Northwestern Journal of Technology and Intellectual Property

Volume 9 | Issue 8 Article 3

Summer 2011

Gone but Not Forgotten: When Privacy, Policy and Privilege Collide

Louise L. Hill
Professor, Widener University School of Law

N O R T H W E S T E R N
JOURNAL OF TECHNOLOGY
AND
INTELLECTUAL PROPERTY

Gone but Not Forgotten: When Privacy, Policy and Privilege Collide

Louise L. Hill

Summer 2011 VOL. 9, NO. 8

Northwestern Journal of Technology and Intellectual Property
Volume 9, Number 8 (September 2011)

Gone but Not Forgotten: When Privacy, Policy and Privilege Collide

By Louise L. Hill*

I. INTRODUCTION

¶1 Emerging technology has brought new methods for transmitting communications. Concomitant with this, the use of computers, the Internet, e-mail, and other electronic communication devices has been embraced in the workplace and in private settings.[1] As these tools for communicating information become part of everyday life, issues associated with their use continue to evolve, many of which relate to confidentiality and privilege. With respect to the workplace itself, most businesses have established policies that relate to Internet use and electronic communications, although "occasional, personal use of the Internet is commonplace."[2] An issue that has arisen of late relates to information that employers retrieve from the computers that their employees use and the effect this has on employee communications that otherwise would be shielded by the attorney-client privilege.

¶2 The jurisdictions are divided about whether employees give up the protection of attorney-client privilege when they use a company-issued computer to send or receive e-mails. Distinguishing factors, such as the type of e-mail system used, the company policy that is in place, and notice and enforcement of the policy, are among the things considered when the courts evaluate the issue. This Article begins by examining the law of confidentiality and privilege and addressing the matter of privacy in the workplace. It then examines divergent positions that courts have taken on the issue of computer use in the workplace, attorney-client privilege, and work product protection, as well as the impact of these holdings. This Article concludes by positing a position which relates to privacy in the workplace, balancing an employee's reasonable expectation of privacy with public policy concerns and lawyer responsibility.

II. ATTORNEY-CLIENT PRIVILEGE AND CONFIDENTIALITY

¶3 Attorney-client privilege is a rule of evidence, applicable in civil and criminal court proceedings, that "limits the extent to which a party in litigation can force from an unwilling witness a statement or document that is protected as confidential."[3] It is "based on a pragmatic judgment that confidentiality is necessary in order to encourage client

* Professor of Law, School of Law, Widener University.
[1] *See* Stengart v. Loving Care Agency, Inc., 990 A.2d 650, 654 (N.J. 2010).
[2] *Id.* at 655.
[3] Charles W. Wolfram, *The U.S. Law of Client Confidentiality: Framework for an International Perspective*, 15 FORDHAM INT'L L.J. 529, 541–42 (1992).

communication."[4] Such open consultation with lawyers is acknowledged "as providing a significant benefit to society."[5] However, while these attributes are recognized, the privilege is also viewed as "an obstacle to the investigation of the truth," which "ought to be strictly confined within the narrowest possible limits consistent with the logic of its principle."[6]

¶4 Each state in the United States has its own privilege rules, which generally follow the common law doctrine, while Rule 501 of the Federal Rules of Evidence governs federal courts.[7] Rather than establishing fixed rules for attorney-client privilege, the Supreme Court determined that Rule 501 allows privilege issues to be decided on a case-by-case basis.[8] The federal common law of privilege applies when the substantive rights of the parties are determined by federal law, while state privilege law applies if the underlying matter is governed by state law.[9]

¶5 As a general premise, attorney-client privilege attaches to confidential communications made between lawyer and client for the purpose of obtaining or providing legal assistance.[10] "Under federal law, '[a] client has a privilege to refuse to disclose and to prevent any other person from disclosing confidential communications made for the purpose of facilitating the rendition of professional legal services to the client,' between the client and the client's lawyer . . . ."[11] In general, "[a] communication is confidential when the circumstances indicate that it was not intended to be disclosed to third persons other than (1) those to whom disclosure is in furtherance of the rendition of legal services to the client, or (2) those reasonably necessary for the transmission of the

[4] *Id.* at 544. The privilege has been traced to Roman times when attorneys were servants of those whose affairs they managed and, under Roman law, could not testify for or against their masters because the relationship created a duty of loyalty. *See* Max Radin, *The Privilege of Confidential Communication Between Lawyer and Client*, 16 CAL. L. REV. 487, 487–88 (1928).

[5] J. Triplett Mackintosh & Kristen M. Angus, *Conflict in Confidentiality: How E.U. Laws Leave In-House Counsel Outside the Privilege*, 38 INT'L LAW. 35, 38 (2004).

[6] 8 JOHN HENRY WIGMORE ET AL., EVIDENCE IN TRIALS AT COMMON LAW § 2291, at 554 (4th ed., rev. 1961).

[7] *See* Daiske Yoshida, *The Applicability of the Attorney-Client Privilege to Communications with Foreign Legal Professionals*, 66 FORDHAM L. REV. 209, 212–13 (1997).

[8] Upjohn Co. v. United States, 449 U.S. 383, 396 (1981). The Supreme Court acknowledged that this approach could "undermine desirable certainty in the boundaries of the attorney-client privilege." *Id.* at 396–97. Some feel this has resulted in confusion and inconsistencies, creating "practical difficulties for attorneys and other legal advisors." Yoshida, *supra* note 7, at 214.

[9] FED. R. EVID. 501 ("Except as otherwise required by the Constitution of the United States or provided by Act of Congress or in rules prescribed by the Supreme Court pursuant to statutory authority, the privilege of a witness, person, government, State, or political subdivision thereof shall be governed by the principles of the common law as they may be interpreted by the courts of the United States in the light of reason and experience. However, in civil actions and proceedings, with respect to an element of a claim or defense as to which State law supplies the rule of decision, the privilege of a witness, person, government, State, or political subdivision thereof shall be determined in accordance with State law.").

[10] *See* Wolfram, *supra* note 3, at 542.

[11] *In re* Asia Global Crossing, Ltd., 322 B.R. 247, 255 (Bankr. S.D.N.Y. 2005) (quoting SUP. CT. STANDARD 503). Proposed Rule 503 was not adopted as part of the Federal Rules of Evidence but was "promulgated by the Supreme Court of the United States, and . . . 'should be regarded as an authoritative source of the principles of [federal] common law.'" *Id.* at 255 n.6 (quoting BARRY RUSSELL, BANKRUPTCY EVIDENCE MANUAL § 501.2, at 798 (2004)).

communication."[12] There is both a subjective and objective component to confidentiality. The client must intend to give the communication in confidence and must reasonably understand it to have been so given.[13]

A. Waiver of Attorney-Client Privilege

¶6 Attorney-client privilege can be waived; waiver is absolute and "construed broadly against the party claiming the privilege."[14] Waiver of attorney-client privilege can result from intentional voluntary disclosure as well as from inadvertent disclosure.[15] "The client, not counsel, can voluntarily waive the privilege."[16] If a client willingly shares a privileged communication with someone who is non-privileged, "a court will feel free to find that, in this instance, the assurance of confidentiality was not important to the client,

---

[12] *Id.* at 255 (quoting 3 HON. JACK B. WEINSTEIN & MARGARET A. BERGER, WEINSTEIN'S FEDERAL EVIDENCE § 503.15 at 503–57 (Joseph M. McLaughlin ed., 2d ed. 1997)).

[13] *See, e.g.*, Bogle v. McClure, 332 F.3d 1347, 1358 (11th Cir. 2003) (holding that a "privilege holder must prove the communication was '(1) intended to remain confidential *and* (2) . . . was *reasonably* expected and understood to be confidential'").

United States v. Bell, 776 F.2d 965, 971 (11th Cir. 1985)); United States v. Melvin, 650 F.2d 641, 645 (5th Cir. 1981) (holding that "[a] communication is protected . . . if it is intended to remain confidential and . . . was reasonably expected and understood to be confidential").

[14] Mackintosh & Angus, *supra* note 5, at 43.

[15] Wolfram, *supra* note 3, at 544. Waiver can also result from the offensive use of what would otherwise be privileged communications. The offensive use doctrine comes into play when a party to a proceeding introduces an issue related to advice received from a lawyer, impliedly waiving the confidentiality of the communication. *See* Mackintosh & Angus, *supra* note 5, at 43 n.57 (citing Chevron Corp. v. Pennzoil Co., 974 F.2d 1156 (9th Cir. 1992)). Over the years, courts have differed on the application of this doctrine. *See* Louise L. Hill, *Emerging Technology and Client Confidentiality: How Changing Technology Brings Ethical Dilemmas*, 16 B.U. J. SCI. & TECH. L. 1, 11–12 (2010). Some courts find the privilege waived if protected information is integral to the outcome of issues in the lawsuit. *See, e.g.*, Mortg. Guarantee & Title Co. v. Cunha, 745 A.2d 156, 159 (R.I. 2000). Some courts require the privileged material to be "outcome determinative" for there to be waiver. *See, e.g.*, Republic Ins. Co. v. Davis, 856 S.W.2d 158, 163 (Tex. 1993). Still other courts have determined that waiver should be found when assertion of the privilege is the result of a party's affirmative act. *See, e.g.*, Hearn v. Rhay, 68 F.R.D. 574, 581 (E.D. Wash. 1975) ("[T]he asserting party put the protected information at issue by making it relevant to the case; and [] application of the privilege would . . . den[y] the opposing party access to information vital to his defense."). In 2008, the Second Circuit invoked the remedy of mandamus to clarify the uncertainty surrounding "at issue" waivers. *In re* County of Erie, 546 F.3d 222, 224, 226 (2d Cir. 2008). An assertion that information is relevant is not enough for there to be waiver. Rather, for there to be waiver "a party must *rely* on privileged advice from his counsel to make his claim or defense." *Id*. at 229.

> The attorney-client privilege does not apply to a communication occurring when a client:
>
> (a) consults a lawyer for the purpose, later accomplished, of obtaining assistance to engage in a crime or fraud or aiding a third person to do so, or
>
> (b) regardless of the client's purpose at the time of consultation, uses the lawyer's advice or other services to engage in or assist a crime or fraud.

RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS § 82 (2000). Known as the crime-fraud exception, work product immunity for a client is also barred if the client used the attorney's assistance to perpetrate a crime or fraud. *See In re* Green Grand Jury Proceedings, 492 F.3d 976, 980 (8th Cir. 2007).

[16] Mackintosh & Angus, *supra* note 5, at 42–43.

and that the general policy of free access by adversaries to all relevant evidence should prevail."[17]

¶7 Opinion differs on whether attorney-client privilege is waived when there is inadvertent disclosure. Usually, when approaching the issue of inadvertent disclosure, one of three tests is applied: (1) the "strict responsibility test," under which any disclosure, even inadvertent disclosure, waives attorney-client privilege;[18] (2) the "subjective intent test," under which inadvertent disclosure does not waive attorney-client privilege since waiver requires an intention to waive;[19] and (3) the "balancing test," under which waiver is determined by an evaluation of the circumstances.[20] The most popular of the three tests is the balancing test, under which courts generally determine waiver by considering the reasonableness of precautions taken to prevent disclosure, the time taken to recognize the error, the scope of the production, the extent of the disclosure, and considerations of fairness and justice.[21]

¶8 Recent amendments to the Federal Rules of Evidence attempt to resolve the conflicting decisions about the effect of inadvertent disclosure in federal court litigation. Rule 502(b) essentially provides that disclosure of privileged material does not result in the waiver of attorney-client privilege, as long as: "(1) the disclosure is inadvertent; (2) the [party responsible for the disclosure] took reasonable steps to prevent disclosure; and (3) the [party responsible for the disclosure] promptly took reasonable steps to rectify the error" after it occurred.[22] The new rule also attempts to resolve the dispute about whether

---

[17] Wolfram, *supra* note 3, at 544. In litigation, it is generally felt that parties with allied interests should be able to communicate and coordinate their positions in order to more effectively present their claims. Therefore, two or more parties with a common interest that "is the subject of confidential communications generally are allowed to share this information with each other without losing the attorney-client privilege." Joan C. Rogers, *Confidentiality of Corporate Information May Be Waived or Lost in Many Ways*, 16 Laws. Man. on Prof. Conduct (ABA/BNA) 376 (July 19, 2000).

[18] The strict responsibility test is the traditional test, which puts the "risk of insufficient precautions []on the client." WIGMORE ET AL., *supra* note 6, § 2325(3), at 633. The rationale for the strict view is that privilege acts as an obstacle to discovery of the truth; disclosure of privileged materials makes it impossible to achieve the benefits of privilege; therefore, "when the policy underlying the rule can no longer be served, it would amount to no more than mechanical obedience to a formula to continue to recognize it." Vincent S. Walkowiak, Sarah E. Lemons & Thomas J. Leach, *Loss of Attorney-Client Privilege Through Inadvertent Disclosure of Privileged Documents*, *in* ATTORNEY-CLIENT PRIVILEGE IN CIVIL LITIGATION: PROTECTING AND DEFENDING CONFIDENTIALITY 313, 316 (Vincent S. Walkowiak ed., 3d ed. 2004) [hereinafter ATTORNEY-CLIENT PRIVILEGE] (quoting United States v. Kelsey-Hayes Wheel Co., 15 F.R.D. 461, 465 (E.D. Mich. 1954)) (internal quotation marks omitted).

[19] The subjective intent test is the most lenient approach, the rationale of which is "that 'inadvertent production is the antithesis' of an intentional relinquishment of a known right and, if privilege is for the welfare of the *client*, more than the *attorney's* negligence should be required before the *client* loses the privilege." Walkowiak, Lemons & Leach, *supra* note 18, at 318 (quoting Mendenhall v. Barber-Greene Co., 531 F. Supp. 951, 955 (N.D. Ill. 1982)).

[20] *See* Mackintosh & Angus, *supra* note 5, at 43 n.58; Rogers, *supra* note 17.

[21] *See* Mackintosh & Angus, *supra* note 5, at 43 n.58. Although routinely presented as a multi-factor test, it has been asserted that courts primarily concentrate on only "two considerations—the conduct of the client and lawyer claiming the privilege, and the prejudice to the party to whom the privileged material was disclosed should the court uphold the privilege despite disclosure." Walkowiak, Lemons & Leach, *supra* note 18, at 321.

[22] FED. R. EVID. 502(b). The Advisory Committee on Evidence Rules noted the following with respect to the amendment:

> The rule establishes a compromise between two competing premises. On the one hand,

waiver attaches only to those documents or communications that are inadvertently disclosed, or whether it extends to all communications on the subject covered by the inadvertently disclosed communications. The rule takes the position held by the majority of courts, which is that any waiver resulting from inadvertent disclosure is generally limited to the material which is actually disclosed.[23] Additionally, the rule provides that a disclosure first made in state court does not waive the privilege in federal court proceedings (unless the disclosure would be a waiver in a federal court proceeding or under the law of the state where the disclosure occurred),[24] and a federal court order that privilege is not waived extends the protection to other federal and state court proceedings.[25]

B. Work-Product Immunity

¶9 Along with the attorney-client privilege, the law of confidentiality in the United States recognizes the doctrine of work-product immunity, which protects material from discovery that a lawyer generates in preparing a matter for litigation.[26] It is a qualified privilege that "shelters the mental processes of the attorney, providing a privileged area within which he can analyze and prepare his client's case."[27] Unlike attorney-client privilege, work-product immunity does not turn on the expectation or intent that a communication remain confidential. A lawyer can disclose work product to persons not assisting the lawyer in trial preparation without losing immunity status, as long as "the disclosure does not create a substantial risk of divulgence to an adversary in litigation."[28] However, like attorney-client privilege, work-product protection, which can be either "ordinary work product" or "opinion work product," can be waived.[29]

> information covered by the attorney-client privilege or work product protection should not be treated lightly. On the other hand, a rule imposing strict liability for an inadvertent disclosure threatens to impose prohibitive costs for privilege review and retention, especially in cases involving electronic discovery.

Report of the Advisory Committee on Evidence Rules, Committee on Rules of Practice and Procedure of the Judicial Conference of the United States, Committee Note on Subdivision (b), at 11 (June 30, 2006), *available at* http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/Excerpt_EV_Report_Pub.pdf.

[23] FED. R. EVID. 502(a) (Waiver extends to all related material on the same subject "only if: (1) the waiver is intentional; (2) the disclosed and undisclosed communications or information concern the same subject matter; and (3) they ought in fairness to be considered together.").

[24] *Id.* 501(c).

[25] *Id.* 501(d).

[26] *See* Wolfram, *supra* note 3, at 542–43. Protected material must be prepared in anticipation of litigation, which must be more than a "remote prospect," but need not necessarily be imminent. *In re* Special September 1978 Grand Jury (II), 640 F.2d 49, 64, 64 n.19 (7th Cir. 1980).

[27] United States v. Nobles, 422 U.S. 225, 238 (1975). *See also* FED. R. CIV. P. 26(b)(3) (2006) (repealed 2007) ("[A] party may obtain discovery of documents and tangible things otherwise discoverable . . . and prepared in anticipation of litigation or for trial by or for another party or by or for that other party's representative . . . only upon a showing that the party seeking discovery has substantial need of the materials in the preparation of the party's case and that the party is unable without undue hardship to obtain the substantial equivalent of the materials by other means. In ordering discovery of such materials when the required showing has been made, the court shall protect against disclosure of the mental impressions, conclusions, opinions, or legal theories of an attorney or other representative of a party concerning the litigation.").

[28] Wolfram, *supra* note 3, at 543–44.

[29] *See In re* Green Grand Jury Proceedings, 492 F.3d 976, 980 (8th Cir. 2007).

¶10 Ordinary work product consists of raw factual information, while opinion work product consists of mental impressions, conclusions, opinions or legal theories.[30] Since the work-product doctrine protects the attorney's materials, the attorney may waive the benefit of the privilege.[31] The client can waive the privilege as to ordinary work product, while the attorney may contest the waiver as to opinion work product.[32] There are some situations in which work-product protection can be overcome by an opposing party, such as when the opposing party demonstrates a substantial need for the work-product materials.[33] However, with respect to opinion work product, this type of material "is discoverable, if at all, only upon a showing of compelling need."[34]

C. Ethical Obligations Relating to Confidentiality

¶11 The law of confidentiality in the United States is also composed of an ethical obligation to maintain client confidences. This ethical duty is "not limited to judicial or other proceedings, but rather appl[ies] in all representational contexts,"[35] covering all information relating to the representation, not just client communications.[36] The American Bar Association Model Rules of Professional Conduct (Model Rules), on which the states' professional conduct rules are based,[37] call for information relating to

---

[30] *Id.*

[31] *See* Carte Blanche (Singapore) PTE., Ltd. v. Diners Club Int'l, Inc., 130 F.R.D. 28, 32 (S.D.N.Y. 1990).

[32] *See* Buck v. Aetna Life & Cas. Co., No. 91-2832, 1992 WL 130024, at *2 (E.D. Pa. June 5, 1992). A lawyer's independent work-product privilege is considered as a separate matter. *See infra* note 34.

[33] FED. R. CIV. P. 26(b)(3), provides:

> Trial Preparation: Materials.
>
> Documents and Tangible Things. Ordinarily, a party may not discover documents and tangible things that are prepared in anticipation of litigation or for trial by or for another party or its representative (including the other party's attorney, consultant, surety, indemnitor, insurer, or agent). But, subject to Rule 26(b)(4), those materials may be discovered if:
>
> they are otherwise discoverable under Rule 26(b)(1); and
>
> the party shows that it has substantial need for the materials to prepare its case and cannot, without undue hardship, obtain their substantial equivalent by other means.
>
> Protection Against Disclosure. If the court orders discovery of those materials, it must protect against disclosure of the mental impressions, conclusions, opinions, or legal theories of a party's attorney or other representative concerning the litigation.

[34] Rogers, *supra* note 17. As with attorney-client privilege, work-product protection may also be lost by a showing of a crime or fraud. *See supra* note 15 and accompanying text. However, since a lawyer's independent work-product privilege is considered a separate matter, a lawyer may assert the work-product doctrine with regard to opinion work product even if the client has used the lawyer's services for criminal or fraudulent purposes, provided the lawyer was unaware that the client was doing so. *See In re Green Grand Jury Proceedings*, 492 F.3d at 981 ("[W]e hold, as have our sister circuits, that an attorney who is not complicit in his client's wrongdoing may assert the work product privilege with respect to his opinion work product.").

[35] Arthur Garwin, *Confidentiality and Its Relationship to the Attorney-Client Privilege*, *in* ATTORNEY-CLIENT PRIVILEGE, *supra* note 18, at 31, 31.

[36] *See* MODEL RULES OF PROF'L CONDUCT R. 1.6 (2009).

[37] California remains the only state that has legal ethics rules that do not comport with the ABA Model Rule format. *Model Rules: Maine's Shift to Model Rules Allows MJP, Preserves Unique Aspects of Former Code*, 25 Laws. Man. on Prof. Conduct (ABA/BNA) 135 (Mar. 18, 2009). While most states in the United States have adopted the Model Rules, lawyers are not provided with a uniform standard since interpretational differences exist among the jurisdictions, as do differences in the text of some of the rules.

the representation of a client to be held in confidence.[38] Found at Model Rule 1.6, this obligation attaches irrespective of the source of the information,[39] with only limited exceptions.[40] Breach of the obligation of confidentiality can subject a lawyer to professional discipline.[41] Occasionally, although not pursuant to the Model Rules, a client can obtain damage recovery if a lawyer unjustifiably divulges confidential information that results in the client being harmed.[42]

¶12 Due to the proliferation of electronic communications and the increase of their inadvertent transmission, the matter of dissemination of inadvertent communications is also addressed by the Model Rules.[43] To that end, Model Rule 4.4(b) specifically provides:

> A lawyer who receives a document relating to the representation of the lawyer's client and knows or reasonably should know that the document was inadvertently sent shall promptly notify the sender.[44]

¶13 Such notification enables the sender to take protective measures. However, the commentary to the rule specifically notes that additional steps to be taken by the lawyer,

---

See Louise L. Hill, *Electronic Communications and the 2002 Revisions to the Model Rules*, 16 ST. JOHN'S J. LEGAL COMMENT. 529, 531 (2002).

[38] Model Rule 1.6, which addresses confidentiality of information, provides:

> A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).

MODEL RULES OF PROF'L CONDUCT R. 1.6(a) (2009).

[39] *See* RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS § 59 cmt. b (2000).

[40] The Model Rule exceptions to the general prohibition against disclosure of client information are permissive rather than mandatory. Pursuant to Model Rule 1.6, lawyers are permitted to:

> reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary:
>
> (1) to prevent reasonably certain death or substantial bodily harm;
>
> (2) to prevent the client from committing a crime or fraud that is reasonably certain to result in substantial injury to the financial interests or property of another and in furtherance of which the client has used or is using the lawyer's services;
>
> (3) to prevent, mitigate or rectify substantial injury to the financial interests or property of another that is reasonably certain to result or has resulted from the client's commission of a crime or fraud in furtherance of which the client has used the lawyer's services;
>
> (4) to secure legal advice about the lawyer's compliance with these Rules;
>
> (5) to establish a claim or defense on behalf of the lawyer in a controversy between the lawyer and the client, to establish a defense to a criminal charge or civil claim against the lawyer based upon conduct in which the client was involved, or to respond to allegations in any proceeding concerning the lawyer's representation of the client; or
>
> (6) to comply with other law or a court order.

MODEL RULES OF PROF'L CONDUCT R. 1.6(b) (2009).

[41] *See* Wolfram, *supra* note 3, at 545.

[42] *Id.*

[43] *See* Hill, *supra* note 15, at 21–22. "Because of the ease of electronic transmission and the volume of material being exchanged, it has not been unusual for a document, or material embedded in a document, to be inadvertently transmitted." *Id.* at 45. This is particularly prevalent during electronic discovery within the context of civil litigation. *Id.*

[44] MODEL RULES OF PROF'L CONDUCT R. 4.4(b) (2009).

such as returning the document, as well as whether the privileged status of the document has been waived, are beyond the scope of the rule.[45]

III. EXPECTATION OF PRIVACY

¶14 A right to privacy is recognized under both the common law and the Fourth Amendment to the United States Constitution, and in each case, the expectation of privacy must be reasonable.[46] Just as with confidentiality, there are both subjective and objective components to the expectation of privacy.

> The Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated" . . . [and] guarantees the privacy, dignity, and security of persons against certain arbitrary and invasive acts by officers of the Government . . . .[47]

For Fourth Amendment purposes, a person must show "a subjective expectation of privacy . . . that society accepts as objectively reasonable."[48]

¶15 The concerns surrounding the reasonableness of a Fourth Amendment privacy claim are different from those that arise in the private employer setting.[49] In the latter situation, a person who asserts the tort of "intrusion upon seclusion" must show a subjective expectation of privacy which is objectively reasonable.[50] The tort typically provides that "[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person."[51] The standard employed is a strict one, calling for the establishment of an intrusion that "would be highly offensive to the ordinary reasonable man, as the result of conduct to which the reasonable man would strongly object."[52]

---

[45] *Id.* R. 4.4 cmt. 2.
[46] *See* Smith v. Maryland, 442 U.S. 735, 740 (1979) (holding that Fourth Amendment applicability depends on whether person can claim a justifiable, reasonable, or legitimate expectation of privacy that has been invaded); Kline v. Sec. Guards, Inc., 386 F.3d 246, 260 (3d Cir. 2004) (holding that plaintiff asserting cause of action for invasion of privacy must show "reasonable expectation of privacy").
[47] Skinner v. Ry. Labor Execs.' Ass'n,, 489 U.S. 602, 613–14 (1989).
[48] California v. Greenwood, 486 U.S. 35, 39 (1988).
[49] *See* United States v. Simons, 206 F.3d 392, 397–98 (4th Cir. 2000) (involving search warrant for CIA employee's computer on which pornographic images of minors were found); Stengart v. Loving Care Agency, Inc., 990 A.2d 650, 663 (N.J. 2010) (citing O'Connor v. Ortega, 480 U.S. 709, 714–19 (1987)) (discussing search of public hospital employee's workplace as a violation of the employee's expectation of privacy under Fourth Amendment); State v. M.A., 954 A.2d 503, 510–13 (N.J. Super. Ct. App. Div. 2008) (involving Fourth Amendment analysis of search of State Police employee's computer and subsequent theft charges).
[50] Med. Lab. Mgmt. Consultants v. Am. Broad. Cos., 306 F.3d 806, 812 (9th Cir. 2002).
[51] RESTATEMENT (SECOND) OF TORTS § 652B (1977).
[52] *Id.* § 652B cmt. d. This article is focusing on the private employment setting, rather than when the employer is a government entity.

A. Electronic Communications

¶16 No authority exists which suggests that privilege is unavailable simply because a lawyer and client communicate via Internet e-mail.[53] In fact, federal statutory prohibitions against intercepting these communications render them "sufficiently private to satisfy the conditions for the attorney-client privilege to apply."[54] Under the Federal Wiretap Act, intentional interception of wire or electronic communications is prohibited; furthermore, interception of these communications does not waive any otherwise available privilege.[55] As far as a lawyer's obligation to a client is concerned, lawyers are not required to use "all available technology to prevent interception" when communicating with clients.[56] Only steps that are reasonable under the circumstances are necessary.[57]

¶17 In 1999, an American Bar Association committee addressed the matter of mandatory encryption of e-mail, and concluded that a lawyer may communicate with clients via e-mail without using encryption.[58] The committee reasoned that the expectation of privacy for e-mail is the same as that for ordinary telephone calls,[59] and the unauthorized interception of an electronic message is illegal. It was noted, however, that unusual circumstances involving extraordinarily sensitive information might warrant enhanced security measures like encryption, just as ordinary telephones and other typical means of communication would be deemed inadequate to protect confidentiality in some situations.[60]

B. Electronic Communications in the Workplace & Company Policies

¶18 In many instances in the workplace, employees use computer equipment owned by the employer and send and receive e-mails over the company's e-mail system. This

---

[53] *See* David Hricik, *Confidentiality & Privilege in High-Tech Communications*, 60 TEX. B.J. 104, 116 (1997).

[54] *Confidentiality: Electronic Communications Practice Guide*, Laws. Man. on Prof. Conduct (ABA/BNA), 55:401 (1996).

[55] The Federal Wiretap Act provides that "[n]o otherwise privileged wire, oral, or electronic communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character." 18 U.S.C. § 2517(4) (2006) (citation omitted). The Act also forbids the disclosure or use of unlawfully intercepted communications and bars the introduction into evidence of unlawfully intercepted conversations. *Id.* § 2515. As amended by the Electronic Communications Privacy Act, e-mail is protected from interception by the Federal Wiretap Act in that it is an electronic communication. Electronic Communications Privacy Act of 1986, Pub. L. no. 99-508, § 101(a), 100 Stat. 1848, 1848–1849 (1986) (amending 18 U.S.C. § 2510).

[56] *Confidentiality: Electronic Communications Practice Guide*, *supra* note 54 (quoting C. MUELLER & L. KIRKPATRICK, MODERN EVIDENCE § 5.13, at 491–92 (1995)).

[57] *Id.*

[58] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 99-413 (1999).

[59] During most of the twentieth century, lawyers routinely used the telephone to communicate with clients. Even though telephone company employees could listen in on these land-line calls, which could also be intercepted by third parties, people had an expectation that these conversations would be private. *See Confidentiality: Electronic Communications Practice Guide*, *supra* note 54. This expectation of privacy is reflected in the Federal Wiretap Act, which prohibits intentional interception of wire or electronic communications, and provides that interception does not waive any otherwise available privilege. *See supra* note 55.

[60] Formal Op. 99-413, *supra* note 58.

equipment can also be used by employees to access a web-based personal e-mail account, the occasional use of which is considered common in the workplace.[61] It is recognized that employers have the right, if not the responsibility, to monitor workplace use of computers to prevent harm to the company. They can adopt and enforce "lawful policies relating to computer use to protect the assets, reputation, and productivity of a business and to ensure compliance with legitimate corporate policies."[62] However, it has been noted that "a policy that banned all personal computer use and 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."[63]

¶19 There are a variety of ways that an employer can access or monitor an employee's computer use. Some employers track time spent at the keyboard as well as keystrokes and content.[64] Others retain and review e-mail messages, or store and review employees' computer files.[65] When a computer is used, the hard disk makes a "'screen shot' of all it sees, which the computer then stores in a temporary file, including e-mails retrieved from a private password-protected e-mail account on the Internet."[66] These temporary files are not readily available to the average user, although a forensic computer expert can access and retrieve them.[67] Some employees are unaware that a record may exist of their Internet and e-mail use at work.[68]

¶20 Many company policies that address electronic communications state the company's rights with respect to access and review; that such communications are part of the company's business; and that they are not to be considered private or personal to any individual employee. Often, employees are asked to sign an acknowledgment that they are aware of the applicable communications policy. While company policies vary significantly, the proffered policy regarding electronic communications at issue in *Stengart v. Loving Care Agency, Inc.* is somewhat typical, providing in part:

> The company reserves and will exercise the right to review, audit, intercept, access, and disclose all matters on the company's media systems and services at any time, with or without notice.
>
> . . . .
>
> E-mail and voice mail messages, internet use and communication and computer files are considered part of the company's business and client records. Such communications are not to be considered private or personal to any individual employee.

---

[61] *See* Stengart v. Loving Care Agency, Inc., 990 A.2d 650, 655 (N.J. 2010).
[62] *Id.* at 665. Employers "may discipline employees and, when appropriate, terminate them, for violating proper workplace rules that are not inconsistent with a clear mandate of public policy." *Id.*
[63] *Id.*
[64] *See* Adam C. Losey, *Clicking Away Confidentiality: Workplace Waiver of Attorney-Client Privilege*, 60 FLA. L. REV. 1179, 1181 (2008).
[65] *Id.* As of 2006, eighty percent of employers regularly monitored Internet use by employees. *Id.*
[66] Nat'l Econ. Research Assocs., Inc. v. Evans, No. 04-2618-BLS2, 2006 WL 2440008, at *4 (Mass. Super. Ct. Aug. 3, 2006).
[67] *Id.*
[68] *See* Losey, *supra* note 64, at 1181.

> The principal purpose of electronic mail (*e-mail*) is for company business communications. Occasional personal use is permitted; however, the system should not be used to solicit for outside business ventures, charitable organizations, or for any political or religious purpose, unless authorized by the Director of Human Resources.[69]

The policy also prohibits certain uses of e-mail,[70] and states that "[a]buse of the electronic communications system may result in disciplinary action up to and including separation of employment."[71]

¶21 Depending on the underlying electronic communication policy of a company, it may be that use of a company computer diminishes the expectation of privacy that an employee reasonably may have. This may lead to a determination that a communication was not made in confidence, or that an electronic communication will lose its privileged character due to waiver.

C. Expectation of Privacy in the Workplace

¶22 An approach to evaluating an employee's claim of privacy in files stored on company computers is to examine the reasonableness of the employee's expectation. An employee's expectation of privacy in the workplace "may be reduced by virtue of actual office practices and procedures, or by legitimate regulation"; thus, a reasonable expectation of privacy must be decided on a case-by-case basis.[72] In making this determination with respect to an employee's computer files and e-mail, courts have considered: (1) whether the company maintains a policy banning personal use; (2) whether the company monitors the employee's computer or e-mail use; (3) whether third parties have a right of access to the computer or e-mails; and (4) whether the company notified the employee, or the employee was aware, of the use and monitoring policies.[73]

---

[69] Stengart v. Loving Care Agency, Inc., 990 A.2d 650, 657 (N.J. 2010).

[70] Specifically prohibited is "sending inappropriate sexual, discriminatory, or harassing messages, chain letters, '[m]essages in violation of government laws,' or messages relating to job searches, business activities unrelated to [the employer], or political activities." *Id.*

[71] *Id.*

[72] O'Connor v. Ortega, 480 U.S. 709, 717, 718 (1987).

[73] *See In re* Asia Global Crossing, Ltd., 322 B.R. 247, 257 (Bankr. S.D.N.Y. 2005). In *In re Asia Global Crossing*, the Bankruptcy Court recognized these considerations and, in terms of its analysis, assumed certain e-mails were privileged and were subjectively intended to be confidential. *Id.* at 257–58. The court then considered whether any attorney-client privilege was waived with respect to communications sent over an employer e-mail system without encryption, finding a determination could not be made without further development of the record relating to employer policy and monitoring. *Id.* at 261. However, any attorney-client privilege was waived with respect to e-mail communications between employees and their lawyers that had been copied to company counsel or forwarded to a company consultant. *Id.* at 261–62. *Compare* Muick v. Glenayre Elecs., 280 F.3d 741, 743 (7th Cir. 2002) (finding no reasonable expectation of privacy exists where the employer announces he can inspect workplace computers), United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000) (finding no reasonable expectation of privacy exists where the employer has a policy of auditing employees' computer use and the employee does not assert he was unaware of the policy), Thygeson v. U.S. Bancorp, No. CV-03-467-ST, 2004 WL 2066746, at *18–21 (D. Or. Sept. 15, 2004) (finding no reasonable expectation of privacy exists where an employee handbook warns that the employer has the right to monitor files and e-mail), Kelleher v. City of Reading, No. 01-3386, 2002 U.S. Dist. LEXIS 9408, at *24–25 (E.D. Pa. May 29, 2002) (finding no reasonable expectation of privacy in workplace e-mail exists where the employer's guidelines informs employees that there is no expectation of

The correlation between the objectively reasonable expectation of privacy and the objective reasonableness of the intent that a communication be given in confidence is a close one.[74] Accordingly, it has been held that "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."[75]

1. Company E-mail System v. Personal E-mail Account

¶23 While no factor alone is dispositive, focusing on an employer's communications policy, some courts have determined that employees have a lesser expectation of privacy when they communicate via a company e-mail system as compared to a personal web-based account.[76] In *Stengart*, in anticipation of discovery, the employer hired experts to create a forensic image of the company laptop's hard drive that Stengart had used, including temporary Internet files.[77] The experts accessed messages to and from Stengart's lawyer discussing the subject of a future lawsuit, for which she had used a personal password-protected e-mail account instead of her company e-mail address.[78] Focusing on the language of the company policy, the court found that Stengart had a "subjective expectation of privacy" in these messages that was also "objectively reasonable," since the policy did not address personal accounts or warn employees that the contents of personal account e-mails could be forensically retrieved.[79] Thus, the "[p]olicy created doubt about whether those e-mails [were] company or private property."[80]

¶24 In the 2006 Massachusetts case *National Economic Research Associates, Inc. v. Evans*, an employee used a company laptop computer to send and receive attorney-client communications by e-mail, using his personal password-protected Yahoo account.[81]

---

privacy), *and* Garrity v. John Hancock Mut. Life Ins. Co., No. CIV.A.00-12143-RWZ, 2002 WL 974676, at *1–2 (D. Mass. May 7, 2002) (finding no expectation of privacy exists where the employer periodically reminds employees that company e-mail policy prohibits certain uses, the e-mail system belongs to the company, and it could inspect e-mail usage, even though the employee created a password to limit access), *with* United States v. Slanina, 283 F.3d 670, 676–77 (5th Cir. 2002) (finding a reasonable expectation of privacy exists in password-protected computer files maintained in a locked office where the employer does not disseminate a policy preventing storage of personal information on work computers or inform employees that computer usage and Internet access would be monitored), Leventhal v. Knapek, 266 F.3d 64, 74 (2d Cir. 2001) (finding a reasonable expectation of privacy exists where the employer does not have a practice of routinely searching office computers and has not placed the employee on notice that he should not have an expectation of privacy in his office contents, and the employee has a private office and exclusive use of his workplace computer), *and* Haynes v. Office of the Attorney Gen., 298 F. Supp. 2d 1154, 1161–62 (D. Kan. 2003) (finding a reasonable expectation of privacy exists in private computer files where employees are allowed to use workplace computers for private purposes, advised that unauthorized access to user's e-mail is prohibited, and given passwords to prevent access by others, despite a computer screen warning that there should be no expectation of privacy).

[74] *See In re Asia Global Crossing*, 322 B.R. at 258–59.

[75] *Id.* at 259.

[76] *See Stengart*, 990 A.2d at 662. The court also noted "[t]he location of the company's computer may also be a relevant consideration." *Id.* at 663; *see also supra* note 73.

[77] *See Stengart*, 990 A.2d at 656.

[78] *Id.*

[79] *Id.* at 663.

[80] *Id.*

[81] No. 04-2618-BLS2, 2006 WL 2440008, at *1 (Mass. Super. Ct. Aug. 3, 2006).

These e-mails were automatically stored in a temporary Internet file on the computer's hard drive, and later forensically retrieved at the direction of the employer.[82] The company manual permitted personal use of e-mail, "provided such use results in personal time savings that can be (at least partially) applied toward work,"[83] but warned that computer resources were property of the company and that e-mails were not confidential and could be read during routine checks.[84] This notwithstanding, the Massachusetts court found the employee's expectation of privacy in e-mails with his attorney was reasonable, primarily since

> the Manual did not expressly declare, or even implicitly suggest, that NERA would monitor the content of e-mail communications made from an employee's personal e-mail account via the Internet whenever those communications were viewed on a NERA-issued computer. Nor did NERA warn its employees that the content of such Internet e-mail communications is stored on the hard disk of a NERA-issued computer and therefore capable of being read by NERA.[85]

The Massachusetts court also referenced the 1999 ABA formal opinion addressing unencrypted e-mail, noting that "lawyers have a reasonable expectation of privacy when communicating by e-mail maintained by an [on-line service provider]."[86]

¶25 In the 2007 New York case *Scott v. Beth Israel Medical Center, Inc.*, a physician used his employer's e-mail system to write several e-mails to his lawyer using his employee e-mail address and the hospital e-mail server.[87] The hospital's computer and communications policy stated that its system "should be used for business purposes only," that employees had "no personal privacy right in any material created, received, saved or sent," and that the employer "reserve[d] the right to access and disclose such material at any time without prior notice."[88] Recognizing the employer's right to regulate its workplace, including the usage of its computers, the New York court determined that the effect of the hospital's policy was "to have the employer looking over your shoulder each time you send an e-mail . . . [so that] the otherwise privileged communication between Dr. Scott and [his lawyer] would not have been made in confidence because of the [employer's] policy."[89] The "no personal use" policy, combined with a policy allowing employer monitoring, diminished any expectation of privacy for employees.[90]

¶26 Arguably, it is one thing when an employee uses company equipment and company accounts to communicate with counsel, having knowledge that a restrictive company policy is enforced. It is quite another thing when an employee uses company equipment and a personal account that is password protected. In the former case—both subjectively

---

[82] *Id.* At the instruction of the company's lawyer, these e-mails were not reviewed pending guidance from the court. *Id.* at *2.
[83] *Id.* at *3.
[84] *Id.* at *2.
[85] *Id.* at *3.
[86] *Id.* at *4 (quoting Formal Op. 99-413, *supra* note 58) (alteration in original) (internal quotation marks omitted).
[87] 847 N.Y.S.2d 436, 438 (N.Y. Sup. Ct. 2007).
[88] *Id.* at 439.
[89] *Id.* at 440.
[90] *Id.* at 443.

and objectively—it seems that the expectation of privacy should be diminished. Conversely, the expectation of privacy does not seem to be diminished in the latter case, especially if personal use of company equipment is tolerated.

2. Use of a Company Computer as Waiver of Attorney-Client Privilege

¶27 It is well settled that voluntary disclosure of communications protected by attorney-client privilege generally results in waiver of that privilege.[91] It can be argued that, depending on the nuances of a company policy, knowing and deliberate employee communications on a company computer are not confidential. Or, if they are confidential, it can be argued that such use is tantamount to a voluntary waiver of privilege. Alternatively, when addressing the issue of waiver, some courts have considered an employer's forensic access to employee personal computer files as a matter involving inadvertent disclosure.[92] However, one court noted that "[a]ssuming a communication is otherwise privileged, the use of the company's e-mail system does not, without more, destroy the privilege."[93] While mere use of a company's e-mail system may not destroy privilege, use of a company system, coupled with knowledge of a company policy that diminishes privacy, might.

¶28 In the 2006 case *Kaufman v. SunGard Investment Systems*, the issue of voluntary waiver arose when Kaufman exchanged e-mails with her lawyer from her company-owned computer, which were sent from and received on her employer's e-mail system.[94] She deleted some communications, but others remained on the company computers. The employer used a computer technician to recover and restore these communications, which Kaufman claimed were privileged.[95] The magistrate judge determined that all the communications were discoverable since the attorney-client privilege had been waived.[96] With respect to the communications that remained on the company computers, the reviewing court affirmed the magistrate judge's decision that Kaufman failed to take reasonable measures to ensure the confidentiality of the communications.[97] Because the court found that Kaufman's actions were "knowing and deliberate," the privilege was waived as a voluntary disclosure.[98] With respect to the e-mails Kaufman deleted, the

[91] *See supra* notes 15–17 and accompanying text.
[92] *See supra* notes 18–30 and accompanying text. When privilege is claimed on the grounds that a communication was made in confidence in the course of a lawyer-client relationship, the communication is presumed to have been made in confidence, and the party opposing the claim of privilege has the burden of proof to establish the non-confidentiality of that communication. *See, e.g.*, People v. Jiang, 33 Cal. Rptr. 3d 184, 202–03 (Cal. App. 2005). The burden then shifts, and the party opposing the claim of privilege must overcome this presumption and prove that the communications were not confidential. *Id.*
[93] *In re* Asia Global Crossing, Ltd., 322 B.R. 247, 251 (Bankr. S.D.N.Y. 2005). The court also referenced Formal Opinion 99-413 of the American Bar Association in its analysis. *Id.* at 256 (citing Formal Op. 99-413, *supra* note 58).
[94] No. 05-cv-1236 (JLL), 2006 WL 1307882, at *1 (D.N.J. May 10, 2006).
[95] *Id.*
[96] *Id.* at *2.
[97] *Id.* at *3.
[98] *Id.* Plaintiff moved for reconsideration, claiming the magistrate judge should have applied state privilege law to all claims asserted. *Id.* at *2. The court determined that state privilege law should govern and that the magistrate judge's "determination that Kaufman's knowing and voluntary disclosure of the e-mail at issue waived any privilege, accords with New Jersey law." *Id.* at *3. Under New Jersey law, "the attorney-client privilege is waived when a privilege holder 'without coercion and with knowledge of his right or

reviewing court also affirmed that she waived any privilege attached to those documents.[99] The court considered the company policy, which called for monitoring, claimed a property interest in all information, and stated that employees should not consider items created with company property private.[100] Kaufman's knowing use of the company network, coupled with knowledge of the company policy, amounted to waiver of any privilege that might attach.[101]

¶29 In the 2007 case *Banks v. Mario Industries of Virginia, Inc.*, waiver of privilege was also at issue.[102] Employee Cook created a document on his work computer, printed it, and sent it to his lawyer for purposes of seeking legal advice.[103] Cook subsequently deleted the document, but Mario's forensic computer expert retrieved the document from the computer's hard drive. Mario Industries permitted their employees to use their work computers for personal business; however, the employee handbook provided there was no expectation of privacy regarding company computers.[104] The Supreme Court of Virginia affirmed that the document should be admitted into evidence, stating that "the [attorney-client] privilege is waived where the communication takes place under circumstances such that persons outside the privilege can overhear what is said."[105]

¶30 The matter of inadvertent waiver was at issue in the 2006 case *Curto v. Medical World Communications, Inc.*, where a forensic consultant restored portions of personal computer files and e-mails that former employee Curto had deleted from her company laptops.[106] The company had a usage policy which prohibited personal use of computers, allowed their personnel to access and review all employee materials, and provided that "[e]mployees expressly waive any right of privacy in anything they create, store, send, or receive on the computer or through the Internet or any other computer network."[107] Employing a mechanism similar to the popular "balancing test,"[108] the New York magistrate called for the balancing of four relevant factors:

> [1] the reasonableness of the precautions taken by the producing party to prevent inadvert[e]nt disclosure of privileged documents; [2] the volume of discovery versus the extent of the specific disclosure [at] issue; [3] the length of time taken

---

privilege, made disclosure of any part of the privileged matter or consented to such a disclosure made by anyone.'" *Id.* (quoting N.J. STAT. ANN. § 2A:84A-29 (West, Westlaw through 2011 legislation)).

[99] *Id.* at *4.

[100] *Id.* ("SunGard [policy] warned: The Company has the right to access and inspect all electronic systems and physical property belonging to it. Employees should not expect that any items created with, stored on, or stored within Company property will remain private. This includes desk drawers, even if protected with a lock; and computer files and electronic mail, even if protected with a password.").

[101] *Id.* The federal district court also affirmed the magistrate judge's ruling that, in light of the company policy, Kaufman had no reasonable expectation of privacy as to the communications at issue. *Id.*

[102] 650 S.E.2d 687 (Va. 2007).

[103] *Id.* at 695.

[104] *Id.* The employee handbook prohibited "the unauthorized removal of files from the computer and information systems, removing or copying Mario's documents, removing company property, and personal use of Mario's computer and information systems that was detrimental to Mario." *Id.* at 690.

[105] *Id.* at 695–96 (alteration in original) (quoting Clagett v. Commonwealth, 472 S.E.2d 263, 270 (Va. 1996)) (internal quotation marks omitted).

[106] No. 03CV6327, 2006 WL 1318387, at *1 (E.D.N.Y. May 15, 2006).

[107] *Id.*

[108] *See supra* note 21 and accompanying text.

> by the producing party to rectify the disclosure; and [4] the overarching issue of fairness.[109]

¶31 Added to these four factors was a fifth "subfactor" to be considered, "whether or not there was enforcement of [any computer usage] policy,"[110] which the reviewing court found to be "a 'subset' of the first factor [relating to] the reasonableness of precautions taken."[111] The magistrate noted that lack of enforcement of a computer usage policy "created a 'false sense of security' which 'lull[ed]' employees into believing that the policy would not be enforced."[112] The magistrate determined, and the reviewing court affirmed, that Curto had not waived her right to assert the attorney-client privilege and work-product protection.[113] Regarding precautions taken, Curto sent e-mails via "her personal AOL account which did not go through [the company's] servers and she attempted to delete the material before turning in her laptops."[114] Regarding the volume of material disclosed, "limited items" were involved.[115] As to the time taken to rectify disclosure, her response was "rather immediate, upon notification."[116] And as to the last factor, fairness "weighed in [Curto's] favor because clients should be encouraged to provide full disclosure to their attorneys without fear that their disclosure will be invaded."[117]

3. Use of a Company Computer as Waiver of Work-Product Immunity

¶32 Along with assertions that attorney-client privilege protects documents sent and received between a lawyer and client are claims that some material generated is protected by the qualified privilege of work product.[118] Work-product immunity does not depend on an intent that it remain confidential, although a waiver will occur when information is voluntarily disclosed to an adversary.[119] However, "no waiver attends a disclosure that

---

[109] *Curto*, 2006 WL 1318387, at *3 (alteration in original).
[110] *Id.* (alteration in original).
[111] *Id.* at *5.
[112] *Id.* at *3 (alteration in original). There were approximately four instances in which employee computer use was monitored, which "occurred under very limited circumstances," namely at the specific request of someone at the company. *Id.* One instance involved an employee allegedly downloading pornographic material, another involved poker playing on the Internet, and a third involved an employee allegedly conducting an outside business. *Id.*
[113] *Id.* at *3, *5. While reserving decision on the issue of privilege itself, the court noted that it was reasonable for Curto to believe her e-mails and personal documents were confidential. Working from a home office and not the offices of her employer, Curto's computers were not connected to her employer's computer server; therefore, use could not be monitored nor could e-mails be intercepted. For her employer to access documents on her laptops, the equipment would have to be physically transported to the employer's offices, or someone from the employer's office would have to examine them in her home. *Id.* at *5.
[114] *Id.* at *3. The magistrate noted that other company employees, including the president, had personal AOL accounts on their company computers. *Id.* at *3 n.2.
[115] *Id.* at *3.
[116] *Id.*
[117] *Id.*
[118] *See supra* notes 26–27 and accompanying text.
[119] *See* United States v. Nobles, 422 U.S. 225, 239 (1975).

has not 'substantially increased the opportunities for potential adversaries to obtain information.'"[120]

¶33 In the 2005 case *In re Asia Global Crossing, Ltd.*, the company maintained that the transmission of e-mails over the company e-mail system waived any privilege that might attach under the work-product doctrine.[121] The employees contended that, to the extent there was any disclosure of privileged material, the disclosure was inadvertent rather than voluntary.[122] The court took up the matter by analyzing the communications from the perspective of inadvertent disclosure, balancing the four factors of reasonableness of precautions, volume of discovery, time taken to rectify the matter, and overarching fairness.[123] However, the court determined that the question of inadvertence could not be resolved on the record as it existed since no distinction had been made between opinion and non-opinion work product.[124] "If the documents included opinion work product, the [employees] could not have waived it."[125]

¶34 In *Curto*, the plaintiff asserted that many of the documents retrieved from the employee's company laptop computer were protected from disclosure by attorney work-product immunity.[126] However, rather than treating attorney-client privilege and work-product immunity as two separate entities, they appear to have been addressed in tandem.[127] In doing so, the court noted the appropriateness of the four factor examination "in analyzing whether 'the producing party's conduct was so careless as to suggest that it was not concerned with the [protection] of the asserted privilege.'"[128] Reviewing the magistrate judge's analysis of the four factors, along with the fifth factor of company policy enforcement, it was determined that the magistrate judge's determination upholding the right to assert the attorney-client privilege and work-product protection was not clearly erroneous or contrary to law.[129]

4. Attorney Notices and Disclaimers

¶35 The majority of communications at issue in these matters involve electronic exchanges between a lawyer and client. Employers have forensically recovered and retrieved communications on company equipment that have been sent by a client to a lawyer, as well as transmissions from a lawyer to a client. Often, a lawyer's e-mails contain boilerplate language that addresses the issue of confidentiality and the privileged

---

[120] *In re* Asia Global Crossing, Ltd., 322 B.R. 247, 263 (Bankr. S.D.N.Y. 2005) (quoting United States v. Stewart, 287 F. Supp. 2d 461, 468 (S.D.N.Y. 2003)).
[121] *Id.*
[122] *Id.*
[123] *Id.*; *see* Curto v. Med. World Commc'ns, Inc., No. 03CV6327, 2006 WL 1318387, at *3 (E.D.N.Y. May 15, 2006).
[124] *See In re Asia Global Crossing*, 322 B.R. at 263; *see also* notes 30–34 and accompanying text.
[125] *In re Asia Global Crossing*, 322 B.R. at 263.
[126] *See Curto*, 2006 WL 1318387, at *2.
[127] The plaintiff asserted that identified documents "should be protected from disclosure under the attorney-client privilege and/or the attorney work product doctrine." *Id.* The magistrate judge subsequently held the plaintiff "had not waived her right to assert the attorney-client privilege or work product protection" as to the documents identified, which the reviewing court affirmed. *Id.* at *2, *8.
[128] *Id.* at *4 (alteration in original) (quoting SEC v. Cassano, 189 F.R.D. 83, 85 (S.D.N.Y. 1999)).
[129] *Id.* at *5, *8.

nature of the communication. However, these notices do not appear to afford the protection for confidential communications that might be warranted.

¶36 In the *Scott* case, within each of the e-mails Dr. Scott's lawyer sent to Dr. Scott's hospital e-mail account was a notice that the "message is intended only for the use of the Addressee and may contain information that is privileged and confidential."[130] Dr. Scott claimed the e-mails were privileged under both the attorney-client privilege and work-product doctrine, while the hospital claimed both privileges were waived by use of the system.[131] With respect to the issue of work product protection, the court noted that in New York, "inadvertent production of a privileged work product document generally does not waive the applicable privilege."[132] However, "there is an exception to that rule if the producing party's conduct 'was so careless as to suggest that it was not concerned with [the] protection of [the] asserted privilege.'"[133] Dr. Scott asserted that his lawyer's notice "is enough to take it out of the exception regarding inadvertent disclosure."[134] Focusing on the issue of confidentiality and the lawyer's pro forma notice, the court stated that "[t]he notice might be sufficient to protect a privilege if one existed," but such notice did not alter the hospital's policy.[135] Neither was a right to confidentiality created, nor was the notice "a reasonable precaution to protect its clients" when client confidences were at risk.[136]

¶37 While a pro forma notice which accompanies a lawyer's communication might not be a reasonable precaution to protect clients in given circumstances, it should alert a reader of the communication of the nature of the document. When forensically retrieved material that might be considered privileged comes into the hands of a lawyer, obligations under Model Rule 4.4(b) are triggered.[137] In *Stengart*, lawyers retained a computer forensic expert to retrieve e-mails that were automatically saved on the employee's company issued laptop.[138] The lawyers reviewed the e-mails, and used the contents of at least one e-mail between Stengart and her attorney in responding to interrogatories.[139] The court acknowledged that the employer's attempt to preserve evidence to defend a civil lawsuit was legitimate, but stated that failing to set aside arguably privileged messages was error.[140] Once they realized that attorney-client

[130] Scott v. Beth Israel Med. Ctr. Inc., 847 N.Y.S.2d 436, 439 (N.Y. Sup. Ct. 2007).
[131] *Id.* at 438–39. Dr. Scott claimed the communications were made in confidence and attempted to rely on a court rule "which states: 'no communication under this article shall lose its privileged character for the sole reason that it is communicated by electronic means or because persons necessary for the delivery or facilitation of such electronic communication may have access to the content of the communication.'" *Id.* at 440 (quoting N.Y. C.P.L.R. 4548 (McKinney 2002)).
[132] *Id.* at 443. "Under New York State law, work product is waived when it is disclosed in a manner that materially increases the likelihood that an adversary will obtain the information." *Id.*
[133] *Id.* (alterations in original) (quoting *SEC*, 189 F.R.D. 83, 85 n.4 (S.D.N.Y. 1999)).
[134] *Id.* at 444.
[135] *Id.*; *see supra* note 87 and accompanying text.
[136] *Scott*, 847 N.Y.S.2d at 444.
[137] *See supra* note 44 and accompanying text.
[138] Stengart v. Loving Care Agency, Inc., 990 A.2d 650, 655 (N.J. 2010).
[139] *Id.* at 656, 666.
[140] *Id.* at 665–66. Attorney error was also noted in the 2009 case *Fiber Materials, Inc. v. Subilia*, in which legal advice on an issue was sought by Subilia from his daughter, who was admitted to practice in Maine. 974 A.2d 918, 922 (Me. 2009). Subilia's daughter referred her father to a law firm which produced a memorandum and e-mailed it to her daughter, who forwarded it to Subilia's company e-mail address. *Id.*

communications were accessed, the lawyers should have notified Stengart or sought the court's permission before reading further, pursuant to Rule 4.4(b).[141]

IV. THE U.S. SUPREME COURT WEIGHS IN WITH *CITY OF ONTARIO V. QUON*

¶38 Courts have struggled when addressing issues relating to privacy in the workplace and use of a company computer as waiver of attorney-client privilege. Many of the decisions have essentially centered on an employee's objectively reasonable expectation of privacy when communicating with an attorney. When the Supreme Court heard arguments in *City of Ontario v. Quon*, many hoped that some definitive direction on the matter of employee expectation of privacy when using employer-provided communications equipment would be forthcoming. However, in its opinion, the Court declined to take this path.[142] While the decision provides useful information, the Court noted that "[p]rudence counsels caution before the facts in the instant case are used to establish far-reaching premises that define the existence, and extent, of privacy expectations enjoyed by employees when using employer-provided communication devices."[143]

¶39 In *City of Ontario v. Quon*, the City acquired pagers capable of sending and receiving messages, which were issued to Quon and other officers in the police

---

Each page of the memorandum contained the notice: "ATTORNEY/CLIENT PRIVILEGE CONFIDENTIAL WORK PRODUCT." *Id.* Counsel for Fiber Materials found this memorandum on Subilia's company owned laptop hard drive and read it at least twice. *Id.* at 923. Because of its content and markings, counsel contacted the ABA Ethics Search Service in deciding what to do next and received materials from the ABA to review. *Id.* Counsel also consulted a Maine Assistant Bar Counsel who said she would get back to her. *Id.* However, counsel turned the laptop over to company officials before bar counsel called her back. *Id.* The court noted:

> Presented with an obvious and important ethical issue in this uncharted area of the law in Maine, Attorney Beedy was right to seek guidance from all possible sources before deciding what to do with a memo from a law firm stamped "ATTORNEY/CLIENT PRIVILEGE." Having appropriately sought an advisory opinion from Bar Counsel, one of the best sources of ethical advice for Maine attorneys, prudence and good practice would strongly suggest obtaining an affirmative answer before embarking upon a potentially risky course of action. It seems equally evident that, having just delivered the memo to FMI officials, a reasonable attorney would return Bar Counsel's phone call to get an expert opinion before a potential legal case progressed. Attorneys do not act more ethically by avoiding relevant but potentially unwelcome information.

Id. at 928.

[141] *See Stengart*, 990 A.2d at 666. The New Jersey version of Rule 4.4(b) is based on the Model Rule, providing as follows:

> A lawyer who receives a document and has reasonable cause to believe that the document was inadvertently sent shall not read the document or, if he or she has begun to do so, shall stop reading the document, promptly notify the sender, and return the document to the sender.

N.J. RULES OF PROF'L CONDUCT R. 4.4(b) (2011). The employer argued that Rule 4.4(b) was inapplicable, since Stengart inadvertently left the e-mails on her laptop rather than sending them. *See Stengart*, 990 A.2d at 665–66. The court disagreed. *Id.* at 666. They were not "items that were simply left behind" in that, unbeknown to Stengart, they were automatically saved on the laptop's hard drive and retrieved by a forensic expert. *Id.*

[142] *See* Ontario v. Quon, 130 S. Ct. 2619, 2629–30 (2010).

[143] *Id.* at 2629.

department.[144] Although the police department had an official policy calling for monitoring and stating that users should have no expectation of privacy, a superior had announced an informal policy of allowing some personal use of the pagers.[145] Ontario's service contract called for a monthly limit on the number of characters each pager could send and receive, with overage resulting in additional fees.[146] When Quon initially exceeded his monthly character limit, he paid the City an overage fee for several months.[147] When Quon and other officers exceeded their monthly character limits for a number of months running, the police department sought to determine whether the character limit was too low. That is, whether officers had to pay fees for sending work-related messages or whether the overages were for personal messages.[148] The City obtained transcripts of Quon and another officer's text messages for August and September of 2002, looking at off-duty message time and whether on-duty messages related to police business.[149] It was discovered that many of Quon's messages were not work-related and that some were sexually explicit; as a result, Quon was disciplined.[150]

¶40 Quon and other respondents alleged that the City violated their Fourth Amendment rights when transcripts of their pager messages were obtained and reviewed.[151] The district court denied the constitutional claims, determining that, while Quon had a reasonable expectation of privacy in the content of his messages, the City's audit was for a legitimate purpose; thus, the Fourth Amendment was not violated.[152] However, the Ninth Circuit disagreed. Although it found that Quon had a reasonable expectation of privacy in his text messages, the court concluded that the legitimate search was not

---

[144] *Id.* at 2624–25.

[145] *Id.* at 2625–26. The official policy provided that the City "reserves the right to monitor and log all network activity including e-mail and Internet use, with or without notice. Users should have no expectation of privacy or confidentiality when using these resources." *Id.* at 2625. Quon, furthermore, signed a statement acknowledging that he had read and understood the policy. *Id.* "Although the Computer Policy did not cover text messages by its explicit terms, the City made clear to employees, including Quon, that the City would treat text messages the same way as it treated e-mails." *Id.*

[146] *Id.*

[147] *Id.*

[148] *Id.* at 2626.

[149] *Id.*

[150] *Id.* The audit of Quon's text messages noted that he

> sent or received 456 messages during work hours in the month of August 2002, of which no more than 57 were work related; he sent as many as 80 messages during a single day at work; and on an average workday, Quon sent or received 28 messages, of which only 3 were related to police business.

Id.

[151] *Id.*

[152] *Id.* at 2626–27. While the District Court found that Quon had a reasonable expectation of privacy in the content of his messages, it was the intent of the audit which would determine if it was nonetheless reasonable.

> "[I]f the purpose for the audit was to determine if Quon was using his pager to 'play games' and 'waste time,' then the audit was not constitutionally reasonable"; but if the audit's purpose "was to determine the efficacy of the existing character limits to ensure that officers were not paying hidden work-related costs, . . . no constitutional violation occurred."

Id. at 2627 (alteration in original) (quoting Quon v. Arch Wireless Operating Co., 445 F. Supp. 2d 1116, 1146 (C.D. Cal. 2006)). The jury determined that the audit was ordered to determine character limit efficacy, so the Fourth Amendment was not violated. *Id*.

reasonable in scope since there were less intrusive means that could have been used to determine character limit efficacy.[153] The Supreme Court found this was error. The search of Quon's text messages was reasonable and did not violate his Fourth Amendment rights.[154]

¶41 The parties in the case disagreed about whether Quon had a reasonable expectation of privacy. The City claimed its official policy established that pager messages were not to be considered private.[155] Quon asserted that statements by a superior overrode the official policy, so that employees could expect that the content of messages would remain private.[156] However, the Supreme Court declined to engage in a discussion of matters that would "bear on the legitimacy of an employee's privacy expectation."[157] Noting matters such as rapid changes in communication and information transmission,[158] evolution of work place norms,[159] and recent statutory enactments,[160] the Court mentioned that "[a] broad holding concerning employees' privacy expectations vis-à-vis employer-provided technological equipment might have implications for future cases that

---

[153] *Id.*
[154] *Id.* at 2633.
[155] *Id.* at 2629.
[156] *Id.*
[157] *Id.* The Supreme Court "agreed with the general principle that '[i]ndividuals do not lose Fourth Amendment rights merely because they work for the government instead of a private employer.'" *Id.* at 2628 (alteration in original) (quoting O'Connor v. Ortega, 480 U.S. 709, 717 (1987) (plurality opinion)). With respect to the proper analytical framework for Fourth Amendment claims against government employers, the four-Justice plurality in *O'Connor* put forward a two step analysis:

> First, because "some government offices may be so open to fellow employees or the public that no expectation of privacy is reasonable," a court must consider "[t]he operational realities of the workplace" in order to determine whether an employee's Fourth Amendment rights are implicated. On this view, "the question whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis." Next, where an employee has a legitimate privacy expectation, an employer's intrusion on that expectation "for noninvestigatory, work-related purposes, as well as for investigations of work-related misconduct, should be judged by the standard of reasonableness under all the circumstances."

Id. (quoting *O'Connor*, 480 U.S. at 725–26) (alteration in original) (citations omitted). However, Justice Scalia took a different approach in his concurring opinion in *O'Connor*, dispensing with an inquiry into operational realities, and concluding "that the offices of government employees . . . are covered by Fourth Amendment protections as a general matter." *Id.* (alteration in original) (quoting *O'Connor*, 480 U.S. at 731 (Scalia, J., concurring)) (internal quotation marks omitted). Additionally, he noted "that government searches to retrieve work-related materials or to investigate violations of workplace rules—searches of the sort that are regarded as reasonable and normal in the private-employer context—do not violate the Fourth Amendment." *Id.* (quoting *O'Connor*, 480 U.S. at 732 (Scalia, J., concurring)) (internal quotation marks omitted).
[158] *Id.* at 2629. The Court noted these changes are "evident not just in the technology itself but in what society accepts as proper behavior." *Id.*
[159] *Id.* at 2630 ("Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification. That might strengthen the case for an expectation of privacy. On the other hand, the ubiquity of those devices has made them generally affordable, so one could counter that employees who need cell phones or similar devices for personal matters can purchase and pay for their own. And employer policies concerning communications will of course shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated.").
[160] *Id.* The Court noted that "the law is beginning to respond to these developments, as some States have recently passed statutes requiring employers to notify employees when monitoring their electronic communications." *Id.*

cannot be predicted."[161] Preferring to dispose of the case on "narrower grounds," the Court assumed that Quon had a reasonable expectation of privacy in the text messages sent on his city-provided pager.[162] Additionally, the Court assumed that the City's review of his message transcripts was a search within the meaning of the Fourth Amendment and that "the principles applicable to a government employer's search of an employee's physical office apply with at least the same force when the employer intrudes on the employee's privacy in the electronic sphere."[163]

¶42 The Supreme Court determined that the City's search of Quon's text messages was reasonable.[164] "Although as a general matter, warrantless searches 'are *per se* unreasonable under the Fourth Amendment,'" there is an exception for "the 'special needs' of the workplace."[165] Here there were "reasonable grounds for suspecting that the search [was] necessary for a noninvestigatory work-related purpose" regarding the character limit issue, and a two month review was not "excessively intrusive."[166] The Court concluded that "[b]ecause the search was motivated by a legitimate work-related purpose, and because it was not excessive in scope, the search was reasonable"[167] and "would be 'regarded as reasonable and normal in the private-employer context.'"[168]

---

[161] *Id.*
[162] *Id.*
[163] *Id.*
[164] *Id.*
[165] *Id.* Relying on the *O'Connor* plurality, the Supreme Court stated that a "government employer's warrantless search is reasonable if it is 'justified at its inception' and if 'the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of' the circumstances giving rise to the search." *Id.* (quoting O'Connor v. Ortega, 480 U.S. 709, 725–26 (1987) (plurality opinion)). However, Justice Scalia's concurring opinion takes the position that "the proper threshold inquiry should not be whether the Fourth Amendment applies to messages on *public* employees' employer-issued pagers, but whether it applies *in general* to such messages on employer-issued pagers." *Id.* at 2634 (Scalia, J., concurring).
[166] *Id.* at 2631 (alteration in original) (internal quotation marks omitted). The Court noted that it "has 'repeatedly refused to declare that only the "least intrusive" search practicable can be reasonable under the Fourth Amendment.'" *Id.* at 2632 (quoting Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 663 (1995)).
[167] *Id.* (quoting *O'Connor*, 480 U.S. at 726).
[168] *Id.* at 2633 (quoting *O'Connor*, 480 U.S. at 732). The Court notes that its treatment satisfies the approach taken in the plurality, as well as the approach taken in Justice Scalia's concurrence in *O'Connor*. *Id.* However, in a concurring opinion by Justice Scalia, he chides the majority for inadvertently boosting the *O'Connor* plurality standard. *Id.* at 2635 (Scalia, J., concurring) ("Despite the Court's insistence that it is agnostic about the proper test, lower courts will likely read the Court's self-described "instructive" expatiation on how the *O'Connor* plurality's approach would apply here (if it applied) as a heavy-handed hint about how *they* should proceed. Litigants will do likewise, using the threshold question whether the Fourth Amendment is even implicated as a basis for bombarding lower courts with arguments about employer policies, how they were communicated, and whether they were authorized, as well as the latest trends in employees' use of electronic media. In short, in saying why it is not saying more, the Court says much more than it should.") (citation omitted).

V. FUNDAMENTAL CONCERNS

A. Public Policy

¶43 Free communication between a lawyer and client is considered to be a significant benefit to society.[169] As the U.S. Supreme Court has stated, the purpose behind the attorney-client privilege 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."[170] While narrow construction of the privilege has been called for,[171] courts are mindful that "the privilege carries through policy purposes,"[172] which are the foundation of the doctrine. These purposes are evident in the 2007 Western District of Washington case *Sims v. Lakeside School*.[173]

¶44 In *Sims*, employer Lakeside School obtained possession of employee Sims's laptop and made an image of his hard drive. Its electronic communications policy, set forth in the employee manual, stated that user "[a]ccounts are property of Lakeside School and are to be used for academic and administrative purposes only."[174] Regarding the school's e-mail system, the employee manual declared: "Lakeside does not assure the confidentiality of e-mail."[175] The employee acknowledged that he had read and reviewed the policy, leading the court to determine that Sims did not have a reasonable expectation of privacy in the contents of his laptop or in the e-mails he sent and received using the school's e-mail accounts.[176] In contrast, the court extended protection under attorney-client privilege to Sims' web-based e-mails as well as other materials Sims prepared to communicate with his counsel.[177] The court noted that "[n]otwithstanding defendant Lakeside's policy in its employee manual, public policy dictates that such communications shall be protected to preserve the sanctity of communications made in confidence."[178] The court relied on the precedent that "the attorney-client privilege is predicated upon the belief that it is in the public interest to encourage free and candid communications between clients and their attorneys, by protecting the confidentiality of such communications."[179]

¶45 Policy regarding privilege was also an issue in *Stengart*, in which the court acknowledged the "important public policy concerns underlying the attorney-client privilege,"[180] which is "enshrined in history and practice."[181] With regard to the

---

[169] *See supra* note 5 and accompanying text.
[170] Upjohn Co. v. United States, 449 U.S. 383, 389 (1981).
[171] *See supra* note 6 and accompanying text.
[172] *In re* Teleglobe Commc'ns Corp., 493 F.3d 345, 360 (3d Cir. 2007).
[173] No. C06-1412RSM, 2007 U.S. Dist. LEXIS 69568 (W.D. Wash. Sept. 20, 2007).
[174] *Id.* at *2 (alteration in original) (internal quotation mark omitted).
[175] *Id.* at *3 (internal quotation marks omitted).
[176] *Id.*
[177] *Id.* at *4. Plaintiff Sims also asserted that materials generated to communicate with his wife were protected under marital privilege. *Id.* at *5. The court agreed and extended protection to communications between Sims and his wife. *Id.*
[178] *Id.* at *4.
[179] *Id.* at *5 (citing United States v. Louisville & Nashville R.R., 236 U.S. 318, 336 (1915)). In *Curto*, the court considered the matter when balancing the factor of fairness, noting "clients should be encouraged to provide full disclosure to their attorneys without fear that their disclosure will be invaded." Curto v. Med. World Commc'ns, Inc., No. 03CV6327, 2006 WL 1318387, at *3 (E.D.N.Y. May 15, 2006).
[180] Stengart v. Loving Care Agency, Inc., 990 A.2d 650, 665 (N.J. 2010).

communications retrieved by the employer from the computer Stengart used, the court stated:

> They are conversations between a lawyer and client about confidential legal matters, which are historically cloaked in privacy. Our system strives to keep private the very type of conversations that took place here in order to foster probing and honest exchanges.[182]

¶46 While matters relating to expectation of privacy and waiver seem to be the central focus of much judicial scrutiny, the public's interest in the policies underlying the attorney-client privilege must not be brushed aside. The historic values behind the privilege should be paramount. This does not mean that a company's communication policy should not regulate use or provide for monitoring employee communications. However, "allowing employers to use technologically sophisticated methods to covertly intercept attorney-client communications could allow the employer to fold the protections of privilege into a paper tiger."[183] In balancing the public interest in fostering open exchanges between a lawyer and client, an employer's right and responsibility to control the workplace environment, and the factual circumstances surrounding an employee's exchange of information, protecting privileged communications should carry a heavy weight.

B. Lawyer Responsibility

¶47 It is clear that the legal mandates surrounding the issues of privacy in the workplace vary. As a result, lawyers must tread with caution when communicating with their clients. A fundamental value within the legal profession, reflected in an initial Model Rule, is that of competence.[184] Lawyers who communicate electronically with clients must be aware of the "perils associated with electronic transmission of documents."[185] For instance, with respect to digital documents and metadata,[186] it has

---

[181] *Id.* at 659.
[182] *Id.* at 664.
[183] Losey, *supra* note 64, at 1188.
[184] Model Rule 1.1 provides as follows:

> A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

MODEL RULES OF PROF'L CONDUCT R. 1.1 (2009).
[185] Hill, *supra* note 15, at 52.
[186] Metadata is hidden information in digital documents. It accompanies every word document unless it is removed, a process usually called "scrubbing." *See* Martin Whittaker, *Speakers Examine Metadata Phenomenon and Explore Whether Lawyers Should Fear It*, 23 Laws. Man. on Prof. Conduct (ABA/BNA) 305 (June 13, 2007). In addition,

> metadata falls into categories, the first of which is data that is generated and stored in a document by the software used to create it. Software generated metadata, sometimes referred to as system metadata, appears on the drafter's disk drives. While it does not appear in the on-screen or printed version of a document, typically, it can be accessed relatively easily. A second type of metadata, sometimes referred to as substantive metadata, is generated by the person who created the document. This metadata can track the revision history of a document and can either appear in the on-screen or printed version of the document, or be hidden from

been indicated that failure to stay abreast of technological developments may indicate a lack of reasonable care.[187] It may also indicate a lack of competence.

¶48 An ethics opinion of the ABA stated that when extraordinarily sensitive material is being communicated, enhanced security measures might be warranted.[188] Arguably, in this digital age, lawyers have an obligation to be even more vigilant when communicating information to a client that might be considered privileged. For instance, in *Scott*, Dr. Scott's lawyer sent sensitive material to Dr. Scott's work e-mail account which was received over the Beth Israel e-mail server.[189] It seems that transmitting sensitive material to a client's work e-mail account should have raised red flags for the lawyer. This conduct, in and of itself, might result in a waiver of opinion work product. In light of the fact that many companies have electronic communication policies that could impact the matter of privileged material, lawyers must be on guard with their own transmissions and alert clients of impending risks.

¶49 In *Scott*, the concern of communicating with a client via the client's work e-mail address should have been apparent to the lawyer. However, even if communications are being sent to a private address which is password protected, lawyers should still tread cautiously. Since the actual equipment being used by a client may not be apparent, lawyers should alert clients of risks and the possible impact that use of company equipment can have. As noted in *Scott*, a pro forma notice in a lawyer's communication is not a sufficient protection. While it might protect a privileged communication if one exists, it does not alter company policy.[190]

VI. CONCLUSION

¶50 The twenty-first century has seen the proliferation of electronic communications in business and private life. Employees are routinely issued company-owned computers, the use of which typically is governed by a company policy addressing legitimate

---

> view. A third type of metadata, sometimes referred to as embedded metadata, is "inferred through a relationship to another document." This metadata is data or content input by the user which is not typically visible in the output display, such as spread sheet formulas, hidden columns, linked files, database information or field codes. Metadata does not appear in the final print-ready version of a final electronic document, but it can be easily accessed.

Hill, *supra* note 15, at 22–23 (footnotes omitted). The primary issue surrounding metadata concerns "an electronic document, sent to a non-client, which may have confidential information available to a non-privileged viewer. Questions arise as to whether this destroys the privileged nature of the document, as well as" the responsibilities of lawyers who send and receive these documents. *Id.* at 23.

[187] The New York State Bar Association concluded that under their disciplinary rules, lawyers have a duty "to use reasonable care when transmitting documents by e-mail to prevent the disclosure of metadata containing client confidences or secrets." N.Y. State Bar Ass'n Comm. on Prof'l Ethics, Op. 782, at 3 (2004). The Committee stated that what constitutes reasonable care will vary with the circumstances, but noted it may "call for the lawyer to stay abreast of technological advances and the potential risks in transmission in order to make appropriate decisions with respect to the mode of transmission." *Id.* The Florida Bar addressed the obligations of lawyers when transmitting electronic documents, noting such obligations "may necessitate a lawyer's continuing training and education in the use of technology in transmitting and receiving electronic documents in order to protect client information." Fla. Bar Prof'l Ethics Comm., Op. 06-2 (2006).

[188] *See* Formal Op. 99-413, *supra* note 58.

[189] *See* Scott v. Beth Israel Med. Ctr. Inc., 847 N.Y.S.2d 436, 439 (N.Y. Sup. Ct. 2007).

[190] *Id.*

business concerns. Employees' expectations of privacy with respect to electronic transmissions and files associated with this equipment vary. Usually, whether the expectation of privacy is reasonable depends on nuances of the company's policy, the company's monitoring practices relating to use, third parties' right of access to material, and the employee's awareness of these matters.

¶51 Most companies allow employees to use company equipment for personal use. However, along with this, many company policies claim ownership of workplace communications, provide for access and review of transmissions, and alert employees that their electronic exchanges are not to be considered private. Therefore, when 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. Arguably, there is neither a subjective nor an objective privacy expectation with these transmissions. Rather, either the transmissions are not confidential, or, if they are considered confidential, use of this mechanism likely constitutes a voluntary waiver of any privilege that would otherwise protect the communication.

¶52 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. 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. In situations such as these, otherwise privileged communications should be protected. A company policy attempting to hold otherwise should be deemed unenforceable.

¶53 Notwithstanding the issues of privacy, confidentiality, and waiver, a lawyer who has reason to believe a communication *may be* privileged should notify the sender of the communication and comply with jurisdictional mandates before examining the content of a transmission. Concomitant with this duty is the lawyer's responsibility to see that requisite care is taken when communicating with clients and to ensure that clients are aware of the perils associated with electronic transmissions in the workplace. In the recent U.S. Supreme Court case *City of Ontario v. Quon*, the Court addressed its hesitance to embrace a broad holding on employee privacy expectation with references to rapid changes in communication and information transmissions, evolution of work-place norms, and recent statutory enactments. True—technology continues to evolve rapidly, and the law, as well as legal professional mandates, scamper to keep up in its wake. However, the benchmark public policy concerns that surround privilege issues, along with the professional responsibility of lawyers, should be brought to the forefront. Privacy and privilege are fundamental mandates which tip the balance in favor of protecting these interests.