

The Perils of Employer-Provided Technology: Employer Inaction and the Attorney-Client Privilege

by Lauren E. Fisher

Employers regularly provide employees with computers, cell phones, and wireless networks, presumably—and sometimes explicitly—for business use. Employees occasionally use that technology to email their personal attorneys. Of course, for an email between attorney and client to be privileged, it must have been made in confidence.¹ Though many attorneys assume that emails sent using employer-provided technology could not have been made in confidence, and thus cannot be privileged, this oversimplified view is often incorrect.

Courts consider a combination of factors in deciding whether such emails are privileged. These include whether the employer established a policy banning personal use of company computers and email, monitored the use of its computers and email, had a right to access its computers and emails, notified employees of its policy regarding computer and email use, and implemented its computer and email use policy consistently.² If the employee can show that the employer failed in even one of these areas, the attorney-client privilege may attach to emails sent using employer technology.

First, emails between an employee and an attorney may be privileged if the employer's email policy is imprecise. For example, in *Stengart v. Loving Care Agency*,³ the employer had a policy and practice of saving a snapshot of every web page an employee viewed.⁴ As a result, the employer could examine every email sent by the employee, regardless of the email system used.⁵ Pursuant to that policy, the employer examined a past employee's hard drive and uncovered emails between the employee and her personal attorney that had been sent through a web-based email account.⁶ The employer's policy allowed for the personal use of email⁷ but did not put the employee on notice that her web-based emails were subject to monitoring.⁸ Largely because of these considerations, the court decided that

the employee's expectation of privacy in those web-based emails was reasonable.⁹

An employer's failure to enforce its email policy may also enable its employee to assert the attorney-client privilege. In *Curto v. Medical World Communications Inc.*,¹⁰ the employer acted pursuant to its email policy, as set forth clearly in its employee handbook, when it recovered Web-based emails from the laptop of a terminated employee.¹¹ However, the employer had enforced its email policy on only four prior occasions.¹² Moreover, the employer could not monitor the employee's laptop during her employment, as the policy stated it would, because the employee worked from home and used a private server that could not be accessed by the employer.¹³ Under those circumstances, the court found that the employee had a reasonable expectation of privacy in her emails to an attorney.¹⁴

An employee may also assert the privilege if his or her employer fails to effectively communicate an email policy. In *Mason v. ILS Technologies LLC*,¹⁵ the employee never agreed to abide by the employer's email policy, and whether he had even been notified of the policy's existence was hotly contested.¹⁶ Consequently, the court found that emails between the employee and his attorney and sent from through the company email system were sufficiently private to be privileged.¹⁷

Finally, if an employer interprets its email or computer use policy in a way that is inconsistent with a strict reading of the policy, that inconsistency may lead to a leak of privileged emails. In *DeGeer v. Gillis*,¹⁸ for example, the employer conducted a review of a former employee's work laptop to determine whether any privileged information existed on the computer.¹⁹ The court viewed this privilege review as material, as it contradicted the employer's position that no information stored on the

computer could be privileged. The court deemed emails from the employee to his attorney to be privileged.²⁰

Email is now a recognized part of all discovery and litigation and invariably employees will communicate with their personal attorneys using employer-provided technology. Attorneys who represent employers should advise their clients to implement policies banning the personal use of any technology the employer provides. Employers must also know that merely having a policy is not enough; rather, employers should consistently enforce their policies—especially policies that call for the regular monitoring of emails.

On the other hand, attorneys with employee clients must discourage their clients from using employer-provided technology to communicate with counsel. Employee clients should know that if their employers consistently apply email and computer-use policies, then any communications through employer-provided channels may not be private enough to be privileged.²¹

Endnotes:

- 1 See *Banks v. Mario Industries*, 274 Va. 438, 454, 650 S.E.2d 687, 695–696 (“[T]he [attorney-client] privilege is waived where the communication takes place under circumstances such that persons outside the privilege can overhear what is said.”) (citations omitted).

Technology continued on page 62



Lauren E. Fisher is an associate with the Richmond firm Shelley & Schulte PC and practices in civil litigation with an emphasis on employment law.

- 2 See, e.g., *In re Asia Global Crossing Ltd.*, 322 B.R. 247, 257 (S.D.N.Y. 2005); *United States v. Hatfield*, No. 06-CR-0550, 2009 U.S. Dist. LEXIS 106269, at 28 (E.D.N.Y. Nov. 13, 2009); *Geer v. Gilman Corp.*, No. 3:06 CV 889, 2007 U.S. Dist. LEXIS 38852, at 3 (D. Conn. Feb. 12, 2007), cases *infra*.
- 3 201 N.J. 300, 990 A.2d 650 (2010).
- 4 See *id.* at 307, 990 A.2d at 655–656 (recounting the process through which webpages were saved on the employee’s hard drive).
- 5 See *id.* at 307, 990 A.2d at 656.
- 6 See *id.* at 309, 990 A.2d at 656 (describing how the employer could view the emails sent through the personal, password-protected Yahoo account of the employee).
- 7 See *id.* at 311, 990 A.2d at 657 (“The principal purpose of electronic mail (*email*) is for company business communications. Occasional personal use is permitted”).
- 8 See *id.* at 314, 990 A.2d at 659.
- 9 See *id.* at 322, 990 A.2d at 663 (noting that the policy does not address web-based emails and that occasional personal use of email was permitted, and deciding that the employee could reasonably expect her emails to remain private).
- 10 No. 03-CV-6327, 2006 U.S. Dist. LEXIS 29387 (E.D.N.Y. May 15, 2006)
- 11 See *id.* at 4.
- 12 See *id.* at 8 (“[L]ack of enforcement by MWC of its computer usage policy created a ‘false sense of security’ which ‘lull[ed]’ employees into believing that the policy would not be enforced.”) (citations omitted), see also *Leventhal v. Knapek*, 266 F.3d 64, 73 (2d Cir. 2001) (stating that whether an expectation of privacy is reasonable can vary depending on whether the employer monitors its computers).
- 13 See *id.* at 17 (describing the difference between the case at hand and cases in which the employer “retained the key” to the employee’s computer through remote access technology).
- 14 See *id.* at 26.
- 15 No. 3:04-CV-139, 2008 U.S. Dist. LEXIS 28905 (W.D.N.C. Feb. 29, 2008).
- 16 See *id.* at 11–12 (emphasizing the importance of effectively conveying an email policy to employees).
- 17 See *id.* at 10 (“If Plaintiff lacked knowledge of the email policy, and Defendant cannot show that Plaintiff was notified of the policy, then Plaintiff had a reasonable expectation of privacy and confidentiality in his email communications with his personal attorney.”).
- 18 No. 09 C 6974, 2010 U.S. Dist. LEXIS 97457 (N.D. Ill. Sept. 17, 2010)
- 19 See *id.* at 27.
- 20 See *id.* at 28 (“If Huron interpreted its computer usage policy as meaning that employees waive the attorney-client privilege by using their work email addresses and Huron computers to communicate with counsel, such a review would have been unnecessary.”).
- 21 See e.g. *Holmes v. Petrovich*, 191 Cal. App. 4th 1047, 1068 (finding that an employee’s method of emailing her attorney was “akin to consulting her attorney in one of defendants’ conference rooms, in a loud voice, with the door open.”).