I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

Employee E-mails and the Concept of Earning the Privilege

JONATHAN LEVY*

I. INTRODUCTION

This Note addresses the applicability of the attorney-client privilege to employees who communicate with their attorneys via e-mail on an employer's computer, whether through the employer's server or a private e-mail account. The crux of this issue is that while employees may have a subjective belief in the confidentiality of such communications, they may be wrong. This is because employers often have policies that allow them to monitor an employee's computer usage and to take possession of e-mails sent from or viewed on company computers, whether on a work e-mail account or a private one.[1] Indeed, one study concluded that sixty-six percent of companies

---

* Jonathan Levy, J.D., The University of Texas School of Law, 2013. Thanks to the *I/S* editing team for helping develop this Note.

[1] *See* ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 459 (2011) (advising attorneys of the prevalence of employer policies allowing the company access to e-mail communications on its computers). Some states require companies to make employees aware of potential monitoring through such policies. *See* CONN. GEN. STAT. ANN. § 31-48d(b) (West 2003) (requiring prior written notice of potential monitoring except in limited circumstances); DEL. CODE ANN. tit. 19, § 705(b) (West 2005) (forbidding monitoring unless the employer either (1) provides notice of monitoring potential at least once each day that the employee accesses employer e-mail or Internet services, or (2) has given a one-time notice of a monitoring policy in writing or electronic record acknowledged by the employee).

And as for federal statutes, for an article proposing an interpretation of the Electronic Communications Privacy Act (ECPA) and Stored Communications Act that would provide more protection for employees' e-mails, see Ariana R. Levinson, *Toward a Cohesive Interpretation of the Electronic Communications Privacy Act for the Electronic Monitoring of Employees*, 114 W. VA. L. REV. 461, 485–529 (2012). *But see* Lawrence E. Rothstein, *Privacy or Dignity?: Electronic Monitoring in the Workplace*, 19 N.Y.L. SCH. J.

monitor Internet use and forty-three percent monitor e-mail use.[2] Moreover, companies often later retrieve e-mails that are stored on their servers.[3] E-mails are therefore "like weeds in a garden. Once you think you have obliterated them all, they reappear."[4]

While "[n]othing about server-storage, itself, gives notice to the employee that safeguards need to be in place to preserve privilege confidentiality from server access,"[5] employer policies may give such notice.[6] One court declared that a belief that e-mails would not be stored and retrievable given such notice was "unreasonable . . . in this technological age . . ." [7] Nevertheless, employees continue to communicate with their attorneys via e-mail on company computers.[8] Thus, in this situation "legal principle collides with reality"[9] and

---

INT'L & COMP. L. 379, 401–03 (2000) (noting that the ECPA "has generally proven ineffective in protecting employees in the workplace from their employers' monitoring" and pointing to three exceptions in the statute that give employers practically free rein to monitor).

[2] *See The Latest on Workplace Monitoring and Surveillance*, AM. MGMT. ASS'N (Mar. 13, 2008), http://www.amanet.org/training/articles/The-Latest-on-Workplace-Monitoring-and-Surveillance.aspx (summarizing the findings of the 2007 Electronic Monitoring & Surveillance Survey).

[3] *See, e.g.*, Curto v. Med. World Commc'ns, Inc., No. 03CV6327 (DRH) (MLO), 2006 U.S. Dist. LEXIS 29387, at *3–4 (E.D.N.Y. May 15, 2006) (including forensic retrieval of e-mails in the factual scenario); Nat'l Econ. Research Assocs. v. Evans, 04-2618 BLS2, 2006 Mass. Super. LEXIS 371, at *3–4 (Mass. Super. Aug. 3, 2006) (same); Stengart v. Loving Care Agency, Inc., 990 A.2d 650, 656 (N.J. 2010) (same); Banks v. Mario Indus., 650 S.E.2d 687, 691 (Va. 2007) (same).

[4] 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, 278 (2006).

[5] *Id.* at 280.

[6] *See infra* Part II.C (explaining cases in which employers' policies make clear that employees have no expectation of privacy in the use of company computers).

[7] Alamar Ranch, LLC v. Cnty. of Boise, No. CV-09-004-S-BLW, 2009 U.S. Dist. LEXIS 101866, at *11 (D. Idaho Nov. 2, 2009).

[8] *See* John K. Villa, *Emails Between Employees and Their Attorneys Using Company Computers: Are They Still Privileged?*, 26 No. 3 ACC DOCKET 102, 102 (2008) (observing that employees use corporate computers for otherwise privileged attorney communications "even in matters where the employee and the company are adverse").

[9] *Id.*

judges have to "decide whether a commonly held incorrect belief is an objectively reasonable one."[10]

Courts addressing the applicability of the attorney-client privilege to employees who communicate with their attorneys via e-mail on an employer's computer have come up with a variety of conclusions.[11] One commentator points out why this might be the case:

> [P]roblems may emerge when considering such variables as (1) use of a personal password-protected e-mail account, (2) other employees' use of personal e-mail at work, (3) employee attempts to delete or hide files from the employer, (4) the forensic method used by the employer to recover information, or (5) any other technologically related facts where the court is unable to easily determine the objective relevance of the evidence.[12]

Indeed, with the rich variety of factual scenarios that accompany this issue, it may be that courts "reverse-engineer[]" decisions to reach the desired result.[13]

The goal of this Note is to propose and defend an analytical framework for this issue that will lead to greater predictability in cases and will create workable compromises. This Note proposes that courts replace the current reasonableness test with the following two-part test: (1) The attorney-client privilege is presumed to not apply if, and only if, there is a clear policy allowing monitoring or retrieval of e-mails, and the employee knows or should know about it;[14] (2) The employee can override that presumption by attempting to protect his e-mails at all relevant times.

---

[10] Adam C. Losey, Note, *Clicking Away Confidentiality: Workplace Waiver of Attorney-Client Privilege*, 60 FLA. L. REV. 1179, 1201 (2008).

[11] *See infra* Part II.C (outlining the holdings and rationales of many courts).

[12] Losey, *supra* note 10, at 1203; *see also infra* Parts II.C, III.A–B (discussing those and other variables).

[13] Losey, *supra* note 10, at 1199.

[14] For another note that proposes beginning with such a presumption, see Losey, *supra* note 10, at 1202–04 (arguing that the application of a presumption of waiver as a first step will prevent the collision of the "broad (modern) approach" to and the "narrow (traditional) interpretation" of the attorney-client privilege).

To set the stage for the proposal, Part II will discuss the competing policies underlying the attorney-client privilege by summarizing *In re Asia Global Crossing, Ltd.*,[15] the leading case on this issue, and explain the recent body of case law. Part III will then explain the proposal, apply it to certain factors, discuss its benefits, and address objections. Finally, Part IV will summarize the proposal, discuss the significance of the recent ABA opinion on attorneys' duties to clients regarding workplace e-mails, and note the limitations of the proposal with respect to the future.

II. BACKGROUND

A. *Policies Underlying the Attorney-Client Privilege*

Because employee e-mails on an employer's computer presents a gray area with respect to the attorney-client privilege, whether one would apply the privilege in a given scenario may depend on what underlying policy one holds as more important. On the one hand, application of the privilege may keep out relevant evidence. Professor Wigmore argued that the privilege "ought to be strictly confined within the narrowest possible limits consistent with the logic of its principle," because while "[the privilege's] benefits are all indirect and speculative[,] its obstruction is plain and concrete . . . . It is worth preserving for the sake of a general policy, but it is nonetheless an obstacle to the investigation of the truth."[16]

On the other hand, the privilege's "purpose is to encourage full and frank communication between attorneys and their clients and thereby promote broader public interests in the observance of law and administration of justice."[17] Without the protection of the privilege,

---

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

[16] 8 JOHN HENRY WIGMORE, EVIDENCE IN TRIALS AT COMMON LAW § 2291 (John T. McNaughton ed., rev. ed. 1961), *quoted in* Losey, *supra* note 10, at 1185; *accord* Aventa Learning, Inc. v. K12, Inc., 830 F. Supp. 2d 1083, , 1110 (W.D. Wash. 2011) ("The privilege is so limited because it sometimes results in the exclusion of relevant and material evidence, contrary to the philosophy that justice requires the fullest disclosure of the facts." (quoting Sitterson v. Evergreen Sch. Dist. No. 114, 196 P.3d 735, 741 (Wash. Ct. App. 2008))); Kelcey Nichols, *Hiding Evidence from the Boss: Attorney-Client Privilege and Company Computers*, 3 SHIDLER J. L. COM. & TECH. 6, 7 (2006) ("Courts construe attorney-client privilege narrowly because the privilege results in withholding information from the fact-finder.").

[17] Upjohn Co. v. United States, 449 U.S. 383, 389 (1980).

"the employee has a strong incentive to avoid seeking legal advice. This is the chilling effect the privilege is designed to prevent,"[18] but it occurs when an opponent can "fold the protections of privilege into a paper tiger."[19] But applying the privilege "provide[s] a shield which creates a safe harbor so that clients can confide in their attorneys with confidence."[20]

With respect to employee e-mails on employers' computers, both of these arguments come into play. Because employees and employers are generally opposing parties in these cases,[21] the latter have an interest in killing the application of the privilege in order to discover potentially helpful information. They have support in the Wigmore view. But if employers can "intercept[]" otherwise privileged attorney-client communications "without the employee's knowledge and [use them] against the employee," the "chilling effect" may occur.[22] So employees have a strong argument in favor of applying the privilege in these situations.

---

[18] Losey, *supra* note 10, at 1188.

[19] *Id.*, *quoted in* Louisa L. Hill, *Gone But Not Forgotten: When Privacy, Policy and Privilege Collide*, 9 NW. J. TECH. & INTELL. PROP. 565, 588 (2011). A paper tiger is "one that is outwardly powerful or dangerous but inwardly weak or ineffectual." MERRIAM-WEBSTER, http://www.merriam-webster.com/dictionary/paper%20tiger (last visited Mar. 27, 2013).

[20] Gergacz, *supra* note 4, at 271. For an argument that the need for clients' confidence in confiding in their attorneys outweighs the concern for admissibility of evidence purportedly covered by the privilege, see *id.* at 270–71.

[21] *See infra* Part II.C (providing numerous examples of cases in which an employee opposed his company). For examples of cases where a party other than the employer sought to utilize employee e-mails on the employer's computer, *see*, e.g., DeGeer v. Gillis, No. 09 C 6974, 2010 U.S. Dist. LEXIS 97457, at *2, *16 (N.D. Ill. Sept. 17, 2010) (co-employees who subpoenaed the employer for the external hard drive of the plaintiff's company-issued computer); United States v. Hatfield, No. 06-CR-0550 (JS), 2009 U.S. Dist. LEXIS 106269, at *2–3 (E.D.N.Y. Nov. 13, 2009) (United States, which obtained purportedly privileged material from the defendants' employer); Alamar Ranch, LLC v. Cnty. of Boise, No. CV-09-004-S-BLW, 2009 U.S. Dist. LEXIS 101866, at *2, *11 (D. Idaho Nov. 2, 2009) (plaintiff, who subpoenaed a nonparty's attorney for documents, some of which were e-mails sent by a client from her work address on a company computer).

[22] Losey, *supra* note 10, at 1188. *But see id.* at 1187 ("If courts apply the [Wigmore] view of attorney-client privilege, it is unclear whether employees would be discouraged from speaking with counsel while at work.").

B. *The Asia Global Decision*

Asia Global set the stage for the current reasonableness-based analysis of the attorney-client privilege's applicability to employee e-mails. In *Asia Global*, the Chapter 7 trustee of Asia Global's bankruptcy case was investigating certain transactions of five of the company's principal officers.[23] The officers withheld from production certain e-mails containing attorney-client communications that were left on the company e-mail servers.[24] Following the trustee's motion to compel production, the trustee argued that use of the company e-mail system destroyed the privilege *per se* and, alternatively, that Asia Global's e-mail policy signified that use of the e-mail system amounted to a waiver of otherwise privileged material.[25] The company officers being investigated argued that there was no such e-mail policy.[26]

The court's central holding was that "the use of [a] company's e-mail system does not, without more, destroy the privilege."[27] In addition, the court held that because of conflicting evidence as to whether an e-mail policy even existed, the use of Asia Global's e-mail system did not render the privilege waived.[28]

But the import of *Asia Global* was in its analysis. The court first set out the requirement of confidentiality for the privilege to apply: "The attorney-client privilege applies only to a confidential communication . . . . Confidentiality has both a subjective and objective component; the communication must be given in confidence, and the client must *reasonably* understand it to be so given."[29] The court then discussed Fourth Amendment cases in order to arrive at a framework for determining the reasonableness of a given employee who uses his or her company's e-mail server to communicate with his or her attorney, and who believes the

---

[23] *In re* Asia Global Crossing, Ltd., 322 B.R. 247, 252 (Bankr. S.D.N.Y. 2005).

[24] *Id.* at 253.

[25] *Id.*

[26] *Id.*

[27] *Id.* at 251.

[28] *Id.* at 259-61.

[29] *Id.* at 255.

communication is confidential.[30] It asserted 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."[31]

The court adapted the privacy analysis to employee e-mails on employers' computers and enumerated four factors that courts should look to in determining whether an employee's expectation of privacy in those e-mails was reasonable:

> (1) [D]oes 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?[32]

These factors have proven to have lasting significance, as many cases have applied them to the issue of employee e-mails on employers' computers.[33]

C. *Explanation of Recent Case Law*

The purpose of this subpart is to show how cases since *Asia Global* have analyzed the applicability of the attorney-client privilege to employee e-mails on employers' computers. This includes application of the *Asia Global* factors and other considerations such as the use of

---

[30] *Id.* at 256–58.

[31] *Id.* at 258–59. *But see generally* Edward J. Imwinkelried, *The Dangerous Trend Blurring the Distinction Between a Reasonable Expectation of Confidentiality in Privilege Law and a Reasonable Expectation of Privacy in Fourth Amendment Jurisprudence*, 57 LOY. L. REV. 1 (2011) (arguing that courts should not use an expectation-of-privacy analysis in privilege cases).

[32] *Asia Global*, 322 B.R. at 257.

[33] *See, e.g.*, Dombrowski v. Governor Mifflin Sch. Dist., No. 11-1278, 2012 WL 2501017, at *6 (E.D. Pa. June 29, 2012); Goldstein v. Colborne Acquisition Co., 873 F. Supp. 2d 932, 935–36 (N.D. Ill. June 1, 2012); Aventa Learning, Inc. v. K12, Inc., 830 F. Supp. 2d 1083, 1109-11 (W.D. Wash. 2011); *In re* Royce Holmes, LP, 449 B.R. 709, 737–41 (Bankr. S.D. Tex. 2011); Scott v. Beth Israel Med. Ctr. Inc., 847 N.Y.S.2d 436, 441–43 (N.Y. Sup. Ct. 2007).

a personal, password-protected e-mail account and the location of the computer.

1. *Clarity of the Employer's Computer Usage Policy*

Before a computer usage policy can kill the privilege, the court must first hold that such a policy applies. For example, in *Asia Global*, the court held that because an applicable e-mail policy may not have even existed, use of the company e-mail system did not kill the privilege.[34] Additionally, in *TransOcean Capital, Inc. v. Fortin*,[35] TransOcean hired another company to handle its human resources matters, and the hired company had its own computer policy.[36] But TransOcean "neither explicitly nor implicitly adopted [the policy] as its own."[37] The court held that Fortin did not waive the privilege through the use of TransOcean's e-mail system.[38]

Sometimes there is an applicable company policy, but it is too unclear to kill the privilege. In *Stengart v. Loving Care Agency, Inc.*,[39] the company policy, which gave the company access to "all matters on the company's media systems," neither defined "media systems" nor addressed personal e-mail accounts at all.[40] Therefore, "employees [did] not have express notice that messages sent or received on a personal, web-based e-mail account [were] subject to monitoring if company equipment [was] used to access the account."[41] The court held that Stengart had a reasonable expectation of privacy in the communications and that use of the company computer did not kill the privilege.[42] Likewise, in *National Economic Research Associates*

---

[34] *In re* Asia Global Crossing, Ltd., 322 B.R. 247, 259–61 (Bankr. S.D.N.Y. 2005).

[35] TransOcean Capital, Inc. v. Fortin, No. 05–0955–BLS2, 2006 WL 3246401 (Mass.Super. Oct. 20, 2006).

[36] *Id.* at *4.

[37] *Id.*

[38] *Id.* The court also held that some of those communications were waived for other reasons. *Id.* at *5.

[39] Stengart v. Loving Care Agency, Inc., 990 A.2d 650 (N.J. 2010).

[40] *Id.* at 659.

[41] *Id.*

[42] *Id.* at 655.

v. Evans,[43] the policy declared that the company would monitor "*sites*" but did not say so for "*content.*"[44] Moreover, the policy did not "declare, or even implicitly suggest, that [the company] would monitor the content of e-mail communications made from an employee's personal e-mail account" or that the e-mails would be stored.[45] And in *Orbit One Communications, Inc. v. Numerex Corp.*,[46] the policy stated that everything stored on company computers was recoverable except for "communications [that] may be subject to the attorney-client privilege . . . or some other protection which is recognized by the law."[47] Thus, it was "uncertain whether an employee's expectation of confidentiality would be unreasonable under any circumstances."[48]

Another source of the lack of clarity is when a policy does not ban personal use of computers. Courts differ on the significance of that circumstance: some courts find that an employee's expectation of privacy is more reasonable if the company policy does not ban personal use,[49] while others find that such a circumstance does not help the employee's case.[50] The difference seems to be around whether an employee may reasonably infer that privacy extends to e-mail use if it extends to personal use. Naturally, then, a policy that explicitly

---

[43] Nat'l Econ. Research Assocs. v. Evans, No. 04-2618 BLS2, 2006 Mass. Super. LEXIS 371 (Mass. Super. Aug. 3, 2006).

[44] *Id.* at *8–9.

[45] *Id.* at *9.

[46] Orbit One Commc'ns, Inc. v. Numerex Corp., 255 F.R.D. 98 (S.D.N.Y. 2008).

[47] *Id.* at 108 n.11.

[48] *Id.*

[49] *See, e.g.*, Convertino v. U.S. Dep't of Justice, 674 F. Supp. 2d 97, 110 (D.D.C. 2009) (citing the fact that the policy did not ban personal use as one reason the employee's expectation of privacy was reasonable); United States v. Hatfield, No. 06-CR-0550 (JS), 2009 U.S. Dist. LEXIS 106269, at *30–31 (E.D.N.Y. Nov. 13, 2009) (counting the fact that the policy did not "expressly prohibit" personal use in the employee's favor even though the policy stated that employees were "expect[ed]" to use company computers "solely for business purposes").

[50] *See, e.g.*, Aventa Learning, Inc. v. K12, Inc., 830 F. Supp. 2d 1083, 1109 (W.D. Wash. 2011) (averring that the personal use factor counted against applying the privilege because personal use was "discouraged" even though not banned outright); Banks v. Mario Indus., 650 S.E.2d 687, 695–96 (Va. 2007) (holding that the employee waived the privilege even though she was permitted to use work computers for personal business).

states that the company may monitor e-mail use often prevents the privilege from applying.[51]

2. *Monitoring*

The second *Asia Global* factor asks, "[D]oes the company monitor the use of the employee's computer or e-mail[?]"[52] Some cases suggest that the relevant question is whether the company actually monitors computer usage.[53] In *Curto*, the policy stated that the company "*may* . . . monitor use of computer resources."[54] In fact, the company did not enforce its usage policy except in four instances under very limited circumstances, and this led to a "false sense of security."[55] This was one reason the court held that the magistrate judge's ruling of no waiver was not clearly erroneous or contrary to law.[56] But other cases

---

[51] *See, e.g.*, Long v. Marubeni Am. Corp., No. 05Civ.639(GEL)(KNF), 2006 WL 2998671, at *3 (S.D.N.Y. Oct. 19, 2006) (holding that the privilege did not apply when the company policy stated that (a) personal use was banned, (b) employees "ha[d] no right of personal privacy in . . . e-mail," and (c) the company had the right to monitor its computers); Kaufman v. SunGard Inv. Sys., No. 05-cv-1236 (JLL), 2006 WL 1307882, *4 (D.N.J. May 10, 2006) (holding that the magistrate judge's ruling that the e-mails were not privileged was not clearly erroneous or contrary to law when the company policy stated that e-mails over the computer system were company property and subject to monitoring); Holmes v. Petrovich Dev. Co., 119 Cal. Rptr. 3d 878, 882–83 (Cal. Ct. App. 2011) (holding that the e-mails were not privileged because the company policy warned employees that personal use was banned, that the company would monitor its computers, and that employees using company computers for personal information or e-mails "have no right of privacy with respect to that information or message"); Scott v. Beth Israel Med. Ctr. Inc., 847 N.Y.S.2d 436, 440 (N.Y. Sup. Ct. 2007) ("[T]he effect of an employer e-mail policy, such as that of [Beth Israel], is to have the employer looking over your shoulder each time you send an e-mail.").

[52] *In re* Asia Global Crossing, Ltd., 322 B.R. 247, 257 (Bankr. S.D.N.Y. 2005).

[53] *See, e.g.*, Curto v. Med. World Commc'ns, Inc., No. 03CV6327 (DRH) (MLO), 2006 U.S. Dist. LEXIS 29387, at *23 (E.D.N.Y. May 15, 2006) ("Although the court in *Asia Global* did not explicitly discuss whether the employer actually monitored employees' computer usage, . . . it did recognize enforcement as a factor to be considered.").

[54] *Id.* at *2–3 (emphasis added).

[55] *Id.* at *8.

[56] *See id.* at *23–5.

suggest that it is irrelevant whether a company actually monitors computer usage as long as it clearly states it has the right to do so.[57]

3. *Knowledge Requirement*

Without knowledge of the company policy, an employee's belief in the confidentiality of his e-mail communications with his attorney is reasonable.[58] Because the *absence* of a policy renders the belief reasonable, and absence of the policy has the same effect (or noneffect) on one's belief as not knowing of the policy's existence, the same result follows for lack of knowledge. But a court may infer knowledge from circumstantial facts—it need not find actual knowledge, but rather that the employee knew of the policy *or should have known.* In this way, such knowledge can be constructive. This is often the case with employees in a supervisory role.[59]

---

[57] *See, e.g.*, *In re* Royce Holmes, LP, 449 B.R. 709, 739 (Bankr. S.D. Tex. 2011) ("Although the Trustee introduced no evidence on actual enforcement of the Debtor's monitoring policy, whether the Debtor actually reads an employee's e-mails is irrelevant."); Holmes v. Petrovich Dev. Co., 119 Cal. Rptr. 3d 878, 898 (Cal. Ct. App. 2011) ("Absent a company communication to employees explicitly contradicting the company's warning to them that company computers are monitored . . . it is immaterial that the 'operational reality' is the company does not actually do so."); Scott v. Beth Israel Med. Ctr. Inc., 847 N.Y.S.2d 436, 442 (N.Y. Sup. Ct. 2007) ("The second requirement is satisfied because [Beth Israel]'s policy allows for monitoring. Although BI acknowledges that it did not monitor Dr. Scott's e-mail, it retains the right to do so in the e-mail policy."); *see also* Jae Park, *Electronic Communications and the Attorney-Client Privilege*, MCKENNA LONG & ALDRIDGE LLP, 3 (Feb. 5, 2008), http://www.mckennalong.com/assets/attachments/Electronic_Communications_and_The_Attorney_Client_.pdf ("If a company clearly notifies its employees that personal e-mails and Internet use are not private and may be monitored, whether the company actually monitors e-mails and Internet use should be inconsequential.").

[58] Mason v. ILS Techs., LLC, No. 3:04-CV-139-RJC-DCK, 2008 U.S. Dist. LEXIS 28905, at *10 (W.D.N.C. Feb. 29, 2008) (holding that the employee's belief was reasonable where the company "fail[ed] to show that [it] effectively conveyed [the] . . . email policy").

[59] *See, e.g.*, United States v. Hatfield, No. 06-CR-0550 (JS), 2009 U.S. Dist. LEXIS 106269, at *32 (E.D.N.Y. Nov. 13, 2009) (stating that "it is fair and logical to presume that [the employee] had knowledge of" the policy when it was "implemented under his watch"); Aventa Learning, Inc. v. K12, Inc., 830 F. Supp. 2d 1083, 1107 (W.D. Wash. 2011) ("As a senior level manager, Mr. Benitez was 'expected to know the contents of company policies so [he] could properly manage and supervise employees.' Accordingly, Mr. Benitez is fairly charged with constructive knowledge of the company's policies concerning electronic communications." (citation omitted)); *Scott*, 847 N.Y.S.2d at 443 (holding that the employee had constructive knowledge of the policy where "[h]e required newly hired doctors under his supervision to acknowledge in writing that they were aware of the policy.").

4. *Use of a Personal, Password-Protected Account*

Courts are divided on the significance of the use of a personal, password-protected account. In *Evans*, it was one of several factors that led the court to conclude that the employee took adequate steps to ensure the confidentiality of his communications, thus securing the privilege.[60] In *Stengart*, the court held that the employee's expectation of privacy was objectively reasonable when the company policy did not specifically address personal accounts.[61] And the court went even further in dicta:

> Because of the important public policy concerns underlying the attorney-client privilege, even . . . a policy that . . . provided unambiguous notice that an employer could retrieve and read an employee's attorney-client communications, if accessed on a personal, password-protected e-mail account using the company's computer system—would not be enforceable.[62]

Likewise, in *Sims v. Lakeside School*,[63] the court drew a line based on policy considerations between e-mails Sims sent from his company account and those he sent from his personal account: after holding that Sims had no expectation of privacy over "Lakeside e-mails," the court held that "to the extent that the laptop contain[ed] web-based e-mails . . . such information is protected . . ."[64] The court explained, "[P]ublic policy dictates that such communications shall be protected

---

[60] Nat'l Econ. Research Assocs. v. Evans, No. 04-2618BLS2, 2006 Mass. Super. LEXIS 371, at *9, *11, *13 (Mass. Super. Aug. 3, 2006). Other contributing factors were that he did not save the e-mails as documents, he tried to delete all personal documents on his company laptop before returning it, and he defragmented the computer in an attempt to render his personal documents irretrievable. *Id.* at *11. *But see id.* at *5 (insinuating that the company could make e-mails from a personal account discoverable by stating clearly in its policy that such e-mails are stored and retrievable).

[61] Stengart v. Loving Care Agency, Inc., 990 A.2d 650, 663 (N.J. 2010).

[62] *Id.* at 665. For a discussion of these public policy concerns, *see supra* Part II.A.

[63] Sims v. Lakeside Sch., No. C06-1412RSM, 2007 WL 2745367 (W.D. Wash. Sept. 20, 2007).

[64] *Id.* at *2.

to preserve the sanctity of communications made in confidence."[65] One commentator also lends support to the *Sims* court's rationale: "Should an employee use company equipment to transmit a communication via a personal account rather than a company account, it stands to reason that the expectation of privacy increases."[66]

Other cases have held that the use of a personal, password-protected account does not make the expectation of privacy reasonable. In *Holmes v. Petrovich Development Co.*,[67] the court held that use of such an account was of no moment given the clear warning that employees had no expectation of privacy in e-mails on company computers: "This is akin to consulting [one's] attorney in one of defendants' conference rooms, in a loud voice, with the door open, yet unreasonably expecting that the conversation overheard by [the employer] would be privileged."[68] In *Long v. Marubeni America Corp.*,[69] the employees, despite using personal accounts, "disregarded the [company policy's] admonishment voluntarily and, as a consequence, ha[d] stripped from the e-mail messages . . . the confidential cloak with which they claim[ed] those communications were covered."[70] In *Aventa Learning, Inc. v. K12, Inc.*,[71] the court stated there was "no reason to distinguish between emails that were sent from or received on the company's email system and emails that were accessed through the company's laptop on [the employees'] web-based email accounts."[72]

Although many courts have weighed in on the effect of using a personal, password-protected account, at least one court explicitly left the issue open, "leav[ing] for another day whether there is waiver

---

[65] *Id.*

[66] Hill, *supra* note 19, at 590.

[67] Holmes v. Petrovich Dev. Co., 119 Cal. Rptr. 3d 878 (Cal. Ct. App. 2011).

[68] *Id.* at 896.

[69] Long v. Marubeni Am. Corp, No. 05Civ.639(GEL)(KNF), 2006 WL 2998671 (S.D.N.Y. Oct. 19, 2006).

[70] *Id.* at *3.

[71] Aventa Learning, Inc. v. K12, Inc., 830 F. Supp. 2d 1083 (W.D. Wash. 2011).

[72] *Id.* at 1110.

when the employee attempts to protect work-based e-mails through a personal password-protected web site."[73]

5. *Location of the Computer*

At least two courts have suggested that the location of the computer is a significant factor (one that was not included in *Asia Global*), holding that an expectation of confidentiality was reasonable where the employee did not use the computer in the employer's offices.[74] The implication is that it is reasonable to believe that if an employer cannot get his or her hands on the physical computer, then neither can the employer get expunged e-mails sent from or viewed on the computer while it was not connected to the company server. One commentator supports that view, arguing that "[t]he physical location of the computer has logical and legal significance in workplace waiver cases . . . . Allowing an employee to take a computer into his or her home, then later using information stored on that computer against the employee, smacks of a Trojan Horse."[75]

III. ANALYSIS

A. *The Proposal*

Rather than trying to determine the reasonableness of a belief in e-mail confidentiality, courts should apply the following test: (1) The privilege is presumed to not apply if, and only if, there is a clear policy allowing monitoring or retrieval of e-mails, and the employee knows

---

[73] Alamar Ranch, LLC v. Cnty. of Boise, No. CV-09-004-S-BLW, 2009 U.S. Dist. LEXIS 101866, at *10–11 (D. Idaho Nov. 2, 2009).

[74] *See* Curto v. Med. World Commc'ns, Inc., No. 03CV6327 (DRH) (MLO), 2006 U.S. Dist. LEXIS 29387, at *16–17 (E.D.N.Y. May 15, 2006) (distinguishing the facts from those in Fourth Amendment cases by use of the computer at home, holding that the employee's belief in the confidentiality of the e-mails was reasonable where the computer was not connected to the company's server and the employee deleted all personal files before returning the computer, and limiting the holding to whether use of a company computer at home waives the privilege); Orbit One Commc'ns, Inc. v. Numerex Corp., 255 F.R.D. 98, 108 (S.D.N.Y. 2008) (analogizing the facts to those of *Curto* because the company "never had ready access to [the employee's] computer" and holding that the expectation of confidentiality was reasonable under the circumstances).

[75] Losey, *supra* note 10, at 1197 (footnotes omitted).

or should know about it; (2) The employee can override that presumption by attempting to protect his e-mails at all relevant times.

1. *Step One: Presumption That the Privilege Does Not Apply*

Without a policy clearly allowing employers to view employee e-mails, the privilege should apply. With such a policy, the privilege should be presumed dead. The *Stengart* and *Evans* cases show how clear the policy should be.[76] As a practical matter, companies should err on the side of clarity because if they do not, courts that are otherwise inclined to favor the application of the privilege will in fact apply it.[77] And courts *should* apply it in that scenario. If a reasonable person could interpret a company policy to mean that employees had a reasonable expectation of confidentiality, then by definition, an employee's belief in the confidentiality of those e-mails is objectively reasonable.

But if the policy clearly allows the employer to view an employee's e-mails and the employee understands this, then an employee's expectation of confidentiality should be presumed unreasonable. One commentator explicitly promotes the use of such a presumption.[78] Another commentator recommends utilizing Justice Holmes's "one free bite rule" in *Bates v. Dresser*[79] for analyzing employee e-mails.[80]

---

[76] *See supra* notes 39–45 and accompanying text. *But see* Fazio v. Temp. Excellence, Inc., No. A-5441-08T3, 2012 WL 300634, at *13 (N.J. Super. Ct. App. Div. Feb. 2, 2012) (distinguishing this case from *Stengart* and holding that even where the company lacked an e-mail policy, the e-mails were not privileged because the employee "took no steps whatsoever to shield the e-mails from his employer" and "us[ed] his employer's own e-mail system on its own computer equipment, and did not password-protect those communications"). *Fazio* shows that it may even be better for employers to have no policy than an unclear one; under *Fazio*, use of the employer's server may be enough to warn of monitoring.

[77] *See, e.g.*, Stengart v. Loving Care Agency, Inc., 990 A.2d 650, 655, 665 (N.J. 2010) (declaring in dicta that even a clear policy would not trump the privilege when the employee uses a personal, password-protect account, and holding that the employee had a reasonable expectation of privacy in the e-mails because the application of the policy was not clear enough).

[78] Losey, *supra* note 10, at 1204 ("If the policies make clear that the employee has no expectation of privacy while using a workplace computer, then it is logical to establish a presumption that privilege has been waived.").

[79] Bates v. Dresser, 251 U.S. 524 (1920).

[80] Gergacz, *supra* note 4, at 280.

In *Bates*, Holmes wrote, "Some animals must have given at least one exhibition of dangerous propensities before the owner can be held [liable]."[81] A policy that clearly allows an employer to view employees' e-mails is an "exhibition of dangerous propensities" when it comes to the confidentiality of attorney-client communications. And many other commentators, while not explicitly suggesting a no-privilege presumption, suggest that the existence of a clear company policy should diminish the reasonableness of an expectation of privacy in e-mails.[82] The Supreme Court also acknowledges the effect of company policies, noting that they "will of course shape the *reasonable* expectations of their employees, especially to the extent that such policies are clearly communicated."[83] The implication is that clear company policies lower the threshold for reasonableness—in other words, it becomes less likely that a given employee's expectation of privacy is reasonable because when there is a clear company policy, employees in general lower their expectations.

Whether a policy bans all personal use of company computers should not matter for the no-privilege presumption. Allowing personal use is logically consistent with an explicit warning that personal use, including e-mails, may be monitored. This is so because personal use need not be prohibited behavior—it can be permitted behavior that comes with a price, which may be that personal use may be monitored. Of course, if there is no policy stating that personal use may be monitored, perhaps allowing it increases the reasonableness of believing it will not be monitored, while banning it decreases the reasonableness because the ban serves as a warning. (Even with a personal-use ban, the absence of a policy that e-mails may be

---

[81] *Bates*, 251 U.S. at 529.

[82] *See, e.g.*, Gergacz, *supra* note 4, at 281 (following the discussion of the "one free bite rule," see *supra* notes 79–81 and accompanying text, with the statement that "[a]n 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"); Hill, *supra* note 19, at 590 ("[W]hen an employee uses a monitored company e-mail account on an employer-issued computer having knowledge of this type of company policy, any expectation of privacy should be diminished."); Kara R. Williams, Note, *Protecting What You Thought Was Yours: Expanding Employee Privacy To Protect the Attorney-Client Privilege from Employer Computer Monitoring*, 69 OHIO ST. L.J. 347, 363 (2008) ("[I]f the employer has a policy of monitoring its employees and the employee is aware of the policy, the attorney-client privilege may not apply because the employee 'understand[s] . . . that the communication is to be made known to others.'" (quoting *In re* Grand Jury Proceedings, 727 F.2d 1352, 1356 (4th Cir. 1984)).

[83] City of Ontario v. Quon, 130 S. Ct. 2619, 2630 (2010) (emphasis added).

monitored should render the expectation of privacy in e-mails *per se* reasonable. So many companies have monitoring policies that the absence of one is too significant.) But an explicit policy stating that personal use may be monitored enumerates the price of personal use if allowed—it thus takes away any evidentiary value of allowing personal use for the employee who thinks that means there will be no monitoring. So given such a policy, the fact that an employee may use the computer for personal matters should not make his expectation in the confidentiality of those matters more reasonable. Moreover, holding that the privilege trumps a company policy when the policy allows for personal use may lead to negative consequences for both employers and employees by encouraging prohibitions of personal use.[84]

As for whether actual monitoring or merely the right to monitor should be required, the latter is more logical. Whether a company policy states the employer "will" or "may" monitor computer usage, the employee presumably does not know whether the employer is actually monitoring. And given the prevalence of monitoring,[85] the mere allowance of it in a clear company policy should render an employee's expectation of confidentiality presumed unreasonable.[86]

2. *Step Two: The Concept of Earning the Privilege*

Even if a company policy creates a presumption that the privilege does not apply, employees should be able to override that presumption by showing they earned the protection of the privilege by attempting to protect the e-mails at all relevant times.

a. *Earning the Protection*

Employees should be able to overcome the presumption that the privilege does not apply to e-mails on employers' computers by showing, essentially, that they deserve the protection of the

---

[84] *Id.* at 2629–30 ("[M]any employers expect or at least tolerate personal use of such equipment by employees because it often increases worker efficiency." (citing Brief of Elec. Frontier Found. et al. as Amici Curiae Supporting Respondents, City of Ontario v. Quon, 130 S. Ct. 2619 (2010) (No. 08-1332)).

[85] *See supra* notes 1–4 and accompanying text.

[86] *But see infra* Part III.B.1 (showing how employees may earn the protection of the privilege under this Note's proposal if they know their employers do not actually monitor computer usage).

privilege.[87] Employees can do this by engaging in protective behavior at all relevant times.[88] Without engaging in protective behavior, employees are at best only assuming that the privilege would apply despite the clear threat to confidentiality from the company policy; under this proposal, it would not.[89]

In this way, the privilege is not a "paper tiger."[90] But it is a caged one. By engaging in protective behavior, employees can let the tiger out of its cage and enjoy its protection.

b. *Protective Behavior*

To raise the privilege above the presumption against it, employees should have to engage in behavior that they believe will prevent employers from viewing employee e-mails, whether on the employer's server or a private account. While this is related to the reasonable-expectation inquiry,[91] it is not necessarily connected. Employees can satisfy this facet of the test with behavior that a court would hold does not lead to a reasonable expectation of confidentiality. For example, while many courts hold that use of a private, password-protected account does not lead to a reasonable expectation of confidentiality,[92]

---

[87] This poses the reverse of the question the *Curto* court posed. In *Curto*, the "heart of the overriding question" was whether the employee's conduct was "so careless as to suggest that she was not concerned with the protection of the privilege." Curto v. Med. World Commc'ns, Inc., No. 03CV6327 (DRH)(MLO), 2006 U.S. Dist. LEXIS 29387, at *15 (E.D.N.Y. May 15, 2006). Here, rather than starting with the privilege then asking whether the employee's carelessness kills it, this proposal begins with the presumption that the privilege does not apply (assuming the company policy is clear) then asks whether the employee has earned the privilege.

[88] For specific examples of such behavior, see *infra* Part III.B.

[89] *See* Gergacz, *supra* note 4, at 283 ("Failure to implement protective measures demonstrates the employee's disregard for confidentiality and, thus, jeopardizes the privilege."). Under this Note's proposal, such disregard would not jeopardize the privilege because the privilege would not exist to begin with due to the presumption based on company policy. Rather, the failure to implement protective measures would prevent the employee from overriding the presumption against the application of the privilege.

[90] Losey, *supra* note 10, at 1188.

[91] *See* Hill, *supra* note 19, at 590 ("The expectation is especially increased if protective measures are taken, such as using a personal account that is password-protected, deleting a message, or intentionally not saving a message.").

[92] *See supra* notes 67–72 and accompanying text.

under the proposed test here, it could.[93] Conversely, employees can fail to satisfy this test with behavior that some courts hold does lead to a reasonable expectation of privacy. For example, while some courts hold that use of a company computer outside of the office renders an expectation of confidentiality reasonable, [94] under this test, an employee who uses a computer at home but fails to take protective action when handing the computer back to the employer jeopardizes the privilege.[95]

c. *At All Relevant Times*

There are two key time periods in this inquiry. One is when the employee uses the employer's computer for e-mail. At that moment, the employer may be monitoring the computer. The second is when the employer retrieves the e-mails. In order to overcome the presumption, the employee should be required to engage in behavior intended to protect confidentiality at both of those times, if applicable. If, for example, an employee deletes e-mails in an effort to prevent the employer from retrieving them, that alone should not overcome the presumption if the employee had not attempted to prevent the employer from monitoring the computer to begin with.

d. *State of Mind Requirement*

If one knows that a particular protective behavior would not work, then engaging in it cannot overcome the presumption. For example, in *Kaufman v. SunGard Investment Systems*,[96] the company policy warned that the employer had the right to access e-mails even if they were password-protected.[97] An employee with actual or constructive knowledge of that policy could not then overcome the presumption by using a personal, password-protected account. This is because the employee would not have a subjective belief in the confidentiality of the e-mails.

---

[93] *See infra* Part III.B.2 (discussing the circumstances under which using a personal, password-protected account would overcome the presumption against the privilege).

[94] *See supra* note 74 and accompanying text.

[95] *See infra* note 102 and accompanying text.

[96] Kaufman v. SunGard Investment Systems, No. 05-cv-1236 (JLL), 2006 WL 1307882 (D.N.J. May 10, 2006).

[97] *Id.* at *4.

B. *The Proposal Applied*

1. *Timing*

Before discussing how timing plays a role in this analysis, it is important to distinguish between non-application and waiver of the privilege. The privilege does not apply if the communication one seeks to protect is not confidential . . . .[98] The privilege is waived when, once it applies, the privilege-holder does not sufficiently protect it.[99]

If an employee fails to take action to protect e-mails from being monitored at the time he writes or views them, the privilege should not apply to begin with. One step employees can take toward earning the privilege is showing that they know the employer does not actually monitor computers, regardless of what the policy says.[100] For instance, in *Curto*, the company had monitored computers on only four occasions under limited circumstances.[101] If the employee knew that the company monitored computers under limited circumstances and that none of those circumstances applied to his situation, the privilege should be preserved. By discovering (or confirming) the truth about monitoring, employees would have taken protective measures, and the privilege should therefore apply.

If an employee fails to take action to protect e-mails from being retrieved at a later stage, the privilege, if any still exists,[102] should be

---

[98] *See In re* Asia Global Crossing, Ltd., 322 B.R. 247, 255 (Bankr. S.D.N.Y. 2005) ("The attorney-client privilege applies only to a confidential communication . . . . Confidentiality has both a subjective and objective component; the communication must be given in confidence, and the client must *reasonably* understand it to be so given.").

[99] *See, e.g.*, Gergacz, *supra* note 4, at 279 ("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.").

[100] Rather than placing the burden on the employer to show that the company actually monitors employee e-mails, this proposal requires the employee to show an absence of actual monitoring. After all, it is the employee's state of mind that is relevant.

[101] Curto v. Med. World Commc'ns, Inc., No. 03CV6327 (DRH) (MLO), 2006 U.S. Dist. LEXIS 29387, at *8 (E.D.N.Y. May 15, 2006).

[102] If the employee did not try to protect the e-mails from monitoring to begin with, the privilege would not still exist. But if the employee already earned the privilege at the time of potential monitoring, or if, for example, the employee used the employer's computer at home, where monitoring was not possible, then his later protective actions become dispositive.

held waived. Behavior that should preserve the privilege at this time includes deleting e-mails in order to protect them,[103] defragmenting the computer,[104] or encrypting e-mails.[105]

2. *State of Mind*

One factor in particular ought to turn on the employee's state of mind. If an employee uses a personal, password-protected account, the dispositive issue should be his motivation. If he uses such an account to prevent monitoring and retrieval of the e-mails, the privilege should survive because the use of a personal account would be a protective action. If instead the use of the personal account is coincidental, the presumption against the privilege should win out because there is, at best, only an assumption.

Of course, use of personal accounts is easy and commonplace, and it may be difficult to ascertain the motivation behind it. Courts can avoid this problem by presuming that use of a personal account where a workplace account was otherwise available had a protective goal, and placing the burden on the employer to show otherwise.[106]

C. *Benefits of the Proposal*

This proposal would introduce two compromises. First, it responds to both the concern of excluding relevant evidence and that of discouraging attorney communications. By presuming that the privilege does not apply if the company policy is clear, this Note's proposal tips the scale in favor of admissibility. But by allowing employees to override the presumption by earning the privilege, the

---

[103] *See* Nat'l Econ. Research Assocs. v. Evans, No. 04-2618 BLS2, 2006 Mass. Super. LEXIS 371, at *3 (Mass. Super. Aug. 3, 2006); *Curto*, 2006 U.S. Dist. LEXIS 29387, at *17. This is another example of behavior that can earn the privilege even though courts may hold that it does not lead to a reasonable expectation of confidentiality. *See, e.g.*, Banks v. Mario Indus., 650 S.E.2d 687, 695–96 (Va. 2007) (holding that a document was not privileged even though the employee deleted it from the employer's computer prior to forensic retrieval).

[104] *See Evans*, 2006 Mass. Super. LEXIS 371, at *3.

[105] *See* Gergacz, *supra* note 4, at 284 ("Encrypting electronic messages, like locking a document in a safe, should be sufficient to ward off waiver, even if the barricade is overcome.").

[106] *But see supra* Part III.A.2.d (showing where even use of a personal account cannot overcome the presumption against the privilege).

proposal allows clients to confide in their attorneys without discouraging such behavior: those employees who think that taking some action will protect the privilege are right, while those who stand idly by in the face of a clear company policy will not have the privilege to begin with.[107] Even if the employee's action does not *actually* protect the e-mails (for example, if an employee deletes e-mails and defragments the computer but the employer is still able to retrieve the e-mails forensically), the protective action saves the privilege nonetheless. That is the point: employees who are wrong about a particular course of action's efficacy may still enjoy the privilege if that is the reason they engaged in the action to begin with. And the action need not be substantial—as long as the employee subjectively believes that the action will protect the e-mails, the action should save the privilege. (Whether that belief itself would be reasonable may serve as evidence of the employee's actual subjective belief.) Employees will therefore be no more discouraged by this rule than by the rule that communications are not privileged if not confidential.

The second compromise of this proposal is between extreme stances on the significance of certain factors. For example, while some courts hold that the use of a personal, password-protected account is irrelevant and others hold that it is dispositive,[108] under this proposal, it depends on the employee's state of mind.[109] Likewise, the significance of deleting e-mails to protect them from retrieval, for example, depends not on whether judges feel the behavior gives rise to a reasonable expectation of privacy, but rather on whether the privilege survived the monitoring moment to begin with.[110]

For that reason, this proposal also makes outcomes more predictable. The reasonableness test has led to a wide variety of results and is malleable enough for judges to make decisions based on desired outcomes. This test, however, is simpler: the company policy either applies or does not, and the employee either takes protective

---

[107] *Cf. Henry Ford Quotes*, BRAINYQUOTE.COM, http://www.brainyquote.com/quotes/quotes/h/henryford122817.html (last visited Mar. 27, 2013) ("If you think you can do a thing or think you can't do a thing, you're right.").

[108] *See supra* Part II.C.4 (explaining courts' views on the significance of personal, password-protected accounts).

[109] *See supra* Part III.B.2 (declaring that the employee's motivation for using a personal account is dispositive).

[110] *See supra* note 102. Deleting e-mails is one example of a later protective action that would become dispositive.

actions or does not. This will also make judges' jobs easier. Rather than deciding what is reasonable in this modern, technological world,[111] judges would just have to answer these two questions: (1) Does the company policy apply? (2) If so, did the employee take the necessary protective action(s)?

D. *Objections*

One who believes that this proposal reins in the privilege too much might argue that it is unfair for employees who travel a lot or spend long hours at their workplaces.[112] But for employees who believe that taking some action such as deleting the e-mails from the laptop would protect confidentiality: that is all that would be necessary to save the privilege from waiver. Traveling employees would therefore be even better off than their non-traveling counterparts because the travelers would not have to worry about protecting the communications from monitoring.[113]

By contrast, employees who know such measures would not work would not even have a subjective belief in confidentiality. Thus, the privilege could not apply. Perhaps, then, there should be a bright-line rule that the privilege always applies to communications between traveling employees and their attorneys. But that would not take into account the concern of admitting relevant evidence.[114]

---

[111] *See* Losey, *supra* note 10, at 1201–02, 1203–04 (recommending the use of experts to help determine what beliefs are objectively reasonable because "few judges have significant experience with technology, and some appear to personally identify with technologically unsophisticated employees").

[112] *See* Nat'l Econ. Research Assocs. v. Evans, 04-2618BLS2, 2006 Mass. Super. LEXIS 371, at *12 (Mass. Super. Aug. 3, 2006) (warning that if the privilege did not apply, traveling employees would find it difficult to communicate with their attorneys confidentially because the e-mails would be saved on the company laptop); ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 459 (2011) ("Third parties may have access to attorney-client e-mails when the client receives or sends e-mails via a . . . hotel computer . . ."); 1 PAUL R. RICE, ATTORNEY-CLIENT PRIVILEGE IN THE UNITED STATES § 6:8 (2011 ed.) (also raising the issue of urgent legal matters that require constant communication with attorneys even when employees are at work).

[113] *See supra* note 102.

[114] *See supra* Part III.C (showing how this Note's proposal would satisfy both the concern of admitting evidence and that of encouraging attorney-client communications); *see also* Losey, *supra* note 10, at 1203 ("An attempt to produce clarity through the imposition of a forced bright-line test would cause unnecessary rigidity.").

One who believes that this proposal would exclude too much relevant evidence might argue that because the computers are employer-owned, the employers can confiscate them at any time, and therefore employee e-mails are subject to retrieval before employees take protective actions.[115] That would mean the e-mails are never truly confidential even if employees protected them from monitoring. It is often the case, however, that owners who give up some property rights may have to give up others.[116] Because employers are allowing employees to use the computers, they should also have to allow employees to attempt to protect e-mails or other documents or files from retrieval.[117]

IV. CONCLUSION

A. *Summary of the Proposal*

Courts have approached the problem of whether the attorney-client privilege applies to an employee who uses an employer's computer for e-mail by determining whether the employee's belief in the confidentiality of the communications was objectively reasonable. But courts vary widely as to what circumstances give rise to a reasonable belief. Rather than focusing exclusively on reasonableness, courts should instead apply a two-part test. First, does the company policy clearly allow the employer to view employee e-mails through monitoring or retrieval? If not, the communications should be privileged. If so, there should be a presumption that they are not privileged. If there is such a presumption, then the second part of the test is: did the employee engage in protective behavior at all relevant

---

[115] For examples of company policies that seem to allow such behavior, see *supra* note 51.

[116] *See, e.g.*, Marsh v. Alabama, 326 U.S. 501, 506 (U.S. 1946) ("Ownership does not always mean absolute dominion. The more an owner, for his advantage, opens up his property for use by the public in general, the more do his rights become circumscribed by the statutory and constitutional rights of those who use it."); State v. Shack, 277 A.2d 369, 371–72 (N.J. 1971) (holding that a farmer could not "bar access to governmental services available to migrant workers" and averring that "[t]itle to real property cannot include dominion over the destiny of persons the owner permits to come upon the premises").

[117] *Cf.* RICE, *supra* note 112, at § 6:8 (suggesting that cases such as *Asia Global*, *Evans*, and *Sims* "may be part of a larger body of decisional law that will set limits on the types of employee privacy expectations that employers cannot unilaterally make unreasonable because of societal expectations . . . ").

times—before the e-mails can be monitored and before they are retrieved, as applicable? If so, the privilege should apply. If not, it should be held waived. This approach would lead to compromise in policy concerns and in extreme stances on certain circumstances, and to greater predictability of results.

B. *Significance of ABA Formal Opinion 11-459*

In August 2011, the ABA released a formal opinion entitled "Duty to Protect the Confidentiality of E-mail Communications with One's Client."[118] Some commentators had recommended such a measure.[119] Significantly, the opinion leaves the applicability of the attorney-client privilege as an open question.[120] Also, the opinion provides another way for employees to earn the privilege under this Note's proposal: if employees check with their attorneys prior to communicating via e-mail on employers' computers, attorneys should warn them about the risks and encourage them to seek other means of communication. If an attorney fails to give such a warning and the employee communicates using the employer's computer, the act of consulting the attorney should nevertheless count as earning the privilege. The opinion also makes die-hard protection of the privilege in these cases less necessary: attorneys' warnings may provide protection enough. Finally, the opinion is evidence of a changing world.[121]

---

[118] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 459 (2011).

[119] *See* Dion Messer, *To: Client@Workplace.com: Privilege at Risk?*, 23 J. MARSHALL J. COMPUTER & INFO. L. 75, 97–98 (2004) (presenting the option of the ABA issuing a requirement that attorneys warn clients of the risks inherent in workplace e-mails); Williams, *supra* note 82, at 387–89 (recommending the issuance of an ABA opinion requiring extra precaution by attorneys regarding workplace e-mails in order to "provide enhanced protection to the attorney-client privilege in a relatively easy and cost-effective manner").

[120] *See* ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 459 (2011) ("This Committee's mission does not extend to interpreting the substantive law, and therefore we express no view on whether, and in what circumstances, an employee's communications with counsel from the employee's workplace device or system are protected by the attorney-client privilege.").

[121] *See* ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 413 (1999) ("A lawyer may transmit information relating to the representation of a client by unencrypted e-mail sent over the Internet without violating the Model Rules of Professional Conduct (1998) because the mode of transmission affords a reasonable expectation of privacy from a technological and legal standpoint.").

C. *Limitation of the Proposal with Respect to the Future*

This analysis stems partly from a misunderstanding of technology. As the public's understanding grows, analyses must grow with it. Indeed, the cases explained above are "only the tip of the iceberg" in this "rapidly changing world."[122] Because of that, judges, attorneys, and the public alike should pay attention to developments in this and similar areas of the law.

---

[122] Anthony P. Schoenberg, *Attorney-Client Communications Sent over Employer E-mail Systems May Not Be Privileged*, 3 Privacy & Data Security L. J., 369, 374 (2008); *accord* City of Ontario v. Quon, 130 S. Ct. 2619, 2629 (2010) ("Rapid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior.").