recent decision from the U.S. District Court for the Northern District of California, *Terraphase Engineering, Inc., et al. v. Arcadis, U.S., Inc.*, reveals the wisdom of the ABA's advice. In *Arcadis*, the defendant/employer's outside counsel and one of its in-house attorneys reviewed and relied upon e-mails that had been sent to a former employee's company e-mail address by an attorney representing the former employee in a lawsuit against the employer. The employee sought a protective order preventing the employer from using the e-mails in any way during the lawsuit. In response, the employer and its counsel argued, among other things, that their review of the e-mails was appropriate because they were sent "unsolicited" to the individual employee's work e-mail, in which the employee had no reasonable expectation of privacy. The district court emphatically disagreed, and punished the employer by: disqualifying its outside counsel and the in-house counsel who reviewed the e-mails; ruling that the general counsel must be "removed from all aspects of the day-to-day management of the case, including . . . making any substantive or strategic decisions with regard to the case;" ordering that the employer dismiss its counterclaim without prejudice to re-filing the pleading with new counsel; and awarding the employee costs and fees in connection with bringing the motion for protective order. Thus, although the scenario presented in *Arcadis* was almost identical to the hypothetical presented by the ABA in *Opinion 11-460*, the result reached by the district court was decidedly different than the one articulated by the ABA.

Ultimately, what these decisions make clear is that it is crucial for employers, particularly those with a regional or nationwide presence, to understand the law in each state in which they have offices. As the situation with New York and New Jersey demonstrates, a practice or policy that may be appropriate in one state may be entirely inappropriate in a neighboring state.

---

*Peter Gallagher is a commercial litigator at Porzio, Bromberg & Newman, P.C. and an adjunct professor at the Seton Hall University School of Law.*