The Metropolitan Corporate Counsel®

www.metrocorpcounsel.com

Volume 12, No. 11 November 2004

Civil Justice Reform – Law Firms

Best Practices For Maintaining The Attorney-Client Privilege In Email Communications

Joseph L. Buckley and Michael R. Potenza

SILLS CUMMIS EPSTEIN & GROSS P.C.

Joseph L. Buckley

Michael R. Potenza

You are general counsel of a large corporation with an in-house legal department that, as is now the custom, communicates with outside counsel, business people within the company and among each other using email. To maintain the email system, your company uses both a staff of in-house Information Technology ("IT") employees and outside consultants. All of these employees or outside consultants, in order to carry out their functions, can access the emails sent, received and stored by your in-house legal staff. You are now in a "bet-the-company" litigation and your opponent argues that all of your in-house legal staff's email, including emails from outside counsel setting forth the nuts and bolts of your legal strategy on this matter, are discoverable because allowing IT staff and outside consultants such access waived the attorney-client privilege. You contact your outside counsel by telephone (not email) and ask the sixty-four thousand dollar question: Does allowing IT staff and outside technical consultants access to your email servers, which contain images of privileged email communications, waive the attorney-client privilege?

The short answer is that it depends on the reasonableness of steps taken to ensure that the privileged emails remain confidential. One key question is whether the company's internal email policy and its contracts with its outside consultants prohibit accessing the content of emails without first obtaining permission from the company. If these restrictions are in place, the privilege most likely will not have been waived. The remainder of this piece will analyze the relevant case law and set forth some "best practices" to maintain the confidentiality of attorney email communications.

Email, like any other form of communication between a lawyer and client, is protected by the attorney-client privilege, provided that the communications are (1) maintained in confidence and (2) the privilege is not waived.[1] Three generally accepted criteria must be met to establish confidentiality: "(1) the client must intend his communications with his attorney to be confidential; (2) the client's subjective intention of confidentiality must be reasonable under the circumstances; and (3) the confidentiality must have been subsequently maintained."[2] As to waiver, the majority rule is that waiver occurs only where the disclosing party failed to take reasonable steps to maintain the confidentiality of the communications.[3] Factors in determining reasonableness include: (1) the reasonableness of precautions taken to prevent inadvertent disclosure; (2) the number of disclosures; (3) the extent of disclosure; (4) the promptness of measures taken to rectify disclosure; and (5) whether justice would be served by waiver.[4] Both the confidentiality and waiver analyses thus center on the reasonableness of the measures taken to ensure confidentiality.[5]

One commentator addressed the analogous access administrators of email providers have to email communications stored in transit:

"[A]lthough system administrators generally have easy access to all communications transmitted through their computer networks, they are only allowed to read e-mail messages as necessary incident to the rendering of their services or, if necessary to protect their property.[6] This access should not destroy the privilege since the access by system administrators is severely limited."[7] In light of this, perhaps the most important thing a company can do is to make sure there is a contractual commitment – in email policies incorporated into its employment contracts and in any agreements with outside consultants – to preserve confidentiality.

Although there is no case directly on point, at least one court has addressed an analogous situation and concluded that email on a commercial network is subject to a reasonable expectation of privacy. In *United States v. Maxwell,*[8] the U.S. Court of Appeals for the Armed Forces addressed the issue of privacy of emails stored on AOL's central server waiting to be retrieved by the addressees. The issue in the case was whether the defendant had standing to challenge the validity of a search of AOL's servers for the defendant's incriminating emails. A person may challenge a search only if there is both a subjective and objectively reasonable expectation of privacy.[9] Because AOL's policy was "not to read or disclose sub-

***Joseph L. Buckley** is a Member of Sills Cummis Epstein & Gross P.C. in Newark, New Jersey. **Michael R. Potenza** is Of Counsel to the Firm. Both are litigators specializing in complex commercial litigation.*

Please email the authors at jbuckley@sillscummis.com or mpotenza@sillscummis.com with questions about this article.

scribers' email to anyone except authorized users, thus offering its own contractual privacy protection," the Court concluded that the defendant had a reasonable expectation that the emails, while in storage, would remain private.[10]

The American Bar Association addressed a similar issue in ABA Formal Op. 95-398, Access of Nonlawyers to a Lawyer's Database (Oct. 27, 1995). It concluded that "[a] lawyer who gives a computer maintenance company access to information in client files must make reasonable efforts to ensure that the company has in place, or will establish, reasonable procedures to protect the confidentiality of client information." The ABA recognized that "lawyers now use outside agencies for numerous functions such as accounting, data processing and storage, printing, photocopying, computer servicing and paper disposal" which "inevitably entails giving them access to client files." The ABA concluded that a lawyer's ethical obligation to preserve client confidentiality is not breached by retaining third parties to perform these functions as long as the lawyer "ensures that the service provider has in place, or will establish, reasonable procedures to protect the confidentiality of information to which it gains access."

The ability to monitor the communications, without more, should be insufficient to find a waiver. As the Ninth Circuit put it, "the capability of monitoring does not create implied consent to any monitoring that occurs. Cellular telephones and electronic mail are both technologies of questionable privacy, but we nonetheless reasonably expect privacy in our cell phone calls and email messages."[11] Similarly, "lawyers routinely make use of the convenience of overnight delivery, without fear that any privilege is waived or secret improperly revealed, even though the back of the airbill makes it clear that the carrier has an unconditional right to open any envelope or package for any reason or for no reason."[12]

Companies should be aware of the risk of a failure to meaningfully restrict access by third parties. *In re Horowitz*[13] found a waiver based on an accountant's access to privileged communications in a client's files. In that case, a party made all of its files, including privileged communications with his lawyers, available to its accountants for purposes unrelated to the giving of legal advice. Significantly, the defendant placed absolutely no restrictions on the accountant's access to the files and in fact, the accountant "had the authority to look at . . . the legal communications, many of which appeared to deal with the tax and financial matters with which he was particularly concerned."[14] Noting that the party "[a]t the very least . . . could have directed [the accountant] not to look at the privileged documents," but in fact took no "affirmative action to preserve confidentiality," the court held that the attorney-client privilege had been waived.[15] A company can avoid the consequences of *Horowitz* and the cases that follow it by taking affirmative measures to preserve the confidentiality of its email. Such measures can include a formal email policy that prohibits unauthorized access to emails and the inclusion of similar restrictions in its agreements with outside computer technology consultants.

In light of the growing sophistication of computer networks in the corporate context, many companies necessarily must outsource the maintenance of those systems. If companies take reasonable precautions to limit access to attorney-client emails, it is unlikely that a court would find a waiver. In addition to the measures summarized above, companies should consider implementing some or all of the additional measures outlined below to further enhance the confidentiality of its attorney-client communications.

1. All legal email should be identified in the subject line as "Privileged and Confidential," "Attorney-Client Communication," or "Attorney Work Product," as appropriate. An attorney writing an email should identify himself or herself as an attorney in the signature line. Outside counsel should be encouraged to follow these procedures as well.[16]

2. The company should make sure that it has a written confidentiality agreement with all consultants with access to its servers: (1) that prohibits access to legal email communications absent express written authorization of the company; and (2) by which those consultants agree that if they access legal email, either inadvertently or with permission as above, they will not reveal that information.[17]

3. Similar precautions as in #2 above should be included in the company's email policy pertaining to the IT staff's access to legal email.

4. Business and legal email should be kept separately.[18] This can be done either by dedicating a part of the server architecture to store the legal department's emails or by having a separate system for the legal department's email correspondence. Access to the legal email server should be strictly limited both in terms of the number of IT staff and outside consultants with authority to access it and in the precautions (i.e., password protection) to keep unauthorized personnel from accessing the information.[19]

5. Legal emails should be deleted on a regular basis from the servers in accordance with the company's document retention policy and whatever additional restrictions (such as court preservation orders, pending litigation, etc.) may be applicable. Prior to that, legal emails should be transferred to a storage medium (such as a computer disk) and stored in a physically separate area with restricted access. This will minimize the amount of privileged email to which IT staff and/or outside consultants have potential access. The separate media used to store these emails should be logged so that they can be destroyed as provided in the company's document retention policy.[20]

6. Legal email if possible may be encrypted so that, even if IT staff or consultants access the data, they are not able to decipher the substance of the communication.[21]

---

[1] Int'l Marine Carriers, Inc. v. United States, *1997 WL 160371, at *3 (S.D.N.Y. Apr. 4, 1997);* Heidelberg Harris, Inc. v. Mitsubishi Heavy Indus., Ltd., *1996 WL 732522, at *7 (N.D. Ill. Dec. 18, 1996). Of course, the communications must be with the scope of the privilege to begin with; thus, communications, even by or among in-house counsel, concerning purely business matters generally are not considered privileged.*

[2] *Ben Delsa*, E-MAIL AND THE ATTORNEY-CLIENT PRIVILEGE: SIMPLE E-MAIL IN CONFIDENCE, *59 La. L. Rev. 935, 939 (1999).*

[3] Bank Brussels Lambert v. Credit Lyonnais (Suisse) S.A., *160 F.R.D. 437, 443 (S.D.N.Y. 1995).*

[4] United States v. Keystone Sanitation Co., *885 F. Supp. 672, 676 (M.D. Pa. 1994).*

[5] *Because the rules governing attorney-client privilege and waiver differ markedly from state to state, the reader is advised to consult the rules of his or her particular jurisdiction.*

[6] *The Electronic Communications Privacy Act ("ECPA"), provides at 18 U.S.C. § 2511(2)(A)(i) that "It shall not be unlawful for . . . a provider of wire or electronic communication service . . . to intercept [a] communication . . . while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider. . . ."*

[7] *Ben Delsa, 59 La. L Rev. at 944.*

[8] *45 M.J. 406 (Ct. App. Armed Forces 1996).*

[9] Id. *at 417.*

[10] Id. *at 417-19.* See also Playboy Enters., Inc. v. Welles, *60 F. Supp.2d 1050, 1055 (S.D. Cal. 1999) (access to emails by court-appointed computer specialist "will not result in a waiver of the attorney-client privilege") (emphasis in original);* Simon Property Group L.P. v. mySimon, Inc., *194 F.R.D. 639, 642 (S.D. Ind. 2000) (same).*

[11] Dunlap v. Rudder, *1997 WL 414380, at *3 (9th Cir. 1997).*

[12] *Ben Delsa, 59 La. L. Rev. at 944-45.*

[13] *482 F.2d 72, 81 (2d Cir. 1973).*

[14] Id. *at 82.*

[15] Id.

[16] *Theodore Banks et al.*, ATTORNEY-CLIENT PRIVILEGE AND ATTORNEY WORK PRODUCT PROTECTIONS *at 33-104 (2003).*

[17] *Ben Delsa, 59 La. L. Rev. at 944.*

[18] See In re Horowitz, *482 F.2d at 82 ("It is difficult to be persuaded that the documents were intended to remain confidential in the light of the fact that they were indiscriminately mingled with the other routine documents of the corporation and that no special effort to preserve them in segregated files with special protections was made.").*

[19] *Theodore Banks et al.*, ATTORNEY-CLIENT PRIVILEGE AND ATTORNEY WORK PRODUCT PROTECTIONS *at 33-104 (2003).*

[20] *Ben Delsa, 59 La. L. Rev. at 952.*

[21] *Albert Barsocchini, "Should Email Between a Lawyer and Client be Encrypted?", Glasser Legal Works (1998).* \