A young lawyer drops a file on your desk: "We got him cold," he says. "Here are his emails to his lawyer—I bet he has admitted the sexual harassment in some emails to his attorney and once we read them, we can nail him good." But should you open and read them? Something makes you uneasy about reading those emails. Are you right to worry? Yes. While there are cases which would support your claim that the executive waived the attorney-client privilege by using company computers, especially in light of your company policy prohibiting using computers for personal use, the law in this area is neither mature nor settled. Proceed, as they say, at your peril.

Emails Between Employees and Their Attorneys Using Company Computers: Are They Still Privileged?

BY JOHN K. VILLA

Let's focus first on the governing legal principle and then apply it to the practicalities of the modern American workplace. Communications between a lawyer and client/employee are *not* deemed privileged if exchanged in a setting where there is no reasonable expectation of confidentiality for the client/employee. Most corporations have adopted policies prohibiting personal use of company computers and have warned that email traffic may be monitored and read by company officials. This should send the message that confidentiality cannot reasonably be expected. Despite this fact, many employees continue to use corporate computers for personal use including privileged communications with their lawyers even in matters where the employee and the company are adverse. The courts have therefore been confronted with the sticky issue of the applicability of the attorney-client privilege to email communications in the employment context where legal principle collides with reality. Not surprisingly, there is no uniform rule.

Just for fun, let's first review some basics about the attorney-client privilege and then apply them to electronic communications.

Confidentiality—The Key to the Privilege

At its core, the attorney-client privilege protects communications between a client and her attorney that are made *in confidence* for the purpose of obtaining legal advice.[1] The pivotal issue in the cases involving employee emails is the element of confidentiality,[2] which requires that the communication be made with the intent that it be confidential and with the *reasonable expectation and understanding* that, under the circumstances, it will remain confidential.[3] Although you might question the confidentiality of email, it is generally recognized that the mere use of email to transmit a confidential communication to an attorney does not, of itself, vitiate the privilege.[4]

The Four-part Test of Reasonable Expectations of Confidentiality

A different standard applies to determining whether email communications between an employee and her attorney satisfy the confidentiality element so as to fall within the protection of the attorney-client privilege. The limited number of decisions addressing this issue typically focus on four factors: the existence of a company policy banning the personal use of the employer's computer; the enforcement of a no-personal-use policy through the monitoring of company computers; the employee's knowledge of the no-personal-use and monitoring policy; and the right of third parties to access the employer's computers.[5] Where all of these factors are present, the courts have generally held that the privilege is inapplicable.

In one well-known case, *Scott v. Beth Israel Medical Center Inc.*,[6] a wrongful termination action brought by the former chairman of the orthopedic department at the defendant hospital, the plaintiff/surgeon sought a protective order requiring the return of all email communications between the plaintiff and his attorney that were made using the plaintiff's employee email address and the hospital's email system. The evidence disclosed that the defendant had an email policy that limited use of the

JOHN K. VILLA is a partner with Williams & Connolly LLP in Washington, DC. He specializes in corporate litigation (civil and criminal) involving financial services; directors', officers', and lawyers' liabilities; securities; and related issues. He is an adjunct professor at Georgetown Law School and a regular lecturer for ACC. He is also the author of *Corporate Counsel Guidelines*, published by ACC and West. He can be reached at *jvilla@wc.com*.

system for business purposes; provided that all material "created, received, saved, or sent" on the defendant's computer system constituted the property of the defendant; disclaimed any personal privacy right in any such material; and reserved to the defendant the right to access and disclose such material without prior notice.[7] The email policy was included in the defendant's policy and procedure manual which was available on the defendant's intranet, in hard copy at the office of the administrator for each department, and, after 2002, in an employee's handbook distributed to every employee.[8] Although the plaintiff had not signed a form acknowledging familiarity with the email policy, a requirement for doctors hired after the plaintiff, the evidence showed that the plaintiff had served as chairman of the orthopedic department and worked closely with that department's administrator.[9]

In support of his claim that the emails were protected by the attorney-client privilege, the plaintiff relied on a New York statute providing that a communication does not lose its privileged character solely because "it is communicated by electronic means or because persons necessary for the delivery or facilitation of such electronic communication may have access to the content of the communication."[10] The surgeon argued that this provision protected his privileged email communications and rendered any contrary email policy irrelevant.[11] The court rejected this argument and held that the statute does not absolve the holder of the privilege from protecting privileged communications, but instead, recognizes that an email communication may lose its privileged character for other reasons.[12] Applying the four-part test set forth above,[13] the court found that the defendant's no-personal-use email policy, and its policy allowing for the monitoring of the plaintiff's use of the computer system, together with what the court found as the plaintiff's actual *and* constructive knowledge of these policies, undermined the reasonable expectation of confidentiality in the email communications—hence no attorney-client privilege.[14]

According to *Scott*, therefore, a company may defeat a claim of privilege by an employee with respect to email communications using the company's computer system, where the employee knows, or should know, that such usage is contrary to express company policy and is also subject to monitoring. Where such policies exist, even the employee's use of a private password-protected email account may not be enough to support a claim of privilege.[15] Some courts have also found that a monitoring policy, together with the employee's knowledge thereof, may be sufficient to thwart a claim of privilege.[16]

Contrary Views

There are, however, discordant strands in the jurisprudence. Despite the existence of policies banning the personal use of company computers and providing for the monitoring of computer usage, some courts have upheld employee's claims of privilege. For example, where an employee works from a home office using a company computer, sends or receives emails via the internet on a password-protected private account, and takes measures to delete all personal files before returning the computer, some courts have held that the attorney-client privilege remains intact if the evidence also discloses that the company failed to, or was lax in, enforcing the policies,[17] or failed to provide sufficient notice of the extent to which it would monitor internet communications.[18] And, even though attorney-client communications are sent using a company-issued email address and the company's computer system, insufficient notice of the company's no-personal-use email policy will also defeat a company's challenge to a claim of privilege.[19]

What is a Careful Lawyer to Do?

Returning to the beginning hypothetical, where does this leave the company? If there were a pending proceeding, the company would probably have a good challenge to the attorney-client privilege assertion but, not a slam-dunk. But, here, there is not a proceeding from which to secure a ruling. If the company looks at the emails and later litigates and loses the argument, the company lawyers doing so may find themselves disqualified from the defense of the company, or worse.[20] What to do? Well, one option is to hold onto the emails, not read them, and place the issue before the court for decision.[21] This, of course, presupposes a lawsuit will eventually be filed. If there is no lawsuit, one could, if sufficiently imaginative, prompt a judicial resolution of the privilege issue by,[22] or perhaps refer the matter to, an expert for an opinion that may be of some assistance in later litigation.

In the last analysis, proceed with caution in reading an employee's potentially privileged documents unless there is a controlling decision in your jurisdiction that accords closely with the facts of your case. Otherwise, a careful lawyer should approach this with caution and seek judicial review before acting. The law in this area is not sufficiently mature for most lawyers to risk disqualification from reading potentially privileged documents.

NOTES

1 *In re Grand Jury Investigation*, 842 F.2d 1223, 1224 (11th Cir. 1987); *see generally* John Villa, *Corporate Counsel Guidelines*, § 1:1 (Thomson/West 2007).

2 See *Long v. Marubeni American Corp.*, No. 05Civ.639(GEL)(KNF), 2006 WL 2998671, at *3 (S.D.N.Y. Oct. 19, 2006) ("Confidentiality is an aspect of a communication that must be shown to exist to bring the communication within the attorney-client communication privilege.")

3 *Bogle v. McClure*, 332 F.3d 1347, 1358 (11th Cir. 2003); see generally John Gergacz, *Employees' Use of Employer*

Computers to Communicate With Their Own Attorneys and the Attorney-Client Privilege, 10 Computer L. Rev. & Tech. J. 269, 286 (Summer 2006) ("Under the attorney-client privilege, confidentiality requires that the client intend to keep the communication secret, that the setting in which the communication takes place reasonably fosters secrecy, and that the privileged communications remain confidential after they occur.")

4 *See City of Reno v. Reno Police Protective Ass'n*, 118 Nev. 889, 59 P.3d 1212, 1218 (2002) (holding that a confidential document transmitted via email is protected from discovery by the attorney-client privilege, as long as the requirements of the privilege are met); *see also* N.Y. C.P.L.R. 4548 (McKinney) (providing that a communication does not lose its privileged character "for the sole reason that it is communicated by electronic means or because persons necessary for the delivery or facilitation of such electronic communication may have access to the content of the communication"); Cal. Evid. Code § 917(b) (Thomson/West 2007) (same); ABA Formal Ethics Op. 99-413 (1999) (opining that the transmission of privileged information between attorney and client via encrypted email does not, alone, violate the confidentiality provisions of the Model Rules).

5 This four-factor test was first applied by the court in *In re Asia Global Crossing, Ltd.*, 322 B.R. 247, 257 (S.D.N.Y. 2005), a bankruptcy action in which the bankruptcy trustee sought discovery of emails between company officers and their private attorney in connection with the trustee's investigation of certain transactions. In crafting this test, the court drew on cases involving an employee's right to privacy in the workplace environment, noting that "[t]here is a close correlation between the objectively reasonable expectation of privacy and the objective reasonableness of the intent that a communication between a lawyer and a client was given in confidence." 322 B.R. at 258-259. However, because of inconsistent evidence as to the existence or enforcement of a no-personal-use email policy, *id.* at 259, the court was unable to conclude as a matter of law that the officers' use of the company's email system to communicate with their private attorneys "eliminated any otherwise existing attorney-client privilege." *Id.* at 261.

6 No. 602736/2004, 2007 WL 3053351 (N.Y. Sup. Ct. Oct. 17, 2007).

7 2007 WL 3053351, at *2.

8 *Id.*

9 *Id.*

10 *Id.* at *3 (quoting N.Y. C.P.L.R. 4548 (McKinney's 1999)).

11 *Id.* In support of this argument, the plaintiff relied on *People v. Jiang*, 131 Cal. App. 4th 1027, 33 Cal. Rptr. 3d 184 (2005), involving a similar statutory provision. The court distinguished *Jiang*, in which the question of privilege arose in connection with a prosecutor's subpoena of documents stored on a company computer used by the defendant employee, where the email policy of the defendant's employer did not prohibit the personal use of email but was only intended to protect the employer's intellectual property, and where the documents were never transmitted over the employer's email system but were stored in a segregated, password-protected file marked "attorney." *Id.*, 33 Cal. Rptr. at 203-205.

12 *Id.* at *3-*4. According to the Practice Commentary, "[t]he statute provides only that privilege shall not be lost solely because the parties use email. All other aspects of the privilege must be satisfied, including the conventional requirements of confidentiality." N.Y. C.P.L.R. 4548, Practice Commentary (McKinney 1999).

13 The court applied only three of the four factors. Because of C.P.L.R. 4548, which also protects the privileged character of electronic communications even though "persons necessary for the delivery or facilitation" of the communication "may have access to the content of the communication," the court found that the factor dealing with access by third parties was irrelevant. 2007 WL 3053351, at *5.

14 *Id.* at *4-*5. The court also rejected the plaintiff's claim of protection under the work-product doctrine, finding that the *pro forma* notice of confidentiality at the end of the emails sent by plaintiff's attorney were "insufficient and not a reasonable precaution to protect its clients" in view of the defendant's email policy. *Id.* at *6.

15 *See, e.g., Long,* 2006 WL 2998671, at *3 (rejecting employees' contention that use of private, password-protected email accounts on employer's computer protected confidentiality of their communications with their attorneys, where employees knew that policy prohibited personal use of company's computers, disclaimed any right of personal privacy in material stored in, created, or sent over the email and/or internet systems provided by the company, and allowed the company to monitor all data flowing through its computer system).

16 *See, e.g., Kaufman v. SunGard Inv. Sys.*, Civil Action No. 05-cv-1236 (JLL), 2006 WL 1307882 (D. N.J. May 10, 2006) (affirming magistrate's finding that any privilege that attached to employee's email communications with her attorney was waived where the evidence showed that employee used company's computer and network system with knowledge of, and assent to, company policy that allowed company right to access company computers, disclaimed any personal privacy interests in information stored in company property, even if protected by a password, and reserved right to monitor network, Internet, and email usage at any time).

17 *See, e.g., Curto v. Medical World Communications, Inc.*, No. 03CV6327 (DRH)(MLO), 2006 WL 1318387, at *3, *5 (E.D.N.Y. May 15, 2006) (upholding magistrate's finding that the plaintiff had a reasonable expectation in the confidentiality of her email communications with her attorney where, despite company's use and monitoring policy, company was unable to monitor her activity or intercept her emails on home-based laptop issued by company, and even if possible, company's failure to enforce the policy gave employees a "'false sense of security' which 'lulled' employees into believing that the policy would not be enforced.").

18 *See, e.g., National Econ. Research Assocs., Inc. v. Evans,* No. 04-2618-BLS2, 21 Mass. L. Rptr. 337, 2006 WL 2440008, at *3-*4 (Mass. Super. Aug. 3, 2006) (policy that did not expressly declare that company would monitor the content of internet communications, did not expressly or implicitly declare that company would monitor the content of email communications from an employee's personal email account accessed from the internet on a company-

issued computer, and failed to warn that the content of internet email communications was stored on the hard-drive of company-issued computers and was thus subject to review by the company, was insufficient to defeat the plaintiff's claim of privilege); *cf. Jiang*, 33 Cal. Rptr. 3d at 203-205 (employee had reasonable expectation of confidentiality in documents stored on company's laptop and subpoenaed by prosecutor for use in employee's criminal prosecution, where employee maintained documents in a segregated, password-protected file marked "Attorney" and did not use employer's email system to transmit documents, where employer did not warn employees that it would access material stored in such a manner in its computers, and where employer's policy disclaiming any privacy in email communications or company property did not prohibit personal use of computers but was intended to protect the employer's intellectual property).

19 *See, e.g., TransOcean Capital, Inc. v. Fortin*, No. 05-0955-BLS2, 2006 WL 3246401, at *4 (Mass. Super. Oct. 20, 2006) (where company failed to adopt human resource contractor's no-personal-use policy as its own policy or to inform employees that policy could be found on contractor's website, and there was no evidence suggesting that plaintiff understood that contractor had issued an email policy or that his employer had a policy prohibiting personal use and/or monitoring employee use, the company failed to show that plaintiff should reasonably have recognized that his email communications were accessible to his employer; therefore, emails were made in confidence and there was no waiver of the attorney-client privilege).

20 *See Maldonado v. New Jersey ex rel. Administrative Office of Courts-Probation Division,* 225 F.R.D. 120, 138 (D. N.J. 2004) (holding that failure to notify counsel of inadvertently produced privileged document, and subsequent use of such document warranted disqualification of counsel); *Rico v. Mitsubishi Motors Corp.*, 42 Cal. 4th 807, 171 P.3d 1092, 68 Cal. Rptr. 3d 758 (2007) (disqualifying plaintiffs' attorneys and experts for using and disseminating privileged document obtained inadvertently during depositions).

21 *See* Fed. R. Civ. P. 26(b)(5) (2006) (providing that where privileged material is produced during discovery, producing party may notify the receiving party of the claim of privilege, after which receiving party "must promptly return, sequester, or destroy" the material, or may opt to present the material to the court under seal for its determination of the claim of privilege); *see generally* Villa, *supra,* n. 1 at § 1:23.

22 Where the company has a monitoring and no-personal-use policy in place, counsel may want to consider the viability of pursuing a declaratory judgment as to the applicability of the attorney-client privilege. *See United States v. Internat'l Brotherhood of Teamsters, Chauffeurs, Warehousemen and Helpers of America, AFL-CIO*, 119 F.3d 210 (2d Cir. 1997) (affirming issuance of declaratory judgment precluding assertion of the attorney-client privilege).