# Employees' Use of Employer Computers to Communicate with Their Own Attorneys and the Attorney-Client Privilege

*by*
*John Gergacz**

## I. INTRODUCTION

These days, corporate employees are equipped with the latest technology. Portable devices tether them to the workplace at all hours and in any locale. Slim and light-weight laptops replicate an office whether the employee is at home, on an airplane, or in a coffee shop.

Operating systems are provided and maintained for employees by their respective corporations and in-house information technology departments fix what goes awry. This technological transformation enhances business communications.

However, technological advances are not limited to the workplace. The use of cell phones, personal computers, and other electronic devices has also become commonplace at home. The nature of electronic devices means that overlapping between an employee's personal and workplace communications is inevitable. The same cell phone can be used to chat with friends at one point and later to outline a proposal to a major business client. Vacation photographs can be stored on a computer, whether it is employee or employer-owned. Employees can communicate with their attorneys by way of this technology as well.

Unlike other communications, however, those between attorney and client are privileged.[1] For example, consider an e-mail sent by a corporate employee to corporate legal counsel from an office computer using an operating system owned and maintained by the employer. If sent on behalf of the employer the e-mail would likely be privileged, although the corporation, as the lone client, would control it. The message to counsel was conveyed as part of the employee's job, and so that the employer could receive legal advice.[2]

On the other hand, that employee may use the same computer to communicate with an attorney concerning a personal matter. Clearly, the corporate employer would not be the attorney's client, even though a corporate computer was used to transmit the message. In this situation, only the employee is the client. Even though the communication may have the earmarks

---

* John Gergacz is a professor in the School of Business at the University of Kansas. He is the author of Attorney-Corporate Client Privilege 3d (Thomson/West 2000) (2006 supp).

1. Upjohn Co. v. United States, 449 U.S. 383, 389 (1981).

2. *See* JOHN GERGACZ, ATTORNEY-CORPORATE CLIENT PRIVILEGE 3-171 (3rd ed. 2004).

of a privileged one, the use of an employer's computer system to transmit it raises questions about its confidentiality.[3]

This article will analyze the balance between privilege and confidentiality in the electronic age. Three scenarios will be discussed: first, whether the mere use of employer-technology affects the employee's privilege claim; second, how an employer's no-personal-use policy may defeat an employee's confidentiality expectation and undermine the privilege claim; and third, whether encrypting those messages nullifies the effect of the employer's policy.

However, before this discussion gets underway, an overview of the attorney-client privilege will be provided.

## II. Brief Overview of the Attorney-Client Privilege[4]

The attorney-client privilege dates back to Elizabethan England.[5] It has always been a part of American Law.[6] When applied, the privilege shields certain materials from disclosure. Consequently, a person may discover information from any source, except another's confidential attorney-client communications. Those communications are "privileged."

Although withholding information from the fact-finder at trial risks an unjust result, the need for client candor with counsel outweighs this concern.[7]

3. Curto v. Med. World Commc'ns, Inc., 2006 WL 1318387, at *7 (E.D.N.Y. May 15, 2006); *In re* Asia Global Crossing Ltd., 322 B.R. 247 (Bankr. S.D.N.Y. 2005); People v. Jiang, 33 Cal. Rptr. 3d 184 (Cal Ct. App. 2005); Reno v. Reno Police Protective Ass'n, 59 P.3d 1212 (Nev. 2002).

4. *See generally* Gergacz, *supra* note 2 (discussing generally the attorney-client privilege).

5. John Henry Wigmore, Wigmore on Evidence 8 542 (McNaughton ed., 1961); *See* Geoffrey C. Hazard, *An Historical Perspective on the Attorney-Client Privilege*, 66 Cal. L. Rev. 1061 (1978); *See* Max Radin, *The Privilege of Confidential Communication Between Lawyer and Client*, 16 Cal. L. Rev. 487 (1928).

6. United States v. Louisville & Nashville R.R., 236 U.S. 318, 336 (1914) ("The desirability of protecting communications between attorney and client as a matter of public policy is too well known and has been too often recognized by textbooks and courts to need extended comment now. If such communications were required to be made the subject of examination and publication, such as enactment would be a practical prohibition upon professional advice and assistance."); *see also* Hatton v. Robinson, 31 Mass. (14 Pick.) 416 (1833); Crosby v. Berger, 11 Paige Ch. 377 (N.Y. Ch. 1844).

7. *Crosby* 11. Paige Ch. at 377 ("The object of the rule, protecting privileged communications from being disclosed by the attorney or counsel, is to secure to parties who have confided the facts of their cases to their professional advisors, as such, the benefits of secrecy in relation to such communications; so that the client may disclose the whole of his case to his professional advisor, without any danger that the facts thus communicated to his attorney or counsel will be

Consequently, the privilege may be justified because the adversary system requires attorney participation, and the attorney needs full disclosure from the client to be an effective advocate. However, if counsel could later be called as an adverse witness, clients would soon learn that cooperation with their attorneys was foolish. More cooperation with counsel leads to a richer source of information available for an adversary's use. Thus, to encourage client-attorney communications, the law has long provided a shield which creates a safe harbor so that clients can confide in their attorneys with confidence.

An often-cited test for distinguishing privileged communications from all others appeared over a half-century ago in *United States v. United Shoe Machinery*.[8] The *United Shoe Machinery* test can be organized around three themes. First, the court focuses on the roles of the parties to the communication. Second, the court considers the nature of the information communicated. And third, the court examines the confidentiality of the communication.

For the purpose of this article, the first two themes are assumed. Regarding the first theme, the employee communicates as a client and the attorney represents that employee. In a typical corporate employee-attorney communication, the employee is a corporate information provider. The client would then be the corporate entity rather than the employee, and the corporate employee's role is merely to communicate with the corporate entity's attorney.[9] Further, control of the corporation's privilege rests with its management, rather than any specific individuals.[10] The corporate counsel only represents the corporation, not the employee who communicates on its behalf.[11] Similarly, the attorney to whom the client communicates must act in a law-related role.[12] No privilege arises if the lawyer occupies some other

used in evidence against him, without his own consent."). *See generally Upjohn* 449 U.S. 383 (discussing basics of attorney-client privilege).

8. United States v. United Shoe Mach. Corp., 89 F. Supp. 357, 358-359 (D. Mass. 1950) (establishing that the holder of the privilege is or sought to become a client and that the privilege has been claimed and not waived).

9. *See Upjohn*, 449 U.S. 383 (1981) (focusing on which employee communication would create the privilege on the corporation's behalf.). *See generally* GERGACZ, *supra* note 2, at 2.04-2.12, 2.35-2.42.

10. Commodity Futures Trading Comm'n v. Weintraub, 471 U.S. 343, 348 (1985) (bankruptcy trustee occupying management role for bankrupt corporation controlled its privilege, and the former business managers did not have any power).

11. *In re* Grand Jury Subpoena, 274 F.3d 563, 571 (1st Cir. 2001) ("The default assumption is that the attorney only represents the corporate entity, not the individuals within the corporate sphere, and it is the individuals' burden to dispel that presumption.").

12. Great Plains Mut. Ins. Co. v. Mut. Reinsurance Bureau, 150 F.R.D. 193, 197 (D. Kan. 1993) (lawyer-board of directors member acting in role of attorney).

role.[13] In-house counsel, for example, may work in both legal and business management capacities. Only those communications tied to legal practice qualify as privilege-eligible.[14]

In addition, this article assumes that the second or "legal advice" theme of the *United Shoe Machinery* privilege test can also be satisfied, the client must be seeking legal advice before the communications are important enough to qualify as privileged.[15] Neither chit-chat about weather nor discussions of Balzac's novels are protected under the privilege.After all, if the communication is not law-related, no privilege arises, regardless of whose computer was used to communicate.

The third *United Shoe Machinery* privilege theme, and the focus of this article, is "confidentiality," which has two elements. First, the client-attorney communication must be made in confidence.[16] And secondly, the communication must remain confidential thereafter.[17]

Typically, attorney-client communications occur privately.[18] A discussion held in a lawyer's office is one example; no strangers are present, nor is the setting such that others could readily overhear. Similarly, a client's written communications to counsel may also occur privately. A sealed letter sent to counsel qualifies as privileged. On the other hand, a handbill delivered to counsel and also distributed to passersby would not.

---

13. United States v. Frederick, 182 F.3d 496, 501 (7th Cir. 1999) (attorney acting as an accountant); *See In re* Spring Ford Indus., Inc., 2004 WL 1291223 (Bankr. E.D. Pa. 2004) (lawyer acting as foreign language translator). *See generally* GERGACZ, *supra* note 2, at 3.22-3.36.

14. Avianca, Inc. v. Corriea, 705 F. Supp. 666, 676 (D.D.C. 1989) ("Where the communication is with in-house counsel for a corporation, particularly where that counsel also serves a business function, the corporation must clearly demonstrate that the advice to be protected was given in a professional legal capacity."); *See generally* GERGACZ, *supra* note 2, at 3.18-3.19.

15. Celmer v. Marriott Corp., 2004 WL 1822763, at *3 (E.D. Pa. 2004) (incident report sent to corporate claims department initially and thereafter sent to counsel found to be an ordinary business communication rather than a communication with counsel.); *See generally* GERGACZ, *supra* note 2, at 3.43-3.47.

16. Upjohn Co. v. United States, 449 U.S. 383, 395 (1981); *See generally* GERGACZ, *supra* note 2, at 3.56-3.66.

17. *In re* Penn Cent. Commercial Paper Litig., 61 F.R.D. 453, 463 (S.D.N.Y. 1973) ("It is hornbook law that the voluntary disclosure or consent to the disclosure of a communication, otherwise subject to a claim of privilege, effectively waives the privilege."); *See generally* GERGACZ, *supra* note 2, at 5.01-5.64.

18. *See E.g.*, *In re* Keeper of the Records, 348 F.3d 16, 23 (1st Cir. 2003). *See generally* GERGACZ, *supra* note 2, at 3.63-3.66 (calling this attribute of confidentiality, the confidentiality setting).

Further, even if the communication's setting is private, the prospective use of the information also affects its confidentiality.[19] For the attorney-client privilege to arise at all, confidentiality must be intended at the time of communication.[20] Information conveyed in confidence reflects a client's intent that it be the basis upon which legal advice is based. In fact, it is the assurance of confidentiality that encourages clients' communications in the first place. On the other hand, if counsel received information with instructions to convey it to a third party, the client's intent in providing it was for its dissemination, and the privilege would not apply. This "client-intent" element may be inferred from both the communication's setting and from the intended use of the information provided to counsel.

Privilege confidentiality, however, has a second element as stated. The client-attorney communications must remain confidential after they occur.[21] They may not thereafter be disclosed and their secrecy must be safeguarded. A breach in the confidentiality seal waives the protection and the communication becomes discoverable. For example, clients who tell their friends the details of yesterday's meeting with counsel lose the privilege, as does a privileged letter stored in a place where outsiders have ready access.[22]

Recently, several cases arose in which discovery was sought of client communications with counsel conducted over the client's employer's computer.[23] Their focus was whether the means of communication jeopardized the confidentiality required for attorney-client privilege to apply. This article

19. *In re* Ampicillin Antitrust Litig., 81 F.R.D. 377, 390 (D.D.C. 1978) ("[W]here a business proposal is sent to counsel for legal advice, with an accompanying expressed intent to disclose the proposal to a third party, the communication will not be deemed to be made in confidence and thus will not be privileged."). *See generally* GERGACZ, *supra* note 2, at 3.59.

20. *E.g.*, Ashkinazi v. Sapir, No. 02CV0002(RCC), 2004 WL 1698446, at *1 (S.D.N.Y. 2004); *In re* Grand Jury Subpoena, 679 F. Supp. 1403, 1410 (N.D. W.Va. . 1988). *See generally* GERGACZ, *supra* note 2, at 3.58-3.59.

21. United States v. Jones, 696 F.2d 1069, 1072 (4th Cir. 1982) ("Any disclosure inconsistent with maintaining the confidential nature of the attorney-client relationship waives the attorney-client privilege."); Permian Corp. v. United States, 665 F.2d 1214, 1222 (D.C. Cir. 1981) ("We believe that the attorney-client privilege should be available only at the traditional price: a litigant who wishes to assert confidentiality must maintain genuine confidentiality.").

22. Bower v. Weisman, 669 F. Supp. 602, 606 (S.D.N.Y. 1987) ("[L]eaving a document out on a table (as opposed to putting it in a briefcase or in a drawer) in a public room in a suite in which another person is staying is insufficient to demonstrate Weisman's objective interest in its confidentiality. Consequently, Weisman may not assert attorney-client privilege with respect to the letter in question."); *See generally* GERGACZ, *supra* note 2, at 5.42.

23. *In re* Asia Global Crossing, Ltd., 322 B.R. 247, 251 (Bankr. S.D.N.Y. 2005); *See* People v. Jiang, 33 Cal. Rptr.3d 184 (Cal. Ct. App. 2005); *See* Reno v. Reno Police Protective Ass'n, 59 P. 3d 1212 (Nev. 2002).

will consider those cases within a general discussion of the issue, and will analyze three aspects: whether the mere use of the employer's computer is sufficient to compromise the confidentiality of the employee's otherwise privileged communications, whether use in derogation of the employer's "no personal use" policy undermines an employee's confidentiality expectation, and whether encrypting the communication would strengthen the employee's claim for privilege.

## III. Employee's Mere Use of Employer's Computer, Personal-Use Prohibition Policy Lacking

The *In re Asia Global Crossing* case is helpful in analyzing whether, by itself, an employee's use of an employer's computer when communicating with counsel affects the privilege.[24] Asia Global Crossing was in bankruptcy and its bankruptcy trustee was investigating transactions involving the corporation's principal officers.[25] The officers used company computers to communicate with their personal attorneys.[26] The trustee sought access to those attorney-client e-mails, copies of which remained on Asia Global Crossing's servers.[27] The officers asserted the attorney-client privilege to block disclosure.[28]

Throughout its decision, the court assumed that the officers' privilege would apply but for their use of Asia Global Crossing's e-mail system.[29] The focus was on the communications' confidentiality and whether it was thus impaired. For guidance, the court consulted several cases concerning an employee's expectation of personal privacy when using an employer's computer system.[30] These decisions, although useful, should not be considered equivalent to a determination of privilege confidentiality. Privacy seems to

24. *In re* Asia Global Crossing, Ltd., 322 B.R. 247 (Bankr. S.D.N.Y. 2005).

25. *Id*. at 252.

26. *Id*.

27. *Id*.

28. *Id*. at 253.

29. *Id*. at 258 ("As noted earlier, the Court assumes that the Insider E-mails are otherwise privileged, and further, that the Insiders subjectively intended that they be confidential. Thus, the question of privilege comes down to whether the intent to communicate in confidence was objectively reasonable.").

30. *Id*. at 256-258 (This employee privacy expectation was considered analogous to the similar privacy question at hand: whether the employee-client intended that the communications with counsel be confidential. Four factors were derived from the privacy cases for analyzing the privilege-confidentiality issue. "(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?").

be a more limited concept and narrower in its relation to confidentiality than what the attorney-client privilege requires of confidentiality.

"Privacy" may be defined as "the quality or state of being apart from company or observation."[31] In an attorney-client setting, privacy would entail no other person being present or observing the communication. An attorney and client meeting alone in the lawyer's office is private. An e-mail message sent by the client exclusively to the lawyer would also be private, at least when compared with copying it to a third party or posting it on a personal webpage. These examples of privacy also encompass confidentiality for purposes of the attorney-client privilege because the client most likely wants such communications to be confidential.[32] Both the setting in which the communication took place and client intent are apparent.

However, privilege confidentiality is not synonymous with "privacy." Under privilege law, confidentiality is tied to the purpose of the rule. Thus, privilege confidentiality may exist in circumstances that would not be considered private. For example, a third party's presence during an attorney-client meeting is acceptable for privilege confidentiality if that person is needed to facilitate the communication (e.g., a language translator).[33] Similarly, although a voyeur or eavesdropper may breach one's privacy, neither one may affect the privilege confidentiality of an attorney-client conversation.[34]

Nonetheless, the privacy cases discussed in *Asia Global* provide sound guidance for analyzing the employer computer-use issue.[35] After all, private attorney-client communications are likely also confidential in certain circumstances, as discussed above.[36] Further, the privacy cases in *Asia Global* fo-

31. WEBSTER'S NEW COLLEGIATE DICTIONARY (G.C. Merriam Co. 1973), *available at* http://www.webster.com/dictionary/privacy.

32. *See In re* Ampicillin Antitrust Litig., 81 F.R.D. 377, 385-87 (D.D.C. 1978); Ashkinazi v. Sapir, No. 02CV0002, 2004 WL 1698446, at *2 (S.D.N.Y. July 28, 2004).

33. *See also* United States v. Kovel, 246 F.2d 918, 921 (2d Cir. 1961) (explaining that if a third party is necessary or highly useful in facilitating a communication, privilege confidentiality will not be adversely affected); Farahmand v. Jamshidi, No. Civ.A.04-542(JDB), 2005 WL 331601, at *3 (D.D.C. Feb. 11, 2005) (holding that the presence of a foreign language translator did not destroy privilege confidentiality); *See* GERGACZ, *supra* note 2 at 3.65.

34. *See also* United States *ex rel* Mayman v. Martin Marietta Corp., 886 F. Supp. 1243, 1246 (D. Md. 1995) (explaining that privilege was not waived when a document was stolen because reasonable security precautions had been taken). *See* GERGACZ, *supra* note 2 at 5.42, 5.44.

35. *Asia Global*, 322 B.R. at 256-57.

36. *See In re* Ampicillin Antitrust Litig., 81 F.R.D. 377, 385-87 (D.D.C. 1978); Ashkinazi v. Sapir, No. 02CV0002, 2004 WL 1698446, at *2 (S.D.N.Y. July 28, 2004); *See also* United States v. Kovel, 246 F.2d 918, 921 (2d Cir. 1961)

cused on the client's expectation.[37] This focus is similar to the client's intent regarding privilege confidentiality.[38] *Asia Global* derived four factors from its cited privacy cases:

1. Do the employer's policies ban personal or other objectionable use of its computers?
2. Does the employer monitor its employees' computer activities and e-mails?
3. Do third parties have a right of access to company computers and employee e-mails?
4. Did the employer notify employees about the above or were employees aware?[39]

The court further noted that confidentiality is fact-sensitive.[40] These factors are rearranged around two aspects of privilege confidentiality: the second and third factors indicate the setting in which an attorney-client communication takes place, and the first and fourth signify the client's intent.[41]

Unfortunately, the record before the court was inadequate to conduct a proper analysis.[42] The court was unable to determine even whether the employer had a no-personal-use policy, let alone whether the employer monitored its employees' computer use.[43] The record showed only that the officers sent e-mails using Asia Global's computers, which were then stored on the company's servers.[44] Consequently, without sufficient information, the court could not find that the privilege had been waived, but the court recognized that the privileged documents may be a subject of dispute in later proceedings[45]

Nonetheless, *Asia Global* provides a useful structure with which to analyze the employer computer-use issue. Application of the four rearranged

(explaining that if a third party is necessary or highly useful in facilitating a communication, privilege confidentiality will not be adversely affected).

37. *See Asia Global*, 322 B.R. at 256-57. .

38. *See Ampicillin*, 81 F.R.D. at 387.

39. *Asia Global*, 322 B.R. at 257.

40. *Id*. at 259. ("Accordingly, the objective reasonableness of that intent will depend on the company's e-mail policies regarding use and monitoring, its access to the e-mail system, and the notice provided to the employees.").

41. *Id*. at 257.

42. *Id*. at 247.

43. *Id*.

44. *See id*. at 253.

45. *Id*. at 254 (explaining that, in later proceedings, the employee would have the burden to establish privilege while using the employer's computer by using the four confidentiality factors, while the employer would have the burden to show waiver of privilege if the employer can access e-mails on the company server).

privilege factors indicates that employee use of the employer's computer, alone, will not be sufficient to bar the attorney-client privilege from arising. Nor should such use, by itself, constitute a waiver if a server-stored copy is readily accessible. Thus, privilege confidentiality should not turn on the means used to communicate. Instead, the facts surrounding the particular communication are key.[46]

Let us begin this analysis by assessing privilege confidentiality based on the *Asia Global* factors.[47] Consider the setting in which the e-mail communication takes place.[48] Privilege confidentiality looks at how the attorney and client conduct their communication.[49] The more open and unguarded the communication, the less the setting is a confidential one.[50] The *Asia Global* factors relevant to this inquiry are: the employer's no personal-use policy, if any; whether employee computer use is monitored, and whether third parties have access.[51] These factors describe various openness states, in which an e-mail's confidentiality diminishes. For example, the factors concerning employer monitoring and third party access suggest that others will see the employee's e-mails. Thus, under these factors, sending counsel e-mails would be no different from using workplace stationery to write a letter when the employer can read such letters. The lawyer and client may communicate, but their messages would be anything but confidential.

Alternatively, if these factors are not present, all that remains for attacking the confidentiality setting is the means through which the employee communicated, which is the employer's computer. As an analogy, consider an employee using the employer's telephone to speak with counsel. The mere instrumentality for their communication does not suggest a public setting. Similarly, an employee who writes counsel a letter on the employer's stationery also would not undermine confidentiality. The paper itself does not broadcast the message. Use of the employer's computer should be evaluated the same way. It merely facilitates the attorney and client's communication.[52]

---

46. *See id.* at 259.

47. *Id.* at 257.

48. *See* Keeper of Records v. United States, 348 F.3d 16, 23 (1st Cir. 2003).

49. *See id.*

50. *See id.*

51. *Asia Global*, 322 B.R. at 257.

52. *See also* CAL. EVID. CODE § 917(b) (West 2005) (explaining that a communication does not lose its privileged character because it is through electronic means); N.Y. C.P.L.R § 4548 (McKinney 1999) (explaining that no privileged communication loses its character because it is through electronic means).

In addition, privilege confidentiality also focuses on more direct indications of the client's confidentiality intent.[53] If the client communicates regardless of others who overhear, the intent is merely to speak with counsel, not to speak in confidence. Here, the factors focus on what the client knew about company policy, employer monitoring, and access by others. The more such knowledge factors exist, the less likely the client intended confidentiality. After all, if the client knows that the employer monitors e-mails to counsel, the message cannot be said to be private, as between attorney and client. The employer, as monitor, may be privy to it as well.

On the other hand, mere use of a company computer does not automatically carry with it such knowledge. As far as the employee knows only the lawyer-recipient will read the e-mails. There is no reason to presume that the employee "knows" or expects otherwise. The employer has not provided advisory information. Consequently, the client-employee's intended confidentiality should not be affected.[54]

As an analogy, consider again an employee speaking with counsel on the employer's telephone. The use of that telephone, alone, does not carry with it "knowledge" that others are listening in on the conversation. The client's confidentiality expectation would be no different than if using his own telephone. Thus, the means to communicate, by itself, does not trump a client's confidentiality-intent.

Consequently, it is unlikely that an employee's use of an employer's computer, alone, will bar the attorney-client privilege from attaching. However, even if those communications are privileged, that protection may be waived.[55]

Sent e-mails are like weeds in a garden. Once you think you have obliterated them all, they reappear. So it goes with e-mail. Unlike a letter, which has a physical form that is readily controlled and monitored, a sent e-mail scatters electronic copies all over the place. One may be in the sent-messages file. If deleted, it would tumble into the deleted-messages file. If that is deleted, too, a copy may remain on the computer's hard drive. If the employee uses the office e-mail system, there may be a stored copy on the employer's server.

For e-mails employees send to counsel, the existence of all these electronic copies raises a privilege waiver question.[56] Is privilege confidentiality lost if another employee, using the same employer-owned computer, or the employer, wading through stored messages on its servers, stumbles upon the

53. *See In re* Ampicillin Antitrust Litig., 81 F.R.D. 377, 385-87 (D.D.C. 1978); Ashkinazi v. Sapir, No. 02CV0002, 2004 WL 1698446, at *2 (S.D.N.Y. July 28, 2004).

54. *See also Ampicillin*, 81 F.R.D. at 387 (holding that the attorney-client privilege protects those communications that the client intends to be confidential).

55. *See Asia Global* 322 B.R. at 254.

56. *See generally* GERGACZ, *supra* note 2, at 5.01-5.64.

employee's e-mail to counsel? The waiver focus here is whether the e-mail communications with counsel are satisfactorily safeguarded. Here, the potential waiver stems from client inaction, from a failure to adequately protect confidentiality.[57] If a client does not show the e-mails to a third party, then there is no voluntary disclosure of their content.[58] The copies, as technological by-products, are then merely revealed by happenstance.

As an analogy, consider again a privileged letter. An employee voluntarily providing a copy to the employer undermines the letter's confidentiality. Similarly, storing a copy in an open file cabinet used by others risks waiver because nothing was done to protect it. Privilege does not entertain a greater responsibility for safeguarding confidentiality than does the client.[59] On the other hand, waiver would not likely arise if the letter copy was stored in a locked drawer, even if the copy was pilfered by a thief, since confidentiality would be reasonably safeguarded by lock and key.[60]

Two of *In re Asia Global Crossing*'s factors are useful here: first, whether the employee knew that third parties will have access to the computer or to the sent e-mails; second, whether the employee knew that the employer monitored computer use or sent e-mails.[61]

A great waiver risk arises when the employer's computers are shared and log-on passwords are for teams rather than individuals. Sharing passwords among team members leads to the possibility that a teammate-snoop could readily open the sent-messages file and read the e-mail that the employee sent to counsel. No barrier prevents this, except the snoop's own sense of decorum, which snoops clearly lack. Further, given the sharing arrangement, the employee knows that others will be handling the same computer, and even a novice understands that the machine stores easily accessible sent messages.

Without any safeguards in place, the e-mail copies are vulnerable, and privilege will likely be waived if their contents are seen. After all, simple protective steps could have been taken, such as deleting the copy from the sent-message file. Furthermore, deleting the copy from the deleted-messages file would make accessing it from the computer quite difficult. Failure to implement such safeguards may be seen as the employee-client's disregard for privilege confidentiality.

---

57. *Id*. at 5.42.

58. *Id*. at 5.43.

59. *See In re* Sealed Case, 877 F.2d 976, 980 (D.C. Cir. 1989) ("Normally the amount of care taken to ensure confidentiality reflects the importance of that confidentiality to the holder of the privilege . . . . In other words, if a client wishes to preserve the privilege, it must treat the confidentiality of attorney-client communications like jewels B if not crown jewels.").

60. *See* United States *ex rel* Mayman v. Martin Marietta Corp., 886 F. Supp. 1243, 1246 (D. Md. 1995).

61. *In re* Asia Global Crossing Ltd., 322 B.R. 247 (Bankr. S.D.N.Y. 2005).

However, even if the employee is given exclusive use of a computer and creates a personal password to sign-on, the sent e-mails still may leave an electronic version on the employer's servers. Since the employer has a right to access its own server, confidentiality may be affected if, when accessed, the employee's message to counsel is revealed.[62] Should avoiding a privilege waiver, if this happens, demand that the employee do something more? After all, if the employee left a copy of a privileged letter in the employer's file drawer, a waiver might result if the employer ran across it by chance.

However, server copies can be distinguished from hard copies. First, the server storage occurs simultaneously with the sending of an e-mail. The employee does not intentionally place a copy on the server. The server-storage is merely a technological adjunct to e-mail, unique to the means of communication. Second, unless advised otherwise, an employee would not expect server-stored messages to be viewed. Since electronic copies are typically stored, organized, and accessed on the employee's own computer, a server's storage is, thus, not akin to a file cabinet's. It is more like a technological refuse heap, where everything sticks due to the technology's design. Copies of important information, as well as useless marginalia, such as "Smith will be out of the office on July 8," are randomly intermixed. Nothing about server-storage, itself, gives notice to the employee that safeguards need to be in place to preserve privilege confidentiality from server access.

Perhaps, application of the privilege waiver doctrine should take its cue from Justice Holmes' use of the "one free bite rule" in *Bates v. Dresser*.[63] *Bates* concerned a breach of fiduciary duty claim filed against a Cambridge bank's board of directors.[64] An employee drained most of the bank's assets, using a novel swindle to do so.[65] In absolving the directors of responsibility, Holmes wrote that like the dog-owner whose gentle pet unexpectedly bites a neighbor, the directors should not be held responsible for guarding against a never-experienced-before theft of assets.[66]

Privilege waiver claims arising from employers accessing their servers to find copies of employee messages to counsel should be looked at the same

62. *See id*. at 259-263 (Asia Global Crossing's bankruptcy trustee was investigating the corporate officers whose e-mails to counsel, sent on company computers, were stored on their employer's servers). *Id*. at 252-53 (The trustee controlled the servers and, thus, had a right to view their contents). *Id*. *(*The court determined that it lacked sufficient information to find that a waiver occurred). *Id*. at 265.

63. *Bates v. Dresser*, 251 U.S. 524, 529 (1920) ("Some animals must have given at least one exhibition of dangerous propensities before the owner can be held. This fraud was a novelty in the way of swindling a bank so far as the knowledge of any experience had reached Cambridge before 1910.").

64. *Id*.

65. *Id*. at 528.

66. *Id*. at 529.

way as Justice Holmes viewed the directors in *Bates*. For many, digital technology is new, ever-changing, and largely mysterious. Employees should not be held to a high level in understanding its capabilities. Thus, their "safeguarding" responsibility certainly should not exceed that of dog-owners or the board of directors of the Cambridge bank in *Bates*.[67] The attorney-client privilege is too vital to make it so vulnerable to waivers.

Nonetheless, the above analysis assumes that the employee acted without notice that sent e-mails would be monitored. An employer's policy, in that regard, may well create heightened obligation, like the one placed on a dog-owner whose canine is known to bite. Once warned, it seems logical that the failure to use adequate safeguards enhances legal risk. The following section will focus on the effect of an employer's no-personal-use policy on an employee-client's attorney-client privilege.

## IV. Employee Use of Employer Computer in Derogation of Company Policy

An employee's personal use of company computers raises a number of problems for the business. For instance, it can be a time-waster. Following one's favorite team's exploits or keeping up with the latest celebrity gossip is neither an efficient use of the employee's time nor an effective use of company property. Additionally, hackers, viruses, and other ills more readily gain access to the employer's system when employees use it for non-business purposes. Consequently, employers often have policies designed to prohibit such use.[68] An employee's personal communication with counsel, by means of the employer's computer, would violate these rules. Disciplining that employee would be justifiable, as would be the case with any transgression of company policy. However, it does not follow that the mere existence of a no personal-use policy affects the employee's attorney-client privilege. For that to happen, the policy must alter the confidentiality of the communication. Thus, a link between the employer's policy and the privilege confidentiality factor must be established.

Consider as an analogy, a policy that prohibited personal use of company stationery. Letters to friends, grocery lists, or even notes to counsel written on employer-letterhead would violate the rule. All would be misuses of company property, irrespective of their contents. However, such letters would not be less confidential merely because they were written on company stationery rather than on the employee's stationary. No matter whose paper was used, the letters could be sealed in an envelope and sent through the mail without revealing their contents. Thus, the employee's expectation of confidentiality would not change merely by the employer's ownership of the stationery.

---

67. *See id.*

68. People v. Jiang, 33 Cal. Rptr. 3d 184, 204 (Cal Ct. App. 2005); Reno v. Reno Police Protective Ass'n, 59 P.3d 1212, 1219 (Nev. 2002).

Using an employer's computer in violation of company policy should be evaluated in the same manner. Although the computer use may be wrong, it would not, by itself, affect the confidentiality of the employee's communication. The employee could still reasonably intend that only the attorney be a party to the sent e-mail, in which the policy breach would be an employment transgression, but would not, by itself, hinder attorney-client confidentiality. For that to occur, two additional components must be present.[69]

The first additional component concerns monitoring.[70] Monitoring employee computer use would jeopardize the attorney-client privilege by threatening the communication's confidentiality setting. Not only would attorney and client have access to the e-mail, but so would an outsider, in the form of the employer. This setting may be likened to one in which a client sends not only a letter to counsel, but a copy of it to a friend. In both instances, privilege confidentiality would be undermined because the parties to the message extend beyond attorney and client.

The second component concerns the employee's awareness of the monitoring policy.[71] Awareness affects an employee's confidentiality intent. If an employee knows that others may be listening in, but communicates nonetheless, the intent is merely to provide information, not to do so confidentially.[72] Thus, sending an e-mail over a monitored system shows that communicating privately with counsel was not desired, since the employee should expect that the employer is also privy to the message. Such an expectation is inconsistent with the confidentiality intent that is required for attorney-client privilege; therefore, the protection will not likely attach.

Consequently, joining both employer monitoring and employee awareness components to a no personal-use policy substantially diminishes the prospect that attorney-client privilege will arise. Use of the employer's computer, alone, is not prohibited, but when an employee sends a message knowing that the message is available for outsiders to view, waiver may arise. Therefore, even if the privilege would attach to the initial attorney-client communications, a waiver will likely arise if the employer later retrieves the e-mail from its server.

Moreover, an employer's no-personal-use policy augmented by the monitoring and employee awareness components, makes any otherwise privileged e-mail sent to counsel vulnerable to a waiver. Since the employee

69. *In re* Asia Global Crossing Ltd., 322 B.R. 247, 257 (Bankr. S.D.N.Y. 2005) (considering four factors to measure an employer's expectation of privacy in his computer files and email).

70. *See id.*

71. *See id.*

72. *See* United States v. Jones, 696 F.2d 1069, 1072 (4th Cir. 1982); *see* Permian Corp. v. United States, 665 F.2d 1214, 1222 (D.C. Cir. 1981); *see* Bower v. Weisman, 669 F.Supp. 602, 606 (S.D.N.Y. 1987); *see In re* Penn Cent. Commercial Paper Litig., 61 F.R.D. 453, 463 (S.D.N.Y. 1973).

knows the employer may access a copy from its server, protective measures must be taken to preserve the e-mail's confidentiality; otherwise, the contents may be revealed. Failure to implement protective measures demonstrates the employee's disregard for confidentiality and, thus, jeopardizes the privilege.

As an analogy, consider an employee who stores a copy of a privileged letter in an employer's cabinet. Further, assume that the employee knows that the employer may check the cabinet for non-business filings. If, while doing so, the employer comes across that letter, its privileged status will not likely continue. After all, the employee did nothing to shield its contents, not even seal it in an envelope. Although a server's automatic retention of a copy may be distinguished from an employee intentionally storing a letter in a cabinet, the key for privilege waiver purposes is whether the employee took confidentiality protective measures. It is the lack of safeguards, such as knowing that computer usage or a file cabinet may be monitored, that enhances waiver risk.

Thus, an augmented no-personal-use policy compromises both confidentiality elements of the attorney-client privilege. Therefore, it is likely that employee e-mails sent to counsel will be discoverable. Nonetheless, the client-employee's prospects may be heightened if the message was encrypted.

## V. EMPLOYEE COMMUNICATIONS IN DEROGATION OF EMPLOYER POLICY, BUT COMMUNICATION IS ENCRYPTED[73]

Encrypted e-mails keep their contents hidden from anyone other than the intended recipient. Further, electronic documents may be stored in files that are password-protected, so that those without the key will not have access. Thus, an employee who encrypts communications with counsel creates a barrier that separates the fact that the communication occurred from access to the message itself. For example, an employer may see that an employee's e-mail was sent to A.Tourney@lawfirm.org or that a file stored on the employee's assigned computer was entitled "Notes to my attorney," but neither can be read.

Encrypting enhances the probability that the attorney-client privilege will attach. The technology barrier creates a private space setting for the communication, where the only ones within this space are those who the technology lets in, the employee and the attorney. In addition, encrypting the message shows the client's intent to communicate confidentiality. Therefore, erecting the barrier, an act apart from the communication, demonstrates that the client only wants counsel to be a party.

Similarly, an encrypted communication also lessens the risk of waiver. If a message to counsel is later detected, the mere fact that an employer

73. The term, "encryption," as used here, does not refer to any particular program or means to safeguard communication contents. Its focus, instead, is the barrier created between the viewer and the contents. Password-protecting a privileged file would, thus, be included in the term, as used here.

knows that an employee communicated with counsel does not reveal what was said.[74] Consequently, although the no-personal-use policy was violated, the confidentiality of the message remains intact.

Of course, the employer may hack into the encrypted files. However, it is unlikely that this will affect the privilege for numerous reasons. First, waiver requires more than some third party merely gaining access. The test is not one of ironclad secrecy. For example, neither thieves' nor eavesdroppers' actions alone can cause a waiver. The focus, instead, is on what the client did to impede their access.[75] Encrypting electronic messages, like locking a document in a safe, should be sufficient to ward off waiver, even if the barricade is overcome. Second, there is no need for privilege waiver law to sanction such activity, since the employer already knows that the employee violated company policy. Uncovering the content of the communication will have no effect. Third, property ownership has limits. The employer, who owns the equipment, is readily able to protect its interests without hacking into the message. Wrongful use of the computer is evident, and the employee could be disciplined irrespective of the message contents. Furthermore, providing an additional "hacking property right" would impose on the employee's privacy without enhancing the employer's control over use of its computers. The attorney-client privilege is not likely to give way so readily.

Consider, *People v. Jiang*, where an employee used an employer-provided laptop computer to prepare documents for his attorney related to a criminal charge he was facing.[76] The documents were stored in a password-protected file marked "Attorney."[77] The employer had a proprietor-information policy in place, which the employee had signed, providing that the employee would have no privacy in e-mail sent using the company's system or in any company-provided storage facility.[78] Furthermore, the employee was put on notice that the employer could inspect company property at any time.[79] Thus, unlike the situation in *In re Asia Global Crossing*, discussed

74. *See* S. Cal. Gas Co. v. Pub. Utils. Comm'n, 784 P.2d 1373, 1384 (Cal. 1990) ("The attorney-client privilege seeks to protect the conversations and communications between the attorney and client, not merely the conclusions developed by those conversations or the fact that such communications occurred.") (holding disclosure that the attorney had reviewed a document and the attorney's conclusion did not waive the privilege.). *See generally* GERGACZ, *supra* note 2 at 5.18.

75. *See* United States *ex rel* Mayman v. Martin Marietta Corp., 886 F. Supp. 1243, 1246 (D. Md. 1995).

76. People v. Jiang, 33 Cal. Rptr. 3d 184, 203 (Cal Ct. App. 2005).

77. *Id.*

78. *Id.*

79. *Id.*

earlier, there was no doubt that the employee knew he lacked privacy when using an employer's computer and what was stored could be inspected.[80]

The privilege issue arose in the employee's criminal case when the prosecutor subpoenaed the stored attorney-client documents from the employer, maintaining that since the policy gave the employer an inspection right, the documents were not confidential, and, thus, the attorney-client privilege did not apply.[81] With privilege confidentiality the key, the court focused on the client-employee's intent and whether, under the circumstances, his actions were reasonable.[82] The court noted three factors.[83] First, the material had been segregated, labeled, and password-protected, thus keeping prying eyes at bay.[84] Second, the employer's policy did not state that the company would hack into any such material found in its computers.[85] Therefore, an employee would not expect an employer to do so. Finally, the policy was designed to protect the employer's property interests rather than to invade employee privacy.[86] In fact, the policy did not even prohibit employee personal use of their employer-issued computers.[87] Thus, the employee's belief in the password-protected information's confidentiality was reasonable.[88] Consequently, the materials were held to be covered by the attorney-client privilege.[89]

*Jiang*'s analysis properly distinguished between the employee's work relationship with an employer and the employee-client's privilege relationship with counsel, thus, keeping the attorney-client privilege from being inadvertently smothered by workplace practices or regulations. Separating the two also permitted a clear focus on the attorney-client privilege's elements (e.g., communication confidentiality), which although possibly affected by workplace events, are nonetheless independent of them.

The separation-analysis, however, does not foreordain the outcome. Privilege holdings are still driven by the facts. Thus, *Jiang* could have had a different ending had the client-employee not password-protected his files, in which privilege confidentiality would not likely be found to exist.

---

80. *But Cf. In re* Asia Global Crossing Ltd., 322 B.R. 247, 261 (Bankr. S.D.N.Y. 2005).

81. *Jiang*, 33 Cal. Rptr. 3d at 203.

82. *Id.* at 205.

83. *Id.* at 203-205.

84. *Id.*

85. *Id.* at 204-05.

86. *Id.* at 205.

87. *Id.*

88. *Id.*

89. *Id.* at 207.

Finally, *Jiang*'s approach was consistent with the attorney-client privilege analysis, as discussed above. That is, the means by which a client communicates with counsel (e.g., by using an employer's computer) affects a finding of privilege only if the means also affects one of the privilege elements. However, alone, the means of communication is not the decisive factor.

## VI. CONCLUSION

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.

Three variants of the confidentiality-factor were explored in this article: first, whether mere use of the employer's computer affects a privilege claim; second, the degree to which an employer's no-personal-use policy may affect the privilege; and third, irrespective of the employer's policy, whether an employee who encrypts communications with counsel strengthens a privilege claim.

Employees' privilege assertions are most at risk if their communications violated company computer-use policy, the employees' understood that they were doing so, and the policy contained a monitoring provision. Nonetheless, this risk can be substantially limited through encryption.

Proper analysis requires that privilege issues (e.g., confidentiality) be separated from both employer-property issues and those arising from employer-employee relations. Even if an employee may face workplace discipline or dismissal for using the employer's computer to communicate with counsel, this factor should not, by itself, affect the employee's claim of privilege. Instead, privilege should be evaluated based on whether its elements are supported by the facts surrounding the specific attorney-client communication.