



DIGITAL DISCOVERY & E-EVIDENCE



VOL. 8, NO. 5

REPORT

MAY 1, 2008

Reproduced with permission from Digital Discovery & e-Evidence, Vol. 08, No. 05, 05/01/2008. Copyright © 2008 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

INADVERTENT WAIVER

Are You at Risk of Waiving the Attorney-Client Privilege by Using Your Employer’s Computer Systems to Communicate With a Personal Attorney?

By **MATTHEW J. HERRINGTON**
AND **WILLIAM T. GORDON**

You are the CEO of a multi-national corporation under investigation by the SEC and the Department of Justice for potential securities violations—the civil suits have just started coming through the mail slot. Confident of your complete innocence, but mindful of recent high-level corporate prosecutions, you decide to consult with your personal attorney to ensure that

you continue to do nothing wrong. During the course of your normal work day, you prepare a summary of what you know and exchange a few e-mails with your attorney using your company computer. You probably don’t remember that computer use policy you signed off on three years ago. Did you know that you may have just inadvertently waived the attorney-client privilege in those communications?

Legal services are best provided when a client understands that her confidential communications with counsel will not be subject to the scrutiny of third parties. Under federal law and many state laws, the “client has a privilege to refuse to disclose and to prevent any other person from disclosing confidential communications made for the purpose of facilitating the rendition of professional legal services to the client.”¹

A communication is considered confidential “when the circumstances indicate that it was not intended to be disclosed to third persons other than (1) those to whom disclosure is in furtherance of the rendition of legal services to the client, or (2) those reasonably necessary for the transmission of the communication.”²

Matthew J. Herrington, a 1993 graduate of the Yale Law School, is a partner in the Washington office of Steptoe & Johnson LLP, where he is a member of the Litigation Department. Mr. Herrington’s practice focuses primarily on white-collar defense, Congressional investigations, internal investigations, and complex civil litigation.

William T. Gordon graduated with honors from Harvard Law School in 2007. He is an associate in the Washington office of Steptoe & Johnson LLP, where he is a member of the International Department. He assists in conducting internal investigations and compliance audits, and works with companies to develop compliance procedures.

¹ *In re Asia Global Crossing, Ltd.*, 322 B.R. 247, 255 (Bankr. S.D.N.Y. 2005) (citation omitted) (quotation omitted).

² *Id.* (citation omitted).

Impact of E-Mail. The emergence of e-mail as a standard form of communication, however, has greatly muddied the waters on this issue. Questions of waiver emerge when an employee uses the computer systems of an employer to communicate with a personal attorney. Under such circumstances, an employer can claim that because an employee used its computer systems to transmit a communication, the employee waived the attorney-client privilege.³ There is no reason to think enforcement authorities are far behind in adopting this reasoning.

In response to such issues, some states, including New York and California, have enacted laws that protect e-mail communications.⁴ But no false comfort should be taken from these limited legislative fixes.

Case Law. In the 2007 case of *Scott v. Beth Israel Medical Center Inc.*,⁵ a New York court held that a physician's e-mail communications with his attorney, sent using the hospital's e-mail server, were not confidential, for the purposes of attorney-client privilege.⁶ The court determined that Dr. Scott waived the privilege because he should have known that the hospital maintained the right to monitor employee e-mails.

The court emphasized that in his position as a hospital administrator, Dr. Scott required "newly hired doctors under his supervision to acknowledge in writing that they were aware of the policy" that employees were not to use hospital computers for personal use and that the hospital retained the right to monitor employee use of hospital computers.⁷

Although the hospital admitted that it had not previously monitored Dr. Scott's e-mail, the court held that due to the nature of Scott's administrative position, Dr. Scott could not reasonably claim that he did not know that the policy could be enforced.⁸ Therefore, Dr. Scott's transmission of electronic communications via the hospital's e-mail server waived the attorney-client privilege in those communications.

Reasonable Expectations. *Beth Israel Medical Center* cannot be dismissed as an outlier. Rather, it exemplifies a trend in which courts will examine the specific facts of each case to determine whether the employee's expectation of confidentiality is reasonable.

The employee's expectation of privacy is only the starting point for the analysis.⁹ Frighteningly, given the

amount of attention accorded to such policies, "actual office practices and procedures" of the employer can play an important role in assessing the reasonableness of an employee's expectation of privacy, and thus, the legal status of their communications with an attorney.¹⁰

For example, in *Long v. Marubeni America Corporation*,¹¹ a U.S. district court held that an employee could claim no privilege in e-mails exchanged with his attorney because his employer had a formal "no personal use" policy. In *Long*, the employer sent annual reminders to employees that the employer reserved the right to monitor company computers and data flowing through its internal systems.¹²

Thus, the court reasoned that the employee could not claim ignorance of the employer's policy. Accordingly, the court held that the employee's voluntary disregard of the policy "stripped from the e-mail messages . . . the confidential cloak . . . of the attorney-client privilege."¹³

Knowledge Critical. Employee knowledge of a computer usage policy will likely be held to be critical to determining whether the privilege has been waived.¹⁴ In *Transocean Capital Inc. v. Fortin*, a Massachusetts court held that for an employer to successfully argue that attorney-client privilege was waived by the use of an employer's computer system, an employee must have knowledge of the employer's policy of monitoring the information transmitted on its servers.¹⁵

In *Transocean*, the court ruled that no information from the record suggested that the employee had knowledge of any such policy.¹⁶ Although the employer retained a third party to handle various human resources matters, the court was unable to determine that the employer had adopted the computer policies outlined by the third-party.

If the employer had "informed its directors, officers, or employees that it was adopting" the third-party's computer usage policies as its own, the court suggested that it would rule that the privilege had been waived.¹⁷ But since the court could not make this determination, the court ruled that the use of the employer's e-mail address and computer system did not break the attorney-client privilege.¹⁸

Likewise, in *National Economic Research Associates Inc. v. Evans*,¹⁹ the court held that unless an employee understands, based on the employer's computer usage policy that its communications with its attorney can be examined by the employer, the privilege is not waived.

In that case, an employee used his personal Yahoo e-mail account to send confidential communications to his attorney. The employer utilized a strict computer usage policy that the court believed the employee understood.²⁰

³ Such an argument rests on the technical nature of many employer computer systems. Many systems rely on an internal server with the capability of storing and monitoring the use of all who use the system. Due to this capability, employers sometimes argue that because the employee either knew, or should have known, about this capability, they implicitly waived the attorney-client relationship by using the employer's e-mail system.

⁴ New York Civil Practice Law and Rules § 4548 states that a privileged communication does not "lose its privileged character for the sole reason" that it was sent by e-mail "or because persons necessary for the delivery or facilitation [of the e-mail] may have access to the content. . ." N.Y.C.P.L.R. § 4548 (McKinney 2007); see also, e.g., Cal. Evid. Code § 917(b)(2004).

⁵ 847 N.Y.S.2d 436 (N.Y. Sup. Ct. 2007), available at 2007 WL 3053351.

⁶ *Id.*

⁷ *Id.*

⁸ *Id.*

⁹ *O'Connor v. Ortega*, 480 U.S. 709, 718-19 (1987).

¹⁰ *Id.* at 717.

¹¹ 2006 WL 2998671 (S.D.N.Y. Oct. 19, 2006).

¹² *Id.* at *3.

¹³ *Id.*

¹⁴ *Transocean Capital Inc. v. Fortin*, No. Civ. A. 05-0955-BLS2 2006, WL 3246401 (Mass. Super. Ct. Oct. 20, 2006).

¹⁵ *Id.* at *4.

¹⁶ *Id.*

¹⁷ *Id.*

¹⁸ *Id.*

¹⁹ No. 04-2618-BLS2, (Mass. Super. Ct. Suffolk Cty. Aug. 2, 2006).

²⁰ *Id.* at 5.

However, based on the language of the policy, the court did not believe that a reasonable employee with knowledge of the employer's policy could understand that a forensic computer expert could retrieve "screen shots" of e-mail sent using an employee's personal e-mail account.²¹ Thus, the court held that because the employer's manual failed to warn clearly that any e-mails sent using a company computer, including those sent via a private e-mail account, could be accessed by the company, the privilege had not been waived.²² Had such clear language existed, the "reasonable person" should have expected that its employer could access the e-mails, and under such circumstances, the privilege might have been waived.²³

A similar approach was adopted in *In re Asia Global Crossing*,²⁴ where the court proffered the following four factor test to determine whether an e-mail sent over an employer's e-mail server waived attorney-client privilege:

- (1) Does the corporation maintain a policy banning personal or other objectionable use?
- (2) Does the company 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 corporation notify the employee, or was the employee aware, of the use and monitoring policies?²⁵

Thus, the court determined that an employer's enforcement of its computer policy could play a role in deciding whether the employee should have expected confidentiality in his electronic communications, and whether attorney-client privilege was waived.²⁶

The parent company, Global Crossing, had a computer usage and e-mail policy that allowed the employer to monitor employee use.²⁷ No evidence existed that its subsidiary, Asia Global Crossing, ever adopted the policy, or informed its employees of the policy.²⁸ Because the record was inconclusive as to whether Asia Global Crossing possessed a computer policy or if any such policy had been communicated to its employees, the court could not determine whether waiver had occurred.²⁹

Enforcement. In a subsequent case, *Curto v. Medical World Communications, Inc.*,³⁰ a district court upheld a magistrate's decision that the non-enforcement of a computer policy could play a role in evaluating whether an employee has waived attorney-client privilege.³¹ In *Curto*, the employee sent confidential e-mails to her at-

orney through her personal AOL account using a laptop provided by her employer for work purposes. The e-mails were sent in the employee's own home, using no employer property or resources other than the computer itself. The employer's computer usage policy prohibited the personal use of computers and was signed by the employee.

However, because the employer rarely enforced the computer usage policy, the judge found that the policy created a "false sense of security," which "lulled" employees into believing that the policy would not be enforced.³² Thus, the district court reinforced that courts can use the non-enforcement of a computer and e-mail policy as a factor for determining whether an employee waived attorney-client privilege through the use of the employer's computer systems.

Note, though, that non-enforcement or perceived non-enforcement of a computer policy may not always protect an employee from inadvertently waiving the privilege.³³ For example, in *Smyth v. Pillsbury Co.*, the employer assured an employee that e-mail communications would not be intercepted by the employer. The court nevertheless found that no expectation of privacy existed in e-mail sent over the employer's e-mail system.³⁴

Further complicating matters, the wording of a computer policy might also be critical to a court's determination of whether an employee's expectation of confidentiality is reasonable. For example, the court in *Curto* suggested that the computer policy did not provide employees with clear warning that their e-mail communications using company resources would be monitored.³⁵

The court contrasted the policy used by the employer in *Curto* with a policy examined in *United States v. Simons*.³⁶ In *Simons*, the policy stated that electronic auditing "shall be implemented."³⁷ The Fourth Circuit held in that case that such language "placed employees on notice that they could not reasonably expect that their internet activity would be private."³⁸

In contrast, in *Curto*, the policy stated that "employees understand that [the employer] may use human or automated means to monitor use of computer resources."³⁹ Thus, the court suggested that the wording of the policy did not place the employee on notice that the company would monitor her computer use.⁴⁰

Beware that no sense of security may be taken by the language of the policy alone. Language that permits, but does not mandate employer supervision of company computer and network servers might not prevent a court from finding that the employee could not expect that their electronic communications will be confidential.⁴¹ In *Thygeson v. Bancorp*, a court held that the employer's policy stating that it "reserves the right to

²¹ *Id.*

²² *Id.*

²³ *Id.*

²⁴ 322 B.R. at 257.

²⁵ *Id.* (footnote omitted).

²⁶ *Id.*

²⁷ *Id.* at 260.

²⁸ *Id.*

²⁹ *Id.* at 264-65.

³⁰ No. 03CV6327 (DRH) (MLO), 2006 WL 1318387 (E.D. N.Y. May 15, 2006).

³¹ In that case, the court used a different four part test than the test used in *In re Asia Global Crossing* to determine whether the attorney-client privilege had been waived. The balancing test included: "(1) the reasonableness of the precautions taken by the producing party to prevent inadvertent disclosure of privileged documents, (2) the volume of discovery versus the extent of the specific disclosure. . . , (3) the length of

time taken by the producing party to rectify the disclosure; and (4) the overarching issue of fairness." *Id.* at *3.

³² *Id.* (citation omitted) (alteration in original).

³³ *Smyth v. Pillsbury Co.*, 914 F. Supp. 97 (E.D. Pa. 1996).

³⁴ *Id.*

³⁵ *Curto*, 2006 WL 1318387, at *6.

³⁶ 206 F.3d 392 (4th Cir. 2000).

³⁷ *Id.* at 395.

³⁸ *Id.* at 398 (emphasis added).

³⁹ *Curto*, 2006 WL 1318387, at *6.

⁴⁰ *Id.*

⁴¹ *Thygeson v. Bancorp*, No. CV-03-467, 2004 WL 2066746 (D. Or. Sept. 15, 2004).

monitor any employee's e-mail and computer files for any legitimate business reason" should have nullified any expectation the employee had in the privacy of his e-mail communications.⁴²

Case Specific Results. The determination of whether an employee has inadvertently waived attorney-client privilege will be made on a case-by-case basis. Too many unanswered questions remain for anyone to feel comfortable using an employer's computer or computer server to send otherwise confidential attorney-client communications.

⁴² *Id.* at *20.

We do know that using employer information technology systems to send confidential e-mails *can* lead to waiver of the privilege. Such a determination will be heavily fact based, with the ultimate determination likely depending on the employee's reasonable expectation of privacy in any such communication. Therefore, while there may be some protection regarding computer use and the transmission of confidential electronic communications through an employer's server, the use of employer computer systems to send such communications should be approached with extreme caution.

For further information, contact Matt Herrington (202.429.8164, mherring@steptoe.com) or William Gordon (202.429.8013, wgordon@steptoe.com).