

Corporate Counsel

Corporate Governance

Managing the Conflict between Internal Investigations and Potentially Privileged Employee Communications

*Contributed by
Steven S. Scholes, McDermott Will & Emery*

Introduction

During the course of internal investigations, it is common for investigators to obtain access to all employee communications transmitted through, and documents created by employees on, a company's information technology infrastructure. Investigators commonly retrieve emails and other documents maintained on company servers, and in many instances make images of the hard drives of laptop computers the company issued to its employees. These conventional investigative steps give the investigators full and unlimited access to all the communications to which the affected employees have been party, and all the documents they have created or revised, on a company's system.

And it is common today for employees to use company email and document systems, as well as company-issued laptop computers, for a wide variety of unarguably personal matters, including social communications, visits to websites with no conceivable relationship to job performance, and other matters. Because of the seeming confidentiality of the communications,

the convenience of electronic communication, and the often intermittent enforcement of workplace computer-usage policies by employers, employees may subjectively and in good faith expect their personal communications on employers' systems to be confidential.

This set of circumstances presents a serious potential problem. If, during the course of conducting an internal investigation, the investigators identify materials which are either expressly identified as being confidential, such as for example, emails maintained in a folder marked "Personal Privileged and Confidential," or are obviously personal from their context, such as email communications with personal counsel, do the investigators have the right to open, review and make use of those materials? Is it possible for an employee to engage in confidential, privileged communications with her personal counsel on her employer's email system?

The attorney-client privilege has recently become the focal point of a clash between employers seeking to exercise authority over workplace computer and email systems, and employees accustomed to using those systems for quintessentially personal purposes.

Courts have not reached the same results in deciding this issue. Contrary to what may be conventional legal wisdom, the mere existence of a policy warning employees about files stored or emails sent on workplace computers may not be sufficient to eliminate an employee's expectation of privacy in such materials. In fact, there can be serious consequences to an employer conducting an internal investigation, attempting to protect its proprietary information, or engaging in numerous other legitimate business activities.

In an effort to provide guidance to those conducting internal investigations with respect to materials employees may maintain

Originally published by Bloomberg Finance L.P. in the Vol. 2, No. 11 edition of the Bloomberg Law Reports—Corporate Counsel. Reprinted with permission. Bloomberg Law Reports® is a registered trademark and service mark of Bloomberg Finance L.P.

This document and any discussions set forth herein are for informational purposes only, and should not be construed as legal advice, which has to be addressed to particular facts and circumstances involved in any given situation. Review or use of the document and any discussions does not create an attorney-client relationship with the author or publisher. To the extent that this document may contain suggested provisions, they will require modification to suit a particular transaction, jurisdiction or situation. Please consult with an attorney with the appropriate level of experience if you have any questions. Any tax information contained in the document or discussions is not intended to be used, and cannot be used, for purposes of avoiding penalties imposed under the United States Internal Revenue Code. Any opinions expressed are those of the author. Bloomberg Finance L.P. and its affiliated entities do not take responsibility for the content in this document or discussions and do not make any representation or warranty as to their completeness or accuracy.

are privileged, this article examines the approaches of courts that have addressed the competing interests of employers and employees in a variety of contexts.

The Attorney-Client Privilege in the Workplace

Generally, the attorney-client privilege is a rule of evidence that prevents a party in litigation from gaining access to a statement or document that is protected as confidential.¹ The privilege protects all communications between a lawyer and client for the purposes of obtaining or providing legal assistance.² The privilege may, however, be waived through disclosure of pertinent information to a third party, such as the disclosure of a privileged communication by an employee to an employer. Waiver can occur even if the disclosure is inadvertent; i.e., the waiving party did not intend to reveal the communication to a third party, and certainly did not intend to waive the privilege.

The question of when inadvertent disclosure waives the privilege is complicated in the context of company information technology systems. Companies typically have policies addressing email usage and privacy expectations with respect to the use of employers' computers, email systems and servers. Some understandably view such policies as the final word on who has control over files and emails in a company's system. But the issue is not so simple in light of often intermittent enforcement of such policies and the corresponding widespread personal use by employees of workplace computers and email.

Although courts seem to have settled on a general framework for resolving the question, the application of the framework has varied and depends upon the court's approach to what appear to be generally accepted criteria, including the existence of policies on personal computer use, how well the policies were communicated to employees, and sometimes the nature of the files or emails at issue. Adding complexity is the fact that these factors may be viewed differently in different jurisdictions. In any event, as a general proposition, whether the files are protected by the attorney-client privilege depends primarily on whether the employee had a reasonable expectation of privacy in his or her personal files on the employer's computer system.

The Developing Framework for Deciding When an Employee Waives the Privilege

– The Initial Approval: An Apparent Lack of Judicial Respect for Company Computer-Usage Policies

While courts have reached different conclusions when faced with assertions of privilege by employees as to emails or electronic files, they seem to have settled on an analytical framework, which was articulated in *In re Asia Global Crossing, Ltd.*³ In *Asia Global*, the court applied a four-factor analysis to assess whether an employee waived the attorney-client privilege. The court held that whether a waiver occurred essentially depended upon whether

the employee had a reasonable expectation of privacy in his computer files and email.⁴ The four factors that bear on whether an expectation of privacy was reasonable are: (1) whether the employer maintained a policy restricting employees' personal or other objectionable use; (2) whether the employer monitored the employee's computer or email use; (3) whether third parties had a right of access to the computer system or emails; and (4) whether the employee had notice of the use and monitoring policies.⁵

In *Asia Global*, the trustee for a bankrupt company sought access to key employees' emails and computer files as part of an investigation into certain transactions. Several of the emails included communications between the employees and their personal attorneys. The employees asserted the attorney-client privilege and refused to produce the documents. The trustee filed a motion to compel production of the documents, arguing that the employees had waived their right to assert the attorney-client privilege because they used the company's email system to transmit and store the communications.

The court began its analysis of whether the employees had waived the privilege by noting that a person does not generally waive his or her right to assert the attorney-client privilege as long as he or she expected the communication to remain confidential, and the expectation was reasonable under the circumstances. The court reasoned that the privilege is not lost merely because the employee may have sent the privileged communication through an unencrypted email system belonging to someone else.⁶ The fact that the employee used the employer's system is therefore not in itself sufficient to waive the privilege.

Whether the privilege was waived depends instead on whether it was reasonable for the employee to expect that emails or files sent or stored on his employer's computer system would remain confidential. Key to this inquiry is the employer's computer policy and the employer's application of the policy in the particular circumstance.

Applying the four factor test to assess whether the employer's policy divested the employees of the reasonable expectation of privacy, the court held that the employees did not waive the privilege, primarily because they raised sufficient doubts about whether *Asia Global* had a policy at all. While the bankruptcy trustee produced a memo and draft policy from a former *Asia Global* officer, the court found that it was unclear whether the policy applied to *Asia Global* or an affiliated company. In addition, each of the employees asserted that the company maintained no restrictions on personal computer use, and if it did, they were not aware of the policy. *Asia Global's* inability to prove it had a policy, and its failure to require its employees to acknowledge the policy was thus critical to its inability to obtain access to electronic files sent over its system.

In what might have portended a trend, a case decided a year later, *Curto v. Medical World Communications, Inc.*,⁷ affirmed a former employee's assertion of privilege over files stored on her workplace computer, in an action the former employee filed against her former employer. The *Curto* court upheld the expectation of privacy despite the employee's awareness

of company policy which provided that computers were to be used for business purposes only and that employees waived any expectation of privacy in anything they created, stored, sent or received on the system. The policy further stated that the company had a right to access all such material at any time and that the company could use electronic or human means to monitor employee computer use.⁸ During discovery, Curto asserted privilege over certain emails and memos she had exchanged with her personal attorney. Despite Curto's written acknowledgement that she received the policy and was aware of her lack of privacy, the court held that Curto had not waived the privilege.

Several unique circumstances were critical to the court's conclusion. First, the court found significant the fact that the employer never actually enforced its policy. The lack of enforcement "created a false sense of security which lulled employees into believing that the policy would not be enforced."⁹ Indeed, the employer was unable to monitor Curto's computer use effectively because she worked from home, and her company-issued laptop was not connected to the company's servers. Second, the court gave great weight to the fact that Curto took affirmative steps to maintain the confidentiality of the communications, including sending them from her personal, internet-based email account, and deleting the files from her computer before returning it to her employer. The court found that these precautions were reasonable, especially in light of evidence that the employer rarely enforced its policy.

The rationale of *Asia Global* and *Curto* was applied in a criminal context in *United States v. Nagle*,¹⁰ a case in which a witness sought to assert the privilege with respect to a document obtained from his work-issued computer. Company policy clearly stated that internet and email activity was not private, and could be monitored periodically. However, the court found that policy lacking in that it did not prohibit personal use of the computer or email. Additionally, the court found it significant that the policy applied only to internet and email use and not the computer's hard drive, which is where the document in question had been stored. Based on the limited nature of the company's policy, the court concluded that it was reasonable for the employee to believe that his memo would remain private, and that he had not waived attorney-client privilege.

Similarly, the Department of Justice's failure to prohibit its employees' personal use of company email prevented it from defeating a claim of privilege in *Convertino v. U.S. Department of Justice*.¹¹ Although the Department of Justice in that case had access to, and actually saved, its employees' emails on a government server, it had neither banned personal use of the email system nor notified employees of its practice of saving employee emails. The court held that the employees' expectations of privacy were reasonable because personal email use was tacitly permitted, and employees were unaware of any monitoring of such use.

– Narrowing *Asia Global* and *Curto*: Courts Defer To Computer Usage Policies

While the results in *Asia Global*, *Curto*, *Nagle* and *Convertino* may create the impression that courts will respect assertions of privilege as to personal communications on company systems, other decisions, while generally applying the same four-factor test, have given the benefit of the doubt to companies that maintain clear computer usage policies, and provide notice of those policies to employees. They have given significantly less weight to other factors, such as the employer's actual enforcement of the policy. This has even been the case where a company did not actually monitor its employees' computer use and where evidence was lacking that employees were aware of the policies.

For example, in *In re Royce Homes, LP*,¹² the court found that a key decision-maker of a bankrupt home-building company had waived the attorney-client privilege with respect to emails he had sent to his attorney using the company's email system. Neither party in the case disputed that the company had a policy banning personal use of company computers, which stated that employees waived any privacy interest in electronic information sent or stored on the company's system. In addition, because of the policy that all communications were company property, third parties necessarily had access to the employee's emails by "virtue of their mere placement on the [company's] server." Furthermore, the bankruptcy trustee who took title to and control over the company's servers had unfettered access to the employee's emails.

While there was no evidence that the company had ever actually enforced the policy or monitored employee email, the *Royce Homes* court essentially ignored the holding in *Curto*, holding that "whether the [company] actually reads an employee's emails is irrelevant."¹³ Moreover, the court imputed knowledge of the policy to the employee because he was a key employee, even though he denied being aware of the policy and the creditors produced no evidence to the contrary.

Similarly, the court in *In re Reserve Fund Securities and Derivative Litigation*,¹⁴ gave significant weight to a company's computer usage policy in applying the four-factor framework to an assertion of the spousal privilege. In *Reserve Fund*, the SEC sought access to communications between an employee and his spouse, which had been sent over the company's email system. The court found that the computer usage policy clearly banned personal use, and that courts in such situations "frequently find that employees have no reasonable expectation of privacy in email transmitted over that system."¹⁵ The policy further warned employees that all email communications were saved and were subject to disclosure to regulatory agencies. Where the employee conceded that he was aware of these policies, the court held that he could not have reasonably expected his emails with his wife would remain confidential.

A number of other courts have followed the approach of *Royce Homes* and *Reserve Fund*, and have determined that employees with notice of a company's policy banning personal use of workplace computers generally do not have a reasonable

expectation of privacy in workplace files, and as a result, employees waive the attorney-client privilege as to otherwise protected communications if they are made through company computers or systems.¹⁶

Lessons Learned

Based on these judicial decisions, companies seeking to retain access to and control of employee materials generated on company email and document systems for purposes of internal investigations should take a number of steps. Companies should promulgate and disseminate a written computer usage policy. The policy should ban personal use of the company computers, email systems, and the internet. The policy also should provide that files created, sent or stored on such systems are not confidential. Companies should expressly reserve the right to monitor computer use and access employee files and emails, and periodically monitor usage to ensure compliance. Finally, the above steps may not have any effect if employees are not aware of the policies. Companies must notify employees of the policies, and take steps to obtain written acknowledgements from employees that they have read and understand the policies.

Steven S. Scholes is a partner in the Chicago office of the law firm McDermott Will & Emery LLP and a former attorney in the Securities and Exchange Commission's Division of Enforcement. He concentrates his trial practice in all varieties of securities and other complex commercial litigation. Mr. Scholes can be reached at sscholes@mwe.com.

¹ Edna Selan Epstein, *The Attorney-Client Privilege and The Work-Product Doctrine* 3 (5th ed. 2007).

² *See id.*

³ 322 B.R. 247, 257 (S.D.N.Y. Bankr. 2005).

⁴ *Id.*

⁵ *Id.*

⁶ *Id.* at 256.

⁷ No. 03-CV-6327, 2006 BL 59897 (E.D.N.Y. May 15, 2006).

⁸ *Id.* at *1.

⁹ *Id.* at *8.

¹⁰ No. 1:09-CR-384, 2010 BL 228752 (M.D. Pa. Sept. 30, 2010)

¹¹ 674 F. Supp. 2d 97 (2009)

¹² 449 B.R. 709 (S.D. Tex. Bankr. 2011).

¹³ *Id.* at 739.

¹⁴ Nos. 09-MD-2011, 09-Civ-4346, 2011 BL 142178 (S.D.N.Y. May 23, 2011).

¹⁵ *Id.* at *8.

¹⁶ *See, e.g., Alamar Ranch LLC v. County of Boise*, No. CV-09-004-S-BLW, 2009 BL 236897 (D. Idaho Nov. 2, 2009) (emails sent to employee's work account by personal attorney were not protected); *Leor Exploration and Prod. LLC v. Aguiar*, No. 09-60136-CIV, 2009 BL 203242 (S.D. Fla. Sept. 23, 2009) (holding that an employee had no reasonable expectation of privacy in emails sent over company system in the face of clear company policy); *Kaufman v. SunGard Investment Sys.*, No. 05-cv-1236 (JLL) (D. N.J. May 10, 2006) (finding privilege waived where company policy stated that employee had no expectation of privacy in emails sent on company system).