

SOUTHERN DISTRICT CIVIL PRACTICE ROUNDUP

Expert Analysis

Work E-Mail: Clients Beware

E-mail unquestionably enhances the quality of many individual representations. But when clients use their work e-mails, systems or devices to communicate with their lawyers, they may, unwittingly, compromise the privileged nature of those communications, exposing those candid exchanges to their adversaries or to regulators and prosecutors. For some time, many lawyers have advised clients to use personal, web-based e-mail for attorney-client communications, and to refrain from sending e-mails and text messages from their employer-issued BlackBerrys—instructions all too often observed in the breach. A growing body of case law, and a recent opinion issued by the American Bar Association, make clear that lawyers must help clients assess the risks of sending e-mails from work systems or devices.

The 'Asia Global' Factors

The first court in the Southern District of New York to address the question of whether communications that would otherwise be privileged lose that character because they are sent over an employer e-mail system or computer, was the U.S. Bankruptcy Court in *In re Asia Global Crossing, Ltd.*¹ In that case, a bankruptcy trustee sought e-mails sent by the debtor's former employees to their personal attorneys over the debtor's e-mail system—a request resisted by the former employees on the grounds of attorney-client privilege. In the context of e-mail sent through an employer's computer system, the court reasoned that an employee's expectations of confidentiality (essential for any claim of privilege) are closely linked to his or her expectations of privacy, which in turn depend on office practice and procedure.

The *Asia Global* court then articulated a four-factor test, which has been widely adopted as the standard for evaluating claims of privilege for e-mails sent from or through employer devices or systems: (1) Does the employer maintain an e-mail policy banning personal or other objectionable use? (2) Does the employer monitor the use of the employee's computer or e-mail? (3) Do third parties have a right of access to the computer or e-mails? and (4) Did the employer notify the employee, or



By
**Edward M.
Spiro**



And
**Judith L.
Mogul**

was the employee aware, of the use and monitoring policies?²

Applying these factors to the trustee's motion to compel production of the attorney-client communications, the court concluded that the evidence was sufficiently equivocal as to what the company's policies regarding use and monitoring of e-mail were, and how those policies were communicated to the employees, that they could not eliminate any privilege that otherwise existed.

Determinative Factors—Nature of the E-Mail Account or Employer Policy? The employees in *Asia Global* used their company e-mail accounts to transmit the communications at issue in that case. Because the employer had access to its own servers, the court concluded that "sending a message over the debtor's e-mail system was like placing a copy of that message in the company files."³ But the court did not find this factor determinative, focusing instead on the company's use and monitoring policies to determine the reasonableness of the employees' expectation of confidentiality.

It observed that this policy- and practice-based inquiry requires a case-by-case analysis, and indeed the post-*Asia Global* cases have been highly fact-specific, examining the circumstances in which the party asserting the privilege created and sent the communication, and finely parsing the employer's e-mail policies and notice procedures. Yet the factor that appears to be among the most determinative is whether the employee was using a work e-mail account, or a personal, password-protected e-mail account albeit accessed from an employer's computer—a consideration that did not inform the *Asia Global* analysis.⁴

For example, in *Curto v. Medical World Communications Inc.*,⁵ Judge Denis R. Hurley of the U.S. District Court for the Eastern District of New York refused to find a privilege waiver for communications sent by the plaintiff to her attorney from the defendant-employer's computer even in the face of an explicit company policy requiring employees

to waive any expectation of privacy in material created, stored or sent on a company computer. The plaintiff had communicated with her attorney through a personal, web-based, password-protected e-mail account, from company computers that she used from her home office. When she returned those computers to her employer she took steps to delete all personal files. However, with the assistance of a forensic consultant, the company was able to restore some of her communications with counsel.

Judge Hurley affirmed the magistrate judge's decision upholding the employee's assertion of the privilege. The court framed the issue as one of inadvertent production rather than as an expectation of confidentiality question, finding that use of a personal AOL account that did not go through the defendant's servers, and the plaintiff's attempts to delete the confidential communications constituted reasonable steps to maintain confidentiality.

Acknowledging the *Asia Global* focus on company policy, the *Curto* court endorsed an additional gloss on the *Asia Global* test—looking not just to the policy as articulated, but also to how it was enforced. Here, the company's sporadic enforcement of its policy prohibiting personal use of its computers "created a false sense of security" that the policy would not be enforced. Finally, the court stressed that its holding was limited to the circumstance of an employee's use of a company computer in her own home, and did not extend to an employee's expectations of privacy in office computers generally.

In its decision last year in *Stengart v. Loving Care Agency Inc.*,⁶ the New Jersey Supreme Court took a more permissive view of e-mailing from work, holding that an employee had a reasonable expectation of privacy with respect to attorney-client e-mails sent through a personal e-mail account but opened or sent from a work computer. The employer's e-mail policy permitted occasional personal use but the company reserved the right to "review, audit, intercept, access and disclose all matters on the company's media systems and services."

Because the policy made no reference to personal e-mail accounts, the court found that employees did not have express notice that e-mails from or to personal accounts were subject to monitoring. It went on to hold that even though companies have legitimate interests in monitoring the use of their systems and equipment to protect business assets, reputation and productivity, a company has no need to read the content of attorney-client communications in order to enforce those policies. The

EDWARD M. SPIRO and JUDITH L. MOGUL are principals of *Morvillo, Abramowitz, Grand, Iason, Anello & Bohrer*, both concentrating in commercial litigation. Mr. Spiro is co-author of "Civil Practice in the Southern District of New York," 2d Ed. (Thomson West 2010).

court concluded that in light of the important public policy underlying the attorney-client privilege, “even a more clearly written [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.”⁷

If *Curto* and *Stengart* represent the end of the spectrum where an employee’s expectation of confidentiality is most reasonable, the New York State Supreme Court decision in *Scott v. Beth Israel Medical Center Inc.*⁸ illustrates the other end of the spectrum, and the one that more closely approximates the circumstances in which uncounseled clients might find themselves. The plaintiff in that case had communicated with his attorney concerning matters relevant to a dispute with his employer over his company e-mail account. Company policy provided that company equipment and systems were company property and should be used only for business purposes, and that employees had no personal privacy in any material created, received, saved or sent using the company systems. Under the policy, the company reserved the right to access and disclose such material without notice.

Justice Charles E. Ramos held that the plaintiff’s use of the company’s e-mail to communicate with his attorney rendered the communication one “not made in confidence” and thus unprivileged. Relying on *Asia Global* (in the absence of state cases on point), the court found that the company’s e-mail policy banned personal use, and that even though the company acknowledged that it did not monitor the plaintiff’s e-mails, the fact that it could do so under the policy satisfied the second *Asia Global* factor. The court reasoned that the third factor—third-party access—was not relevant in light of CPLR 4548, which provides that access by “persons necessary for the delivery or facilitation of [e-mail] communication” may do so without destroying the privilege. As for the fourth *Asia Global* factor concerning notice, despite plaintiff’s protest that he was unaware of the policy, the court found that he had actual notice because the policy had been sent to him and was posted on the Internet, and constructive notice as a consequence of his status as an administrator charged with knowledge of company policy.⁹

Many cases exploring the question of privilege for e-mails sent from an employer computer or e-mail arise in the context of employment disputes, where the employer seeks information created on or sent through its own systems or equipment. Recently, in *In re Reserve Fund Securities and Derivative Litigation*,¹⁰ the request for e-mails that would otherwise be privileged but for the fact they were sent over the defendant’s work e-mail came from the U.S. Securities and Exchange Commission, not the employer.

In its enforcement action arising out of the collapse of the Reserve Primary Fund, the SEC sought production of a series of e-mails sent between Bruce Bent II, the vice chairman and president of the Reserve Management Company Inc., and his wife, in the “crucial two-day period” following the Lehman bankruptcy. Southern District Judge Paul G. Gardephe drew no distinction between the marital privilege and the attorney-client privilege, analyzing Bent’s claim of marital privilege under the *Asia Global* test. He granted the SEC’s motion

to compel because the e-mails were sent using a company computer and over the company e-mail system, and were stored on the company server.

Judge Gardephe focused closely on the company’s e-mail policy, which prohibited employees from using any e-mail account other than the company’s while on company premises and provided that employees “should limit their use of the e-mail resources to official business.” The policy instructed that if employees received personal messages, they should delete them and remove “personal and transitory messages from personal inboxes on a regular basis.” The policy also reminded employees that e-mail communications were automatically saved and could be disclosed to regulators.

Judge Gardephe concluded that this policy “clearly bans personal use of [the company’s] email system,” rejecting Bent’s argument that the personal use policy was aspirational rather than mandatory, by virtue of its use of the word “should.” He also found unpersuasive Bent’s argument that because the policy had instructions to delete personal e-mails, it somehow authorized personal use of the company’s e-mail system.

The factor that appears to be among the most determinative is whether the employee was using a work e-mail account, or a personal, password-protected e-mail account.

Although its policy stated that the company would not routinely monitor employee e-mails, Judge Gardephe specifically rejected Bent’s argument, based in part on *Curto*, that he should consider how the policy was applied or enforced rather than relying entirely on the written policy.¹¹ He also held that the warning about possible disclosure to regulators satisfied the third *Asia Global* factor concerning third-party access. Because Bent apparently acknowledged notice of the policy as written, Judge Gardephe concluded that all four factors weighed against an expectation of privacy and granted the SEC’s motion to compel.

Ethical Responsibilities

In August 2011, the American Bar Association weighed in on this topic, issuing a formal opinion titled “Duty to Protect the Confidentiality of E-Mail Communications with One’s Client.”¹² In that opinion, the ABA instructs that lawyers who engage in e-mail communication with their clients “must ordinarily warn the client about the risk of sending or receiving [such communications] where there is a significant risk that a third party may gain access.”

In a lengthy accompanying explanation, the ABA Ethics Committee noted the evolving and not entirely consistent approach that courts have taken in assessing the impact of employer e-mail policies on privilege. Declining to express a view on when attorney-client communications sent over workplace devices or systems will be protected, it concluded that as soon as practical after the client-lawyer relationship is established, a lawyer should typically instruct a client to refrain from using a workplace device or system for sensitive or substantive communications. It also questioned

whether that admonition should extend to ministerial communications, observing that even issues of scheduling can have substantive ramifications.

The ABA Opinion frames its discussion in terms of a hypothetical client in an employment dispute who uses an employer computer or e-mail account for sensitive attorney-client communication—a scenario that arguably presents the most extreme risk of access.¹³ It does not explore any distinction between work e-mail accounts and personal, web-based accounts accessed on employer devices, which may, in other contexts, change the risk calculus.

Conclusion

Attorneys should help their clients understand their employers’ e-mail and computer use policies and assist them in weighing the risks and benefits of different approaches to communication. In many circumstances they should advise clients to establish personal, web-based e-mail accounts and encourage them to use those accounts for sensitive communications.

.....●●.....

1. 322 B.R. 247 (Bankr. S.D.N.Y. 2005) (Bernstein, C.J.)

2. *Id.* at 257.

3. *Id.* at 259.

4. As was the case in *Asia Global*, some courts have upheld the privilege for communications sent on an employer e-mail account. See, e.g., *Convertino v. U.S. Dept. of Justice*, 674 F.Supp.2d 97 (D.D.C. 2009) (denying plaintiff’s motion to compel production of Justice Department employee’s e-mail sent to private attorney on work e-mail account). Our research has not located any cases holding that use of a private password-protected e-mail from a work computer waives privilege.

5. 2006 WL 1318387 (E.D.N.Y. May 15, 2006).

6. 201 N.J. 300 (2010).

7. *Id.* at 325. See also *National Economic Research Assoc. v. Evans*, 2006 WL 2440008 (Mass. Super. Ct. Aug. 3, 2006) (employee had reasonable expectation of privacy for e-mails sent through private e-mail account, where policy spoke only of company monitoring of communications sent through company intranet, not through Internet or private e-mail accounts).

8. 17 Misc.3d 934, 847 N.Y.S.2d 436, 444 (N.Y. Sup. Ct. 2007).

9. See also *United States v. Etkin*, 2008 WL 482281 (S.D.N.Y. Feb. 20, 2008) (Karas, J.) (no marital privilege for e-mail (hard copy of which was found in criminal defendant’s car) that defendant sent to wife from work computer which had a notice at log-in warning that use of computer constituted express consent to monitoring and interception of information on system).

10. 2011 WL 2039758 (S.D.N.Y. May 23, 2011).

11. Judge Gardephe distinguished *Curto* on several grounds, including that it was an “inadvertent disclosure case,” and because it was not even clear that the employer’s e-mail policy applied, inasmuch as the plaintiff’s computers in her home office were not connected to the employer’s computer system.

12. American Bar Association, Standing Committee on Ethics and Professional Responsibility, Formal Opinion 11-459 (Aug. 4, 2011).

13. The opinion also notes the risks in using any computer that is not fully private, including borrowed computers and those in hotels or libraries, or, in the context of a matrimonial dispute, even a home computer to which other family members have access.