ARTICLE

EMERGING TECHNOLOGY AND CLIENT CONFIDENTIALITY: HOW CHANGING TECHNOLOGY BRINGS ETHICAL DILEMMAS

LOUISE L. HILL*

* Professor of Law, School of Law, Widener University. The author would like to thank John Nivala for his time and thoughtful reflections when reading drafts of this article. The author would also like to thank Maggie Stewart for her diligent and tireless research assistance on this project.

I. INTRODUCTION

As technology advances, new methods for transmitting communications are created. With this emerging technology, lawyers face ethical issues associated with the conveyance of communications, many of which relate to confidentiality and privilege. Because of concern that third parties may intercept or have access to transmitted material, lawyers tend to tread with caution, especially when sensitive information is at issue.

As new tools for communicating information become a part of everyday legal practice, they challenge the parameters of client confidentiality. A matter drawing significant attention today relates to the transmission of documents in electronic form and "metadata," which is hidden information contained in digital documents. Questions arise about lawyers' responsibilities relating to hidden data imbedded in documents. Should liability attach to a lawyer who transmits a document containing hidden sensitive material? Should a lawyer who receives a digital document search for information that might benefit his client? Questions also arise about the effect of the transmission of hidden material that is confidential. Of particular concern is whether transmission of this information, which may be available to a non-privileged viewer, can destroy the privileged nature of a document or communication.

This article will begin by addressing the law of confidentiality in the United States. It will then consider recent changes in technology, and the impact these changes have had on contemporary legal practice. It raises issues associated with the transmission of electronic documents and metadata, with a focus on matters relating to confidentiality and privilege, as well as lawyer responsibility. This article will also examine the divergent positions that different jurisdictions have taken regarding metadata, as well as the effects of those positions. The article will conclude by positing a position for the treatment of metadata, highlighting the duty attaching to lawyers in its treatment.

II. CLIENT CONFIDENTIALITY

In the United States, the law of confidentiality is composed of three key doctrines: attorney-client privilege; lawyer work-product immunity; and a lawyer's ethical duty to maintain client confidences.[1] These are concepts which are related, but distinct.[2] The attorney-client privilege applies "in judicial and other proceedings in which a lawyer may be called as a witness or otherwise required to produce evidence concerning a client."[3] It essentially protects against compelled disclosure of confidential communications exchanged between lawyer and client.[4] A lawyer's ethical duty to maintain client confidences is "not limited to judicial or other proceedings, but rather applies in all representational contexts,"[5] covering all information relating to the representation, not just client communications.[6] Work-product immunity also extends beyond client communications, protecting material from discovery that a lawyer generates in preparing a matter for litigation.[7]

A. Attorney-Client Privilege

The attorney-client privilege is one of the most recognized of the privileges,[8] referred to by Dean John Wigmore as "the oldest of the privileges

---

[1] *See* Charles W. Wolfram, *The U.S. Law of Client Confidentiality: Framework for an International Perspective*, 15 FORDHAM INT'L L.J. 529, 540-44 (1992). A lawyer's ethical duty to maintain client confidences has been referred to as "the agency law of confidentiality." *Id*. at 545.

[2] Arthur Garwin, *Confidentiality and Its Relationship to the Attorney-Client Privilege*, *in* ATTORNEY-CLIENT PRIVILEGE IN CIVIL LITIGATION 31 (Vincent S. Walkowiak ed., 2004). That which is privileged also is "protected by the confidentiality principle but the reverse is not true." *Id.* at 32; *see* Louise L. Hill, *Disparate Positions on Confidentiality and Privilege Across National Boundaries Create Danger and Uncertainty for In-House Counsel and Their Clients*, *in* LEGAL ETHICS FOR IN-HOUSE CORPORATE COUNSEL A-127, 128 (BNA, Corp. Practice Series No. 87, 2007).

[3] MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 3 (2009).

[4] *See* GEOFFREY C. HAZARD, JR. & W. WILLIAM HODES, THE LAW OF LAWYERING, §. 9.2, 9-6 (3d ed. Supp. 2003). The privilege protects only the communication, not the underlying facts. Thus there is a distinction between information about a client and communication about that information. *See* Garwin, *supra* note 2, at 32.

[5] Garwin, *supra* note 2, at 31.

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

[7] *See* Wolfram, *supra* note 1, at 543.

[8] *See* 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); Joseph Pratt, *The Parameters of the Attorney-Client Privilege for In-house Counsel at the International Level: Protecting the Company's Confidential Information*, 20 NW. J. INT'L L. & BUS. 145, 149 (1999).

for confidential communications."[9] Dean Wigmore traces the attorney-client privilege to sixteenth century England where a solicitor was exempted from offering evidence.[10] The privilege has also been traced to Roman times where attorneys were servants of those whose affairs they managed, and under Roman law, could not testify for or against their masters since the relationship created a duty of loyalty.[11] In the United States, the attorney-client privilege is the only communications privilege recognized in every state.[12] Each state has its own privilege rules which generally follow the common law doctrine, while Rule 501 of the Federal Rules of Evidence governs federal courts.[13]

Rather than establishing fixed rules for attorney-client privilege, the United States Supreme Court determined that Rule 501 allows privilege issues to be decided on a case-by-case basis.[14] The Court acknowledged that this approach could "undermine desirable certainty in the boundaries of the attorney-client privilege."[15] Some feel this has come to fruition, in that there is "inconsistency and confusion at the margins of the privilege,"[16] which creates "practical difficulties for attorneys and other legal advisors."[17]

---

[9] 8 JOHN HENRY WIGMORE, EVIDENCE § 2290 (McNaughton Rev. 1961).

[10] *Id.*

[11] *See* Max Radin, *The Privilege of Confidential Communication Between Lawyer and Client*, 16 CAL. L. REV. 487, 487-88 (1927).

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

[13] *E.g.*, *id*. at 213; Pratt, *supra* note 8, at 151. The Federal Rules of Evidence provide:

> 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 principles of the common law as they may be interpreted by the courts of the United States in 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 witness, person, government, State, or political subdivision thereof shall be determined in accordance with State law.

FED. R. EVID. 501.

[14] Upjohn Co. v. United States, 449 U.S. 383, 396 (1981).

[15] *Id*. at 396-97.

[16] Yoshida, *supra* note 12, at 213. Whether communications of patent agents are entitled to privilege, and whether a general privilege is recognized for communications between in-house counsel and corporate employees, are examples of inconsistencies and confusion created by the case-by-case approach. *Id*. at 214. Third-party disclosure constituting waiver is also an issue on which the Circuits differ. *See* Mackintosh & Angus, *supra* note 8, at 43. The split on third-party disclosures is due in part to ambiguities in statutes that require disclosure of relevant documents and voluntary disclosure provisions of some government agencies. *Id.*

[17] Yoshida, *supra* note 12, at 214.

Attorney-client privilege is based on "a pragmatic judgment that confidentiality is necessary in order to encourage client communication."[18] It is recognized "to promote open and uninhibited consultations with lawyers," which is acknowledged "as providing a significant benefit to society."[19] While acknowledging these attributes, at the same time we are cautioned that the privilege, grounded on subjective considerations, is "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."[20] It is a rule of evidence, applicable in civil and criminal court proceedings, limiting "the extent to which a party in litigation can force from an unwitting witness a statement or document that is protected as confidential."[21]

As a general premise, the privilege attaches to confidential communications made between privileged persons, for the purpose of obtaining or providing legal assistance.[22] A standard rule of attorney-client privilege in the United States, formulated by Dean Wigmore,[23] is as follows:

(1) Where legal advice of any kind is sought
(2) from a professional legal advisor in his capacity as such,
(3) the communications relating to that purpose,
(4) made in confidence,
(5) by the client,
(6) are at his instance permanently protected
(7) from disclosure by himself or by his legal advisor,
(8) except the protection be waived.[24]

A version of the Wigmore rule, put forward by Judge Wyzanski of the United States District Court, District of Massachusetts,[25] finds there is

[18] Wolfram, *supra* note 1, at 544.

[19] Mackintosh & Angus, *supra* note 8, at 38. The public needs to know the law for society to function smoothly. This is furthered by consultation with attorneys, whose counsel should not result in greater liability. *Id.*

[20] WIGMORE, *supra* note 9, § 2291 ("The policy of the privilege has been plainly grounded since the latter part of the 1700s on subjective considerations." Prior to that, its theory was objective rather than subjective, "a consideration for *the oath and the honor* of the attorney rather than for the apprehensions of his client.").

[21] Wolfram, *supra* note 1, at 541-42.

[22] *Id*. In most jurisdictions, that which a lawyer communicates to a client is subject to the privilege, just as a client communication would be. *Id*. at 542.

[23] The position taken by Dean Wigmore was followed and adhered to by the Second, Sixth, Seventh, Ninth and Tenth Circuits. *See* Gregg F. LoCascio, *Reassessing Attorney-Client Privileged Advice in Patent Litigation*, 69 NOTRE DAME L.REV. 1203, 1207 n.23 (1994).

[24] WIGMORE, *supra* note 9, § 2292.

[25] The position taken by Judge Wyzanski was followed by the First, Third, Fourth, Fifth,

attorney-client privilege when:

(1) The asserted holder of the privilege is or ought to become a client;
(2) the person to whom the communication was made
  (a) is a member of the bar of a court, or his subordinate and
  (b) in connection with this communication is acting as a lawyer;
(3) the communication relates to a fact of which the attorney was informed
  (a) by his client
  (b) without the presence of strangers
  (c) for the purpose of securing primarily either
    (i) an opinion of law or
    (ii) legal services or
    (iii) assistance in some legal proceeding, and
  (d) not for the purpose of committing a crime or tort; and
(4) the privilege has been
  (a) claimed and
  (b) not waived by the client.[26]

The Restatement (Third) of the Law Governing Lawyers more briefly defines the attorney-client privilege as: (1) a communication; (2) made between privileged persons; (3) in confidence; (4) for the purpose of obtaining or providing legal assistance to the client.[27] Some courts have "treated the Wigmore and Restatement definitions as sufficiently similar to be somewhat interchangeable."[28]

1. Waiver

Attorney-client privilege can be waived; and waiver of the privilege is absolute, being "construed broadly against the party claiming the privilege."[29] At issue is whether waiver is triggered when confidential information is embedded in a document that is sent to a third party. Waiver can result from intentional voluntary disclosure, inadvertent disclosure, or the offensive use of

Eighth, Eleventh and District of Columbia Circuits. *See* LoCascio, *supra* note 23, at 1209 n.30.

[26] United States v. United Shoe Mach. Corp., 89 F. Supp. 357, 358-59 (D. Mass. 1950).

[27] RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS § 68 (2000). While seemingly simply stated, elements of the Restatement definition are further defined within other Restatement sections. *See* James N. Willi, *Proposal for a Uniform Federal Common Law of Attorney-Client Privilege for Communications with U.S. and Foreign Patent Practitioners*, 13 TEX. INTELL. PROP. L.J. 279, 289 (2005).

[28] *Id*. at 289; *see also* Pratt, *supra* note 8, at 152-53.

[29] Mackintosh & Angus, *supra* note 8, at 43.

otherwise privileged communications.[30] Some members of the legal community see disclosure of protected communications to a third party as the greatest threat to the protections offered by the attorney-client privilege.[31]

a. Voluntary Disclosure

"The client, not counsel, can voluntarily waive the privilege."[32] If a client willingly shares a privileged communication with a non-privileged person, "a court will feel free to find that, in this instance, the assurance of confidentiality was not important to the client, and that the general policy of free access by adversaries to all relevant evidence should prevail."[33] Some courts take the position that voluntary disclosure pursuant to a government subpoena constitutes only "limited waiver," retaining the disclosed communication's privileged status against other parties.[34] Other courts, however, find that voluntary disclosure to any non-privileged party constitutes waiver.[35]

---

[30] *Id*.; Wolfram, *supra* note 1, at 544.

[31] *See* Mackintosh & Angus, *supra* note 8, at 43.

[32] *Id*. at 42-43.

[33] Wolfram, *supra* note 1, at 544. Two or more parties with a common interest that "is the subject of confidential communications generally are allowed to share this information without losing the attorney-client privilege." ABA/BNA, Lawyers Manual on Professional Conduct: Corporate Privilege/Confidentiality Practice Guides 91:2201, LMPC 91:2201 (Westlaw). It is felt that in litigation, parties with allied interests should be able to communicate and coordinate their positions so as to more effectively present their claims. *Id.*

[34] *See* Westinghouse Elec. Corp. v. Republic of the Philippines, 951 F.2d 1414, 1427-29 (3d Cir. 1991) (discussing how various courts have treated the theory of selective waiver); Diversified Indus. v. Meredith, 572 F.2d 596, 611 (8th Cir. 1977); Leonen v. Johns-Manville, 135 F.R.D. 94, 99 (D.N.J. 1990); Palmer v. Farmers Ins. Exch., 861 P.2d 895, 908-09 (Mont. 1993); *see also* ABA/BNA, Lawyers Manual on Professional Conduct: Corporate Privilege/Confidentiality Practice Guides 91:2201, LMPC 91:2201 (Westlaw).

[35] Most federal courts view these acts as voluntary disclosure constituting a complete waiver of the attorney-client privilege. *See* United States v. Mass. Inst. of Tech., 129 F.3d 681, 685 (1st Cir. 1997); Genentech Inc. v. U.S. Int'l Trade Comm'n, 122 F.3d 1409, 1417 (Fed. Cir. 1997); *In re* Steinhardt Partners L.P., 9 F.3d 230, 235 (2d Cir. 1993); Westinghouse Elec. Corp., 951 F.2d at 1424-26 ; *In re* Martin Marietta Corp., 856 F.2d 619, 623-24 (4th Cir. 1988); Permian Corp. v. United States, 665 F.2d 1214, 1220-21 (D.C. Cir. 1981); Mackintosh & Angus, *supra* note 8, at 45 n.87. Although currently under attack by organizations as well as legislators, some federal programs encourage companies to self-report wrongdoing, or give mitigation credit to companies that make voluntary disclosures of privileged material. *See, e.g.*, "House Overwhelmingly Approves Bill to Limit DOJ Policy on Corporate Privilege Waivers," [Current Report] 23 Laws. Man. on Prof. Conduct (ABA/BNA) No. 24, at 604 (Nov. 28, 2007); "Counsel Group Assails Prosecution Policy Compelling Corporations to Waive Privileges," [Current Report] 16 Laws. Man. on Prof.

b. Inadvertent Disclosure

Opinion differs on whether attorney-client privilege is waived when there is inadvertent disclosure. Typically, when approaching the issue of inadvertent disclosure, one of three tests is applied: (1) "the strict responsibility test," where any disclosure, even inadvertent disclosures, waives attorney-client privilege; (2) "the subjective intent test," where inadvertent disclosure does not waive attorney-client privilege since waiver requires an intention to waive; or (3) "the balancing test," where waiver is determined based on an evaluation of circumstances.[36]

The strict responsibility test, which is the traditional test, was adhered to by Wigmore, putting the "risk of insufficient precautions on the client."[37] The rationale for the strict view is as follows: 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."[38] Some courts have favored this strict test because it forces self-regulatory behavior, and to do otherwise would be unfair to the party seeking to use the inadvertently disclosed communication.[39] It is also heralded as predictable and easy to apply.[40] Additionally, some find inadvertence "a euphemism for negligence, and, certainly . . . one is expected to pay a price for one's negligence."[41]

The subjective intent test, the most lenient approach, "holds that as long as the client did not intend to waive, the privilege remains intact, despite disclosure of the client's confidences to her adversary."[42] A court adopting

Conduct (ABA/BNA) No. 10, at 275 (June 7, 2000); *see also* ABA/BNA, Lawyers Manual on Professional Conduct: Corporate Privilege/Confidentiality Practice Guides 91:2201, LMPC 91:2201 (Westlaw).

[36] *See* Mackintosh & Angus, *supra* note 8, at 43 n.58; ABA/BNA, Lawyers Manual on Professional Conduct: Corporate Privilege/Confidentiality Practice Guides 91:2201, LMPC 91:2201 (Westlaw).

[37] WIGMORE, *supra* note 9, at 633.

[38] 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 313, 316 (Vincent S. Walkowiak ed., 2004) (quoting United States v. Kelsey-Hayes Wheel Co., 15 F.R.D. 461, 465 (E.D. Mich. 1954)).

[39] *See* Walkowiak, Lemons & Leach, *supra* note 38, at 317 (citing Suburban Sew 'N Sweep, Inc. v. Swiss-Bernina, Inc., 91 F.R.D. 254 (N.D. Ill. 1981); *In re* Sealed Case, 877 F.2d. 976, 980 (D.C. Cir. 1989)).

[40] *See* Walkowiak, Lemons & Leach, *supra* note 38, at 317.

[41] *Id*. at 316 (quoting *In re* Standard Fin. Mgmt. Corp., 77 B.R. 324, 330 (D. Mass. 1987)).

[42] Walkowiak, Lemons & Leach., *supra* note 38, at 318.

this approach found it "the better-reasoned rule."[43] The essence of the court's rationale was that "'inadvertent production is the antithesis' of an intentional relinquishment of a known right and, if the privilege is for the welfare of the *client*, more than the *attorney's* negligence should be required before the *client* loses the privilege."[44] As with the strict responsibility test, the subjective intent test has the advantage of being reasonably predictable and easy to apply.[45] It is criticized, however, in that "it exalts subjective considerations over objective ones,"[46] and does little to encourage care of privileged documents.[47]

The most popular of the three tests is the balancing test, where courts weigh circumstances which surround an inadvertent disclosure to determine whether a loss of privilege should result.[48] Although its proponents acknowledge that it is more difficult to apply, "ultimately this approach is fairer to both parties and the policy of preserving the privilege for confidential communications as it focuses on the confidentiality aspect of the privilege."[49] Described as the middle ground, this approach is sometimes criticized for being uncertain and for giving too much discretion to the court.[50] When determining if privilege is retained, courts generally balance 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.[51] Although routinely presented as a multi-factor test, it has nevertheless been asserted that courts primarily concentrate on only two considerations, those being "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."[52] Two main questions are implicated: "did the lawyer/client invoking the privilege really act in a careful manner we expect from someone truly concerned with guarding a confidence, both before and after the inadvertent disclosure?" and,

[43] Mendenhall v. Barber-Greene Co., 531 F. Supp. 951, 954 (N.D. Ill. 1982).

[44] Walkowiak, Lemons & Leach, *supra* note 38, at 318 (quoting Mendenhall, 531 F. Supp. at 955).

[45] *Id.* at 319.

[46] *Id.* at 318.

[47] *Id*. at 319.

[48] *Id.*

[49] *Id*. (quoting Kanter v.Superior Court, 253 Cal. Rptr. 810, 815 (Ct. App. 1988)).

[50] *Id.* at 321.

[51] *See* Mackintosh & Angus, *supra* note 8, at 45 n.87. The Chancery Court in Delaware notes that overall fairness must be "judged against the care or negligence with which the privilege is guarded." *In re* Kent County Adequate Public Facilities Ordinances Litigation Consolidated, C.A. No. 2921-VCN, at 5 (Del. Ch. April 7, 2008) 2008 WL 1851790.

[52] Walkowiak, Lemons & Leach, *supra* note 38, at 321.

"[w]ould it be fair to the person who has received the privileged information to try to make her expunge her knowledge of it from the litigation?"[53]

In December 2007, Senators Leahy and Specter introduced legislation in the United States Senate [S.2450] to create a new Federal Rule of Evidence 502.[54] The new rule attempted to resolve the disputes and conflicting decisions about the effect of inadvertent disclosure in federal court litigation. The House of Representatives approved the bill creating the new evidentiary rule by voice vote on September 8, 2008, which became law on September 19, 2008 when it was signed by the President of the United States.[55] The rule 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 took reasonable steps to correct the error after it occurred.[56] The rule also addresses the issue of scope of the waiver. When there is inadvertent disclosure, there is dispute among the courts as to whether the privilege is waived only as to those documents or communications that are inadvertently disclosed, or whether the waiver extends to all communications on the subject covered by the inadvertently disclosed communications.[57] The rule takes the position held by the majority

---

[53] *Id*.

[54] *See* Ralph Lindeman, *Leahy, Specter Introduce Bill to Create Evidence Rule to Prevent Privilege Waivers*, 23 Laws. Man. on Prof. Conduct (ABA/BNA) 646 (Dec. 26, 2007). Any proposed rule that would change an evidentiary privilege must be approved by Congress under the Rules Enabling Act, 28 U.S.C. § 2071. *Id.*

[55] *See* Ralph Lindeman, *House Gives Backing to New Court Rule to Prevent Accidental Privilege Waivers*, 24 Laws. Man. on Prof. Conduct (ABA/BNA) 496 (Sept. 17, 2008).

[56] There were five versions of Bill Number S.2450 for the 110th Congress. *See* http://thomas.loc.gov/cig-bin/thomas. The version which was signed into law, embodied in S.2450, provides as follows at Rule 502(b):

> Inadvertent Disclosure – When made in a Federal proceeding or to a Federal office or agency, the disclosure does not operate as a waiver in a Federal or State proceeding if:
>
> (1) the disclosure is inadvertent;
>
> (2) the holder of the privilege or protection took reasonable steps to prevent disclosure; and
>
> (3) the holder promptly took reasonable steps to rectify the error, including (if applicable) following Federal Rule of Civil Procedure 26(b)(5)(B).

Pub. L. No. 110-322, §1(b), 122 Stat. 3537 (2008). 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, 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

of courts,[58] which is that any waiver is limited to the actual material disclosed, and does not extend to other material which exists on the covered subject.[59] It is only when the waiver is intentional that it will extend to all related material on the same subject.[60]

While the new Federal Rule of Evidence 502 targets litigation in federal court,[61] state proceedings are also affected.[62] The new rule provides that an inadvertent disclosure first made in state court does not waive the privilege in federal court proceedings.[63] The new rule also provides that a federal court order that privilege is not waived extends the protection against inadvertent waiver to other federal and state court proceedings.[64]

Procedure of the Judicial Conference of the United States, Committee Note on Subdivision (b), May 15, 2006 (revised June 30, 2006).

[57] *See* Mackintosh & Angus, *supra* note 8, at 43 n.58 (citing *In re* Grand Jury Proceedings, 727 F. 2d 1352, 1356 (4th Cir. 1984)).

[58] *Id*.

[59] Rule 502(a), embodied in § 2450, provides as follows:

> Disclosure Made in a Federal Proceeding or to a Federal Office or Agency; Scope of Waiver – When the disclosure is made in a Federal proceeding or to a Federal office or agency and waives the attorney-client privilege or work-product protection, the waiver extends to an undisclosed communication or information in a Federal or State proceeding 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.

Pub. L. No. 110-322, §1(a), 122 Stat. 3537 (2008).

[60] *Id*.

[61] *See* Lindeman, *supra* note 54.

[62] Rule 502(f), embodied in § 2450, provides as follows:

> Controlling Effect of This Rule – Notwithstanding Rules 101 and 1101, this rule applies to State proceedings and to Federal court-annexed and Federal court-mandated arbitration proceedings, in the circumstances set out in the rule. And notwithstanding Rule 501, this rule applies even if State law provides the rule of decision.

Pub. L. No. 110-322, §1(a), 122 Stat. 3537 (2008).

[63] Rule 502(c), embodied in § 2450, provides as follows:

> Disclosure Made in a State Proceeding – When the disclosure is made in a State proceeding and is not the subject of a State-court order concerning waiver, the disclosure does not operate as a waiver in a Federal proceeding if the disclosure:
>
> (1) would not be a waiver under this rule if it had been made in a Federal proceeding; or
>
> (2) is not a waiver under the law of the State where the disclosure occurred.

Pub. L. No. 110-322, §1(a), 122 Stat. 3537 (2008).

[64] Rule 502 (d), embodied in § 2450, provides as follows:

> Controlling Effect of a Court Order – A Federal court may order that the privilege or

c. Offensive Use of Otherwise Privileged Communications

Waiver can also result from 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.[65] For instance, in a New York case, it was determined that the privilege was waived when the defendant relied upon the adequacy of an internal investigation as a defense in a sexual harassment suit.[66] Similarly, in a Delaware case, the court found the privilege was waived when respondents relied on communications with attorneys to support a motion for a protective order to preclude depositions.[67] That said, however, courts differ on the application of this

protection is not waived by disclosure connected with the litigation pending before the court – in which event the disclosure is also not a waiver in any other Federal or State proceeding.

Pub. L. No. 110-322, §1(d), 122 Stat. 3537 (2008).

Recently, the U.S. District Court for the Eastern District of Pennsylvania had an opportunity to apply new Federal Rule of Evidence 502 when 812 privileged documents were included in plaintiff's document production of 78,000 e-mail messages during electronic discovery. Rhoads Industries, Inc. v. Bldg. Materials Corp. of Am., 254 F.R.D. 216 (E.D. Pa. 2008). Defense counsel notified plaintiff's counsel that apparently privileged documents had been produced, whereupon plaintiff's counsel immediately responded that any such disclosure was inadvertent and no privilege had been waived. *Id.* at 218. In considering the matter, the district court looked to the new rule, since subsection (c) calls for it to apply in proceedings commenced after its enactment and "insofar as is just and practicable, in all proceedings pending on such date of enactment." *Id.* The court began by looking to see if the producing party showed "at least minimal compliance" with the three factors in Section 502(b). *Id.* at 226. Concluding that minimal compliance was met since plaintiff took steps to prevent and rectify the inadvertent error, the court went on to note, however, that to some extent its efforts were not reasonable. *Id.* Since the matter of reasonableness was at issue, the court proceeded to the five factor test followed by the majority of courts. *Id.* Applying the traditional five factor test, the court found the first four factors favored the defendant, but the final factor favored the plaintiff. *Id.* Denying documents to the defendants would not be prejudicial to them since they had no right to the privileged documents. Concluding that the defendants did not carry the burden of proof as to the 812 e-mails, the court determined the privileged nature of the e-mails was not forfeited by the inadvertent disclosure. *Id*. at 227.

[65] *See* Mackintosh & Angus, *supra* note 8, at 43 n.57 (citing Chevron Corp. v. Pennzoil Co., 974 F.2d 1156, 1162 (9th Cir. 1992)). The "offensive use" doctrine comes into play when "privileged material is used as a 'sword' rather than as a 'shield.'" Vincent S. Walkowiak, *An Overview of the Attorney Client Privilege When the Client is a Corporation*, *in* ATTORNEY CLIENT PRIVILEGE IN CIVIL LITIGATION 1, 19 (Vincent S. Walkowiak ed., 2004).

[66] Brownell v. Roadway Package Sys. Inc., 185 F.R.D. 19, 25 (N.D.N.Y. 1999).

[67] *See In re* Kent County Adequate Pub. Facilities Ordinances Litig. Consol., C.A. No. 2921-VCN, 2008 WL 1851790, at *5 (Del. Ch. April 7, 2008).

doctrine. At issue may be a determination of when a communication actually has been introduced. Some courts find the privilege is waived when the protected information is integral to the outcome of issues in the lawsuit.[68] Other courts require the privileged material to be "outcome determinative" for there to be waiver.[69] Yet still other courts apply more liberal standards, determining that waiver should be found when: assertion of the privilege is the result of a party's affirmative act; the asserting party put the protected information at issue by making it relevant to the case; and application of the privilege would deny the adversary access to information vital to his defense.[70] Referred to as the Hearn Test, the latter standard has been criticized as being "too liberal and potentially chilling confidential attorney-client communications."[71]

Recently, the U.S. Court of Appeals for the Second Circuit invoked the remedy of mandamus to clarify the uncertainty surrounding the "at issue" waiver.[72] Agreeing with the critics of the Hearn Test, the Second Circuit took the position that it "cuts too broadly," noting that it "would open a great number of privileged communications to claims of at-issue waiver."[73] According to the Second Circuit, an assertion that information is relevant is not enough for waiver. The court determined that for there to be waiver, "a party must *rely* on privileged advice from counsel to make his claim or defense."[74] The court also noted that the issue of fairness underlies privilege waiver, which is a matter that is decided "on a case-by-case basis, and depends primarily on the specific context in which the privilege is asserted."[75]

---

[68] *See* Mortgage Guarantee & Title Co. v. Cunha, 745 A.2d 156, 159 (R.I. 2000); Metro. Ins. Co. v. Aetna Casualty & Surety Co., 730 A.2d 51, 60 (Conn. 1991); *see also* ABA/BNA, Lawyers Manual on Professional Conduct: Corporate Privilege/Confidentiality Practice Guides 91:2201, LMPC 91:2201 (Westlaw).

[69] *See* Republic Ins. Co. v. Davis, 856 S.W.2d 158, 163 (Tex. 1993); *see also* ABA/BNA, Lawyers Manual on Professional Conduct: Corporate Privilege/Confidentiality Practice Guides 91:2201, LMPC 91:2201 (Westlaw).

[70] *See* Hearn v. Rhay, 68 F.R.D. 574, 581 (E.D. Wash. 1975).

[71] ABA/BNA, Lawyers Manual on Professional Conduct: Corporate Privilege/Confidentiality Practice Guides 91:2201, LMPC 91:2201 (Westlaw).

[72] *See Second Circuit Clarifies Test for "At Issue" Privilege Waiver*, 24 LAWS. MAN. ON PROF. CONDUCT (ABA/BNA), 556 (Oct. 29, 2008).

[73] *In re* County of Erie, 546 F.3d 222, 229 (2d Cir. 2008).

[74] *Id.*

[75] *Id.* The court noted that the issue of unfairness only comes into play "when a party uses an assertion of fact to influence the decision maker while denying its adversary access to privileged material potentially capable of rebutting the assertion." *Id.* (quoting John Doe Co. v. United States, 350 F.3d 299, 306 (2d Cir. 2003)).

2. Crime-Fraud Exception

If a lawyer and client devise a criminal or fraudulent act, and then use the attorney-client privilege as a shield, "the administration of justice is not served."[76] Therefore, the attorney-client privilege is lost when a client either "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 "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."[77] The lawyer consulted need not be aware of the client's intent to use the lawyer's services to perpetrate a crime or fraud.[78] In addition to losing attorney-client privilege, the crime-fraud exception also bars work product immunity for a client.[79]

B. Work-Product Immunity

Lawyer work-product immunity has been described as "a broadened but flattened version of the attorney-client privilege."[80] It is broader because it encompasses almost everything a lawyer generates in preparing a case for litigation, not just confidential communications between the lawyer and client.[81] The immunity covers "mental impressions, conclusions, opinions, or legal theories of an attorney" that relate to litigation.[82] The immunity is flattened because the material must be prepared in anticipation of litigation.[83] Anticipated litigation is litigation that need not be imminent, but must be more than a "remote prospect."[84] Material protected as work product is not accessible "through the otherwise broad powers of pretrial discovery."[85] It extends a zone of privacy to preparations for litigation, preventing prepared

[76] ABA/BNA, Lawyers Manual on Professional Conduct: Corporate Privilege/Confidentiality Practice Guides 91:2201, LMPC 91:2201 (Westlaw).

[77] RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS § 82 (2000).

[78] *See* United States v. Chen, 99 F.3d 1495, 1504 (9th Cir. 1996); *In re* Grand Jury Proceedings, 102 F.3d 748, 752 (4th Cir. 1996); United States v. Neal, 27 F.3d 1035, 1048 (5th Cir. 1994).

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

[80] Wolfram, *supra* note 1, at 542.

[81] *Id*. at 543. Federal Rule of Civil Procedure 26(b)(3) extends work product to material prepared "by or for another party or by or for that other party's representative (including the other party's attorney, consultant, surety, indemnitor, insurer, or agent)." FED. R. CIV. P. 26(b)(3).

[82] Mackintosh & Angus, *supra* note 8, at 42 (quoting FED. R. CIV. P. 26(b)(3)).

[83] Wolfram, *supra* note 1, at 543-44.

[84] *In re* Special Sept. 1978 Grand Jury (II), 640 F.2d 49, 65 (7th Cir. 1980).

[85] Wolfram, *supra* note 1, at 543.

material from being exploited by adversaries.[86] It is different from attorney-client privilege because 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."[87]

A distinction is made between "ordinary" work product and "opinion" work product.[88] Ordinary work product consists of raw factual information, while opinion work product consists of mental impressions, conclusions, opinions or legal theories.[89] There are some situations in which work product protection can be overcome by an opposing party. To overcome work product protection, an opposing party usually must demonstrate a substantial need for the work product materials.[90] However, with respect to "opinion" work product, this type of material "is discoverable, if at all, only upon a showing of compelling need."[91]

Work product protection may also be vitiated by a prima facie showing of a crime or fraud,[92] or in some instances, unethical conduct by a lawyer.[93]

---

[86] *See* ABA/BNA, Lawyers Manual on Professional Conduct: Corporate Privilege/Confidentiality Practice Guides 91:2201, LMPC 91:2201 (Westlaw).

[87] Wolfram, *supra* note 1, at 544.

[88] *See In re* Green Grand Jury Proceedings, 492 F.3d 976, 980 (8th Cir. 2007); Palmer v. Farmers Ins. Exch., 861 P.2d 895, 908-09 (Mont. 1993).

[89] *In re* Green, 492 F.3d at 980; Palmer, 861 P.2d at 910.

[90] Fed. R. Civ. P. 26(b)(3), provides in part as follows:

> Trial Preparation: Materials
>
> (A) *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:
>
> (i) they are otherwise discoverable under Rule 26(b)(1); and
>
> (ii) 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.
>
> (B) *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.

FED. R. CIV. P 26(b)(3)(A)&(B).

[91] ABA/BNA, Lawyers Manual on Professional Conduct: Corporate Privilege/Confidentiality Practice Guides 91:2201, LMPC 91:2201 (Westlaw); *see* Palmer v. Farmers Ins. Exch., 861 P.2d at 911.

[92] *See* ABA/BNA, Lawyers Manual on Professional Conduct: Corporate Privilege/Confidentiality Practice Guides 91:2201, LMPC 91:2201 (Westlaw); RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS § 93 (2000); *see also supra* notes

However, a lawyer's independent work-product privilege is considered as 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 fraudulent or criminal purposes, so long as the lawyer was unaware that the client was doing so.[94] Seeking the lawyer's advice about the consequences of past activities does not fall within the crime-fraud exception.[95] Nor does the exception apply when the client does not accomplish the crime or fraud, for that would "penalize a client for doing what the privilege is designed to encourage, consulting a lawyer for the purpose of achieving law compliance."[96]

C. Ethical Obligation to Maintain Client Confidentiality

The Model Rules of Professional Conduct [Model Rules], on which almost all states in the United States base their legal ethics rules,[97] call for information relating to the representation of a client to be held in confidence, with limited exceptions.[98] This duty of confidentiality applies to all information related to

76-79 and accompanying text.

[93] *See* Moody v. Internal Revenue Service, 654 F.2d 795, 800 (D.C. Cir. 1981); *see also* ABA/BNA, Lawyers Manual on Professional Conduct: Corporate Privilege/Confidentiality Practice Guides 91:2201, LMPC 91:2201 (Westlaw).

[94] *See In re* Green Grand Jury Proceedings, 492 F.3d at 981 (The Eighth Circuit stated that "we 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.").

[95] *See* RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS § 82 cmt. e (2000); ABA/BNA, Lawyers Manual on Professional Conduct: Corporate Privilege/Confidentiality Practice Guides 91:2201, LMPC 91:2201 (Westlaw).

[96] RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS § 82 cmt. c (2000); *see* ABA/BNA, Lawyers Manual on Professional Conduct: Corporate Privilege/Confidentiality Practice Guides 91:2201, LMPC 91:2201 (Westlaw).

[97] With the adoption of the Model Rules format by Maine in 2009, California remains the only state whose legal ethics rules do not comport with the ABA Model Rule format. *Maine Becomes Penultimate Jurisdiction to Adopt Model Rules*, 25 Laws. Man. on Prof. Conduct (ABA/BNA) 135 (Mar. 18, 2009). However, while almost all states in the U.S. have adopted the Model Rules, lawyers are not provided with a uniform standard. Interpretational differences exist among the jurisdictions, as do differences in the text of some of the rules. *See* Louise L. Hill, *Electronic Communications and the 2002 Revisions to the Model Rules*, 16 ST. JOHN'S J. LEGAL COMMENT. 529, 531 (2002).

[98] MODEL RULES OF PROF'L CONDUCT R. 1.6(b) (2004). 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;

the representation, whatever its source.[99] It has been noted that the Model Rules do "not put generally known information outside the boundaries of confidentiality."[100] While it remains the rule, this approach to public information has been criticized as "so stringent as to approach the unworkable and the unrealistic."[101]

The Model Rule exceptions attaching to the duty of confidentiality were significantly expanded in 2002 and 2003. As originally adopted in 1983, the Model Rules permitted lawyers to disclose information relating to the representation of a client in two instances: to prevent the client from committing a criminal act likely to result in imminent death or substantial bodily harm;[102] and to respond to allegations, or establish a claim or defense on behalf of the lawyer, in designated proceedings.[103] Added to these exceptions in 2002 were securing legal advice about compliance with the Rules,[104] and compliance with other law or a court order.[105] The exceptions were again expanded in 2003 to address financial injury when the lawyer's services had been, or were being used in its furtherance. To that end, disclosure was permitted to prevent a client from committing a crime or fraud reasonably certain to result in substantial injury to the financial interests or property of another;[106] and to prevent, mitigate or rectify substantial injury to the financial

(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.

Id.

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

[100] Garwin, *supra* note 2, at 34.

[101] HAZARD & HODES, *supra* note 4, § 9.15, at 9-60 (Supp. 2005-2).

[102] MODEL RULES OF PROF'L CONDUCT R. 1.6(b)(1) (1983). This was modified in the recent Model Rule revisions to the prevention of "reasonably certain death or substantial bodily harm." *Id*. at R. 1.6(b)(1) (2003).

[103] *Id*. at R. 1.6(b)(2) (1983).

[104] MODEL RULES OF PROF'L CONDUCT R. 1.6(b)(2) (2002).

[105] *Id*. at R. 1.6(b)(4).

[106] MODEL RULES OF PROF'L CONDUCT R. 1.6(b)(2) (2003).

interests or property of another that is reasonably certain to result or which had resulted from the client's commission of a crime or fraud.[107]

The exceptions to the general prohibition against disclosure of client information in Model Rule 1.6 are permissive rather than mandatory. However, once Model Rule 1.6(b) permits a disclosure, other rules or law may require it. For instance, some ethics rules require disclosure to the extent it is permitted under Model Rule 1.6.[108] Breach of the obligation of confidentiality can subject a lawyer to professional discipline, with typical sanctions being reprimand, suspension or disbarment.[109] Occasionally, although not pursuant to the Model Rules, a client can also obtain damage recovery if a lawyer unjustifiably divulges confidential information that results in the client being harmed.[110]

III. EMERGING TECHNOLOGY AND CLIENT CONFIDENTIALITY

Over the years, lawyers have used available technology to communicate with clients. During much of the twentieth century, lawyers routinely spoke with clients on the telephone. Even though telephone company employees could eavesdrop on these land-line calls, which could also be intercepted by third parties, people had an expectation that these conversations would be private.[111] The Federal Wiretap Act reflected this expectation of privacy, prohibiting intentional interception of wire or electronic communications, and providing that interception does not waive any otherwise available privilege.[112]

A. Facsimile Transmissions

When facsimile transmission became affordable and widely used in the 1980's, it was not suggested that the mere use of a fax machine to transmit

---

[107] *Id*. at R. 1.6(b)(3).

[108] Model Rule 4.1(b) provides as follows:

> In the course of representing a client a lawyer shall not knowingly fail to disclose a material fact when disclosure is necessary to avoid assisting a criminal or fraudulent act by the client, unless disclosure is prohibited by Rule 1.6.

Id. at R. 4.1(b) (2009).

[109] *See* Wolfram, *supra* note 1, at 545.

[110] *Id*.

[111] *See* ABA/BNA Lawyers' Manual on Professional Conduct Electronic Communications Practice Guide, 55:401, LMPC 55:401 (Westlaw).

[112] 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). The Act also forbids the disclosure or use of unlawfully intercepted communications and bars the introduction into evidence of unlawfully intercepted conversations. *Id*. at § 2515.

confidential information would contravene an ethics rule.[113] In fact, most courts considering the matter found that transmission by fax did not alter the nature of protection afforded by privilege.[114] However, as with any other means of communication, lawyers were cautioned that they could not ignore their responsibility to maintain the confidentiality of client information when faxing material.[115] Noted was the fact that "careless use of a fax machine may result in inadvertent delivery of client information to the wrong person, triggering a dispute over availability of the attorney-client privilege and possible malpractice liability."[116]

B. Cordless Telephones

When cordless telephones began to be used, the expectation of privacy diminished. Using analog voice signals transmitted by radio-waves that broadcast in all directions, cordless telephone conversations could be picked up by mistake as well as intentionally monitored with relative ease.[117] Inadvertent interception occurred frequently with cordless phones, since using one was like operating a radio station, the broadcast of which could be received by anyone in range.[118] Due to this situation, Congress amended the Federal Wiretap Act in 1986 to exclude the radio portion of a cordless telephone conversation from the definition of "wire communication" and "electronic communication."[119] However, in 1994 these exceptions were removed from the statute,[120] making "legal protections afforded to cordless phone broadcasts identical to those protecting land-based calls."[121] It should be noted that some take the position that privacy is not assured on a cordless phone since federal law does not apply to mistakes, just intentional interceptions.[122]

---

[113] *See* ABA/BNA Lawyers' Manual on Professional Conduct Electronic Communications Practice Guide, 55:401, LMPC 55:401 (Westlaw).

[114] *Id*. "Although a misdirected fax may lose its privilege, no one argues that the use of a fax machine or the possibility of misdirection destroys any claim of privilege." David Hricik, *Confidentiality & Privilege in High-Tech Communications*, 60 TEX. B.J. 104, 110 (Feb. 1997).

[115] *See* ABA/BNA Lawyers' Manual on Professional Conduct Electronic Communications Practice Guide, 55:401, LMPC 55:401 (Westlaw).

[116] *Id.* at§ 55:401.

[117] *Id*.

[118] *See* Hricik, *supra* note 114, at 108.

[119] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 101, 100 Stat. 1848, 1848-1849 (1986) [hereinafter ECPA] amending 18 U.S.C. §§ 2510 (1), (12).

[120] Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, § 202(a), 108 Stat. 4279 (1994).

[121] Hricik, *supra* note 114, at 108.

[122] *See* ABA/BNA Lawyers' Manual on Professional Conduct Electronic

C. Cellular Telephones

The use of cellular telephones followed the cordless phone. With the advent of the cellular phone, radio signals were transmitted to a base station in a geographic area,[123] which were then transmitted via microwaves to the switch center of the cellular service provider, and transferred to local telephone service providers.[124] Capable of being intercepted by any receiver in the broadcast area capable of receiving cellular frequencies, Congress enacted legislation to make it a federal crime to intentionally intercept cellular communications.[125] In 1992, Congress also enacted legislation to prohibit the manufacture and importation of certain scanners primarily used to intercept cellular calls.[126] This notwithstanding, a "monitoring phenomenon" seemed to exist.[127] Due to this ease of monitoring, to protect their analog cellular calls, some lawyers used devices and services to provide protection against eavesdropping. Using scrambling, conversion or encryption techniques, lawyers sought to protect their calls from those who were unaware of the law, or chose to ignore it.[128]

Ethics opinions from various states considered the use of cordless or cellular phones by lawyers. To avoid a possible breach of confidentiality, many bar committees urged lawyers to use cordless or cellular phones with caution. It was suggested that lawyers warn those with whom they conversed that conversations via this technology were not secure and sensitive material should not be discussed.[129] Ethics opinions in several states indicated that communications conducted in this manner might not be considered confidential and might not be covered by the attorney-client privilege.[130] As a

Communications Practice Guide, 55:401, LMPC 55:401 (Westlaw). Today, cordless telephones that use digital transmissions, or that encrypt the digital signal, "thwart casual hobbyists who eavesdrop using commercial scanners." *Id.*

[123] *See* ABA/BNA Lawyers' Manual on Professional Conduct Electronic Communications Practice Guide, 55:401, LMPC 55:401 (Westlaw) (The geographic area is referred to as a "cell.").

[124] *Id.*

[125] *See* ECPA, *supra* note 119, amending 18 U.S.C. § 2511(1).

[126] 47 U.S.C. 302a (d); *see* Hricik, supra note 114, at 108.

[127] *See* ABA/BNA Lawyers' Manual on Professional Conduct Electronic Communications Practice Guide, 55:401, LMPC 55:401 (Westlaw).

[128] *Id.*

[129] *Id.*; *see* [1994] Nat'l Rep. Legal Ethics (Univ. Pub. Am.) Mass. Ethics Op. 94-5; NYCBA Comm. On Professional Ethics, Formal Op. 1994-11 (1994); WSBA Informal Op. 91-1 (1991); *see also* Hricik, *supra* note 114, at 112.

[130] *See* [1995] Nat'l Rep. Legal Ethics (Univ. Pub. Am.) N. C. Proposed RPC 215; [2003] LAWS. MAN. ON PROF. CONDUCT (ABA/BNA) Iowa Ethics Op. 90-44, 1001:3601; [1990] LAWS. MAN. ON PROF. CONDUCT (ABA/BNA) Ill. Ethics Op. 90-7, 901:3001.

result, lawyers shied away from using analog phones for client conversations.

With the advent of digital technology, concerns about interception of cellular telephone conversations diminished. Unlike analog service, digital cellular service turns voices into bits, and calls transmitted in digital format cannot be heard by simple radio frequency scanners.[131] Digital phones offered greater security than their predecessors, eliminating concern about widespread eavesdroppers. Although susceptible to interception by the sophisticated, with digital technology came an expectation of a greater degree of privacy.[132]

D. Internet Transmissions

The mid-1990's saw the emergence of the internet and e-mail as an integral form of communication, and not surprisingly, an integral part of legal practice.[133] Because of this, the legal profession has devoted considerable attention to this type of technology and its ramifications in the practice of law.[134] Although federal statutes prohibit intentional interception of e-mail,[135] lawyers disagreed about the propriety and malpractice risk of communicating confidential client information via unencrypted e-mail.[136] The result of this discourse was the recognition of a reasonable expectation of privacy in e-mail messages, and the determination that the interception of an electronic communication does not cause an otherwise privileged electronic communication to lose its privileged character.[137] This notwithstanding, many lawyers tended to avoid using e-mail for sensitive material and encrypted material, or employed some generally accepted security system when

---

[131] *See* ABA/BNA Lawyers' Manual on Professional Conduct Electronic Communications Practice Guide, 55:401, LMPC 55:401 (Westlaw).

[132] *Id*.

[133] *See* Joan C. Rogers, *Ethics, Malpractice Concerns Cloud E-mail, On-line Advice*, 12 LAWS. MAN. ON PROF. CONDUCT (ABA/BNA) 59 (1996).

[134] From the sender's computer, most internet e-mail goes through several routers before arriving at the intended password protected mailbox of the recipient. The routers, which are owned by various third parties, temporarily store and help distribute e-mail messages. *See* Hricik, *supra* note 114, at 113-14.

[135] 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. ECPA, *supra*, note 119.

[136] *See* [1996] Nat'l Rep. Legal Ethics (Univ. Pub. Am.) Iowa Ethics Op. 96-1; [2003] LAWS. MAN. ON PROF. CONDUCT (ABA/BNA) S.C. Ethics Op. 94-27, 1001:7901; [1995] Nat'l Rep. Legal Ethics (Univ. Pub. Am.) N. C. Proposed RPC 215*; see also* ABA/BNA Lawyers' Manual on Professional Conduct Electronic Communications Practice Guide, 55:401, LMPC 55:401 (Westlaw).

[137] *See* 18 U.S.C. § 2517(4) (2006).

communicating with clients.[138]

No authority exists which suggests that privilege is unavailable simply because a lawyer and client communicate via internet e-mail.[139] It has been argued that the federal statutory prohibitions against intercepting these communications render them "sufficiently private to satisfy the conditions for the attorney-client privilege to apply."[140] Also, it has been noted that "[f]ull use of all available technology to prevent interception is not required."[141] Generally, only steps that are reasonable under the circumstances are called for.

When the matter of mandatory encryption of e-mail was addressed by the American Bar Association in 1999, an ABA Committee concluded that a lawyer may communicate with a client via e-mail without encryption.[142] It reached this conclusion reasoning that the expectation of privacy for e-mail is the same as that for ordinary telephone calls, and the unauthorized interception of an electronic message is illegal. The ABA Committee noted, however, that unusual circumstances involving extraordinarily sensitive information might warrant enhanced security measures like encryption, just as ordinary telephones and other normal means of communication would be deemed inadequate to protect confidentiality in some situations.[143]

---

[138] *See* ABA/BNA Lawyers' Manual on Professional Conduct Electronic Communications Practice Guide, 55:401, LMPC 55:401 (Westlaw). It has been noted that:

> A client with a sensitive issue to discuss is likely to be quite unhappy, and could well sue, if high-tech means of communication lead others to become aware of this discussion and if the client's lawyer failed to take adequate precautions or failed to warn the client of the potential risks. This is so even if 'privilege' as such is not lost.

Rogers, *supra* note 133, at 64 (quoting Peter Jarvis & Bradley Tellam, Electronic Ethics and Malpractice Issues, 5-5, Washington State Bar Seminar on Lawyers and the Internet (1995)).

[139] *See* Hricik, *supra* note 114, at 116.

[140] ABA/BNA Lawyers' Manual on Professional Conduct Electronic Communications Practice Guide, 55:401, LMPC 55:401 (Westlaw).

[141] *Id*. (quoting MUELLER & L. KIRKPATRICK, MODERN EVIDENCE, § 5.13 (1995)).

[142] ABA Comm. on Ethics and Prof'l Responsibility Formal Op. 99-413 (1999).

[143] *Id.* In an ethics opinion of the Committee on Professional Ethics of the Delaware State Bar Association, it was determined that a lawyer may make communications in confidence when using e-mail or a cell phone absent extraordinary circumstances. The test proposed by the committee was whether the lawyer reasonably anticipated the possibility of interception and used the example of sharing e-mail accounts with another. To determine if an extraordinary circumstance exists, the committee suggested the lawyer determine if there is a significant risk of inadvertent disclosure, and if not, then the communication can generally be made in confidence using e-mail or a cell phone. Del. State Bar Ass'n Comm. on Prof'l Ethics, Op. 2001-2 (2001). More recently, in an ethics opinion of the Professional Ethics Commission of the Maine Board of Bar Overseers, it was determined that as a

E. Model Rule 4.4(b)

With the proliferation of electronic communications, the relative ease of transmission has resulted in an increase of inadvertent communications being disseminated. This matter is specifically addressed in Model Rule 4.4(b) and its commentary. The rule itself 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.[144]

Notification to the sender of an "errant" communication enables that person to take protective measures. The commentary to the rule specifically notes that additional steps to be taken by the lawyer, 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.[145]

IV. THE DISPUTE SURROUNDING METADATA

An issue associated with electronic communications that is receiving considerable attention relates to "metadata," which is hidden information in digital documents. As a general premise, 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.[146] Software generated metadata, sometimes referred to as system metadata, appears on the drafter's disk drives.[147] While it does not appear in the on-screen or printed version of a document, typically, it can be accessed relatively easily.[148] A second type of metadata, sometimes referred to as substantive metadata, is generated by the person who created the document.[149] This metadata can track the revision history of a document and can either appear in the on-screen or printed version of a document, or be

general matter, an attorney may utilize unencrypted e-mail without violating the lawyer's ethical obligation to maintain client confidentiality. The Commission went on to note, however, that some circumstances might require a more secure method of communication. Me. Prof'l Ethics Comm'n of the Bd. of Overseers of the Bar, Op. 194 (2007).

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

[145] *Id.* at cmt. 2.

[146] *See* Martin Whittaker, *Speakers Examine Metadata Phenomenon and Explore Whether Lawyers Should Fear It*, 23 ABA/BNA Law. Manual on Professional Conduct 305 (June 13, 2007).

[147] *See* D. Md. Local R., *Suggested Protocol for Discovery of Electronically Stored Information* ("Suggested Protocol") at 25, www.mdd.uscourts.gov/localrules/localrules.html.

[148] *See* Whittaker, *supra* note 146, at 305. Often it can be found in the "file" menu under "properties." *Id.*

[149] *See id.*; *see also* Suggested Protocol, *supra* note 147.

hidden from view.[150] A third type of metadata, sometimes referred to as embedded metadata, is "inferred through a relationship to another document."[151] 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.[152] Metadata does not appear in the final print-ready version of a final electronic document, but it can be easily accessed. It accompanies every Word document unless it is "scrubbed."[153] At issue is 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 how lawyers should deal with hidden data imbedded in documents they receive.

A. The Position of the American Bar Association

There is disagreement among the authorities regarding how lawyers should treat metadata. An ABA Formal Opinion released in 2006 indicates that a receiving lawyer is free to review and use embedded information contained in electronic documents.[154] Noting that the Model Rules do not specifically prohibit such practice, the ABA Committee found MR 4.4(b) [155] to be the most closely applicable rule, calling for the sole requirement of notice to the

---

[150] It is available through the "insert comment" and "track changes" functions of Word. *See* Whittaker, *supra* note 146, at 305-06.

[151] Williams v. Sprint/United Mgmt. Co., 230 F.R.D. 640, 647 (D. Kan. 2005).

[152] *See* Suggested Protocol, *supra* note 147, at 27.

[153] *See* Whittaker, *supra* note 146, at 305. Pennsylvania Bar Association Committee on Legal Ethics and Professional Responsibility Formal Opinion 2009-100 addresses the removal of metadata as follows:

> Corel WordPerfect Versions X3 and X4 permit a user to easily remove all or specific metadata. Microsoft Office products do not permit the easy removal of this information. Microsoft Office 2007 includes several different "Document Inspectors" that may be used to find and remove different kinds of hidden data and personal information. Some of these Inspectors are specific to individual Office programs. The Document Inspector displays different sets of Inspectors in Office Word 2007, Office Excel 2007, and Office PowerPoint 2007 to enable the user to find and remove hidden data and personal information that is specific to each of these programs. Users must be cautious, however, because there are many types of metadata and these processes may not remove all of the metadata.

Pa. Bar Ass'n Comm. on Legal Ethics & Prof'l Responsibility, Formal Op. 2009-100 n.3 (2009).

[154] ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 06-442 (2006) (discussing the review and use of metadata).

[155] MODEL RULE OF PROF'L CONDUCT R. 4.4(b) (2009).

sender[156] that the inadvertently sent information was received.[157] The ABA Committee observed that much metadata is inconsequential and that steps can be taken by the sender to limit the likelihood that metadata will be transmitted in electronic documents.[158] The ABA position, that a lawyer is free to look for hidden embedded data and use it to the advantage of the receiving lawyer's client, was contrary to the position taken previously in two New York State ethics opinions, discussed below.

B. The Position of the New York State Bar Association

In 2001, the Committee on Professional Ethics of the New York State Bar Association considered whether lawyers could use available technology to surreptitiously examine and trace electronic documents.[159] In reaching the conclusion that this would not be permissible, the Committee looked to New York's Disciplinary Rules which prohibit a lawyer from engaging in conduct "involving dishonesty, fraud, deceit or misrepresentation,"[160] and "conduct that is prejudicial to the administration of justice."[161] The Committee then reasoned:

> We believe that in light of the strong public policy in favor of preserving confidentiality as the foundation of the lawyer-client relationship, use of technology to surreptitiously obtain information that *may* be protected by the attorney-client privilege, the work product doctrine or that *may* otherwise constitute a "secret" of another lawyer's client would violate the letter and spirit of these Disciplinary Rules.[162]

Relying on this 2001 New York opinion, in 2004, the New York State Bar Association Committee on Professional Ethics again considered a matter

---

[156] ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 06-442 (2006) (the committee concluded that Rule 4.4(b)'s sole requirement of promptly notifying the sender was "evidence of the intention to set no other specific restrictions on the receiving lawyer's conduct. . .").

[157] *Id*. The committee noted, however, that:

> Whether the receiving lawyer knows or reasonably should know that opposing counsel's sending, producing, or otherwise making available an electronic document that contains metadata was "inadvertent" within the meaning of Rule 4.4(b), and is thereby obligated to provide notice of its receipt to the sender, is a subject that is outside the scope of this opinion.

Id. at 4.

[158] *Id.*

[159] N.Y. State Bar Ass'n Op. 749 (Dec. 14, 2001).

[160] N.Y. CODE OF PROF'L RESPONSIBILITY DR 1-102(A)(4) (2007).

[161] *Id*. at DR 1-102(A)(5).

[162] N.Y. State Bar Ass'n Op. 749, *supra* note 159, at 3 (emphasis added).

involving electronic documents.[163] Looking to the Disciplinary Rule that states a lawyer shall not '"knowingly' reveal a confidence or secret of a client,"[164] the Committee considered whether a lawyer who transmits documents that contain "metadata" reflecting client confidences or secrets violates this rule.[165] The New York Committee 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."[166] As to what constitutes reasonable care, the Committee stated it will vary with the circumstances, including:

> the subject matter of the document, whether the document was based on a "template" used in another matter for another client, whether there have been multiple drafts of the document with comments from multiple sources, whether the client has commented on the document, and the identity of the intended recipients of the document.[167]

It was also noted that reasonable care 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."[168]

C. The Position of the Florida Bar Association

In September of 2006, a month following the release of the ABA opinion on metadata, the Florida Bar issued an opinion addressing the ethical duties of lawyers when sending and receiving electronic documents in the course of client representation.[169] Siding with the approach taken in New York, rather than that of the ABA, the Florida Bar determined that "a lawyer receiving an electronic document should not try to obtain information from metadata."[170] In considering this matter, the Florida Bar set forth the following obligations for lawyers when transmitting electronic documents:

> 1) It is the sending lawyer's obligation to take reasonable steps to safeguard the confidentiality of all communications sent by electronic means to other lawyers and third parties and to protect from other lawyers and third parties all confidential information, including information

---

[163] N.Y. State Bar Ass'n Op. 782 (Dec. 8, 2004).

[164] N.Y. CODE OF PROF'L RESPONSIBILITY DR 4-101(B) (2007).

[165] *See* N.Y. State Bar Ass'n Op. 782, *supra* note 163.

[166] *Id.* at 3.

[167] *Id*. at 2.

[168] *Id.* at 3.

[169] Fla. Bar Prof'l Ethics Comm., Op. 06-02 (2006), http://www.floridabar.org/tfb/tfbetopin.nsf/SearchView/ETHICS,+OPINION+06-2?opendocument.

[170] *Id*.

> contained in metadata, that may be included in such electronic communications.
>
> 2) It is the recipient lawyer's concomitant obligation, upon receiving an electronic communication or document from another lawyer, not to try to obtain from metadata information relating to the representation of the sender's client that the recipient knows or should know is not intended for the recipient. Any such metadata is to be considered by the receiving lawyer as confidential information which the sending lawyer did not intend to transmit.
>
> 3) If the recipient lawyer inadvertently obtains information from metadata the recipient knows or should know was not intended for the recipient, the lawyer must "promptly notify the sender."[171]

The Florida opinion, which did not address electronic documents in the context of discovery,[172] also noted that these 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."[173]

D. The Positions of Other Jurisdictions

When the legal community first began to consider how to handle metadata, two divergent points of view emerged. The ABA position, indicating a receiving lawyer is free to review and use imbedded information,[174] and the position taken by New York and Florida, indicating a receiving lawyer should not try to obtain information from metadata that the lawyer knows, or should know, was not intended for him.[175] While the committees disagreed about the receiving lawyer's responsibilities with respect to metadata, they did not disagree on the sending lawyer's responsibilities. It is the responsibility of the sending lawyer to take reasonable measures to avoid the disclosure of confidential information imbedded in electronic materials.[176]

As subsequent jurisdictions considered the metadata issue, some leaned toward the position taken by the ABA, some favored the approach taken by New York and Florida, while others employed their own variations.

---

[171] *Id.* (citation omitted).

[172] Specifically stating that it did "not address metadata in the context of documents that are subject to discovery under applicable rules of court or law," the opinion noted it did "not address the role of the lawyer acting as a conduit to produce documents in response to a discovery request." *Id.*

[173] *Id.*

[174] *See supra* notes 154-58 and accompanying text.

[175] *See supra* notes 159, 163, 169 and accompanying text.

[176] *See supra* notes 158, 166 and accompanying text.

Committees from Maryland[177] and Colorado[178] were inclined toward the ABA position, while committees from Arizona,[179] Alabama,[180] Maine[181] and New Hampshire[182] sided with the approach taken by New York[183] and Florida. The committee from the District of Columbia distinguished its approach, calling for actual knowledge of inadvertent disclosure before barring access to metadata.[184] The committee from Pennsylvania originally took a middle of the road approach, calling for lawyers who receive electronic information to use their own judgment in deciding whether to look for and use embedded information.[185] However, apparently upon reflection, the Pennsylvania Committee decided to "generally align" itself with the ABA position, "concluding that 'an attorney who receives [. . .] inadvertently transmitted information from opposing counsel may generally examine and use the metadata for the client's benefit without violating the Rules of Professional Conduct.'"[186]

1. Maryland

The Maryland State Bar Association Committee on Ethics was asked to consider whether an attorney who receives electronic documents containing metadata may view or use that metadata without first ascertaining whether the sending attorney inadvertently or intentionally included the material.[187] Viewing the matter from the perspective of electronic discovery, the Maryland Committee answered that question in the affirmative. A receiving lawyer may

[177] Md. State Bar Ass'n Comm. on Ethics, Op. 2007-09 (2007).

[178] Colo. Bar Ass'n Ethics Comm., Formal Op. 119 (2007), http://www.cobar.org/index.cfm/ID/386/subID/23789/CETH/.

[179] Ariz. State Bar Comm. on Rules of Prof'l Conduct, Ethics Op. 07-03 (2007), http://www.myazbar.org/Ethics/opinionview.cfm?id=695.

[180] Ala. Office of Gen. Counsel, Ethics Op. 2007-02 (2007), http://www.alabar.org/ogc/PDF/2007-02.pdf.

[181] Me. Prof'l Ethics Comm'n of the Bd. of Bar Overseers Op. 196 (2008), http://www.mebaroverseers.org/Ethics%20Opinions/Opinion%20196.htm.

[182] N.H. Bar Ass'n Ethics Comm. Op. 2008-2009/4 (2009).

[183] In March of 2008, a committee from the New York County Lawyers' Association Committee on Professional Ethics endorsed the position previously taken by the New York State Bar Association. N. Y. County Lawyers' Ass'n Comm. on Prof. Ethics Op. 738 (Mar. 24, 2008).

[184] D. C. Bar Ethics Op. 341 (2007).

[185] Pa. Bar Ass'n Comm. on Legal Ethics & Prof'l Resp. Op. 2007-500 (2007).

[186] *Lawyers May Review and Use Metadata, Panel Advises in Second Look at Issue*, 25 Laws. Man. on Prof'l Conduct (ABA/BNA) 245 (May 13, 2009) (quoting Pa. Bar Ass'n Comm. on Legal Ethics & Prof'l Resp. Formal Op.2009-100 (2009)).

[187] Md. Ethics Op. 2007-09, *supra* note 177.

view and make use of metadata in electronic documents without first ascertaining whether the sender intended to include it.[188] With respect to a sending attorney's obligations, the Committee took the position that "the sending attorney has an ethical obligation to take reasonable measures to avoid the disclosure of confidential or work product materials," that might be embedded in documents.[189] This obligation is based primarily on Rule 1.1,[190] addressing lawyer competence, and Rule 1.6, addressing client confidentiality.[191] The Maryland Committee noted, however, that not every inadvertent disclosure of privileged or work product material would constitute a violation of Rule 1.1 and/or Rule 1.6. "[E]ach case would have to be evaluated based on the facts and circumstances applicable thereto."[192]

On December 1, 2006, amendments to the Federal Rules of Civil Procedure became effective, which created a set of rules to govern discovery of electronically stored information [ESI].[193] In response to these changes in the

---

[188] *Id.* The Maryland Committee noted that the Maryland Rules of Professional Conduct do not include Model Rule 4.4(b). *See Id.*

[189] *Id.*

[190] The Maryland Rule comports with ABA Model Rule 1.1, which provides:

> 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); *see* MD. RULES OF PROF'L CONDUCT R. 1.1 (2005).

[191] *See* MODEL RULES OF PROF'L CONDUCT R. 1.6(b) (2004). The Maryland Rule permits a lawyer to reveal information likely to result in substantial injury to the financial interest or property of another, and also permits revelation when the client's act is not only fraudulent, but criminal. *See* MD. RULES OF PROF'L CONDUCT R. 1.6 (2004).

[192] Md. Ethics Op. 2007-09, *supra* note 177.

[193] Fed. R. Civ. P. 16(b) was amended "to alert the court to the possible need to address the handling of discovery of electronically stored information early in the litigation if discovery is expected to occur" and "to include among the topics that may be addressed . . . any agreements that the parties reach to facilitate discovery by minimizing the risk of waiver of privilege or work-product protection." FED. R. CIV. P. 16 advisory committee's note (2006). Addressing the contents of the Scheduling Order which the judge must make, Rule 16(b) states that it may "provide for disclosure or discovery of electronically stored information" and "include any agreements the parties reach for asserting claims of privilege or of protection as trial-preparation material after information is produced." FED. R. CIV. P. 16(b)(3)(B)(iii)-(iv).

Amendments to Fed. R. Civ. P. 26(f) were made "to direct parties to discuss discovery of electronically stored information during their discovery-planning conference," hoping to "avoid later difficulties" and "make discovery more efficient." FED. R. CIV. P. 26 advisory committee's note (2006). Aware that "discovery difficulties can result from efforts to guard against waiver of privilege and work-product protection," the amendments also suggest that

rules, a joint bar-court committee in Maryland was formed, which developed a proposed protocol for use in cases which might involve ESI.[194] The purpose of

these issues be discussed. *Id.* Included in the discovery plan which the parties are instructed to make must be "any issues about disclosure or discovery of electronically stored information, including the form or forms in which it should be produced" and "any issues about claims of privilege or of protection as trial-preparation materials, including-if the parties agree on a procedure to assert these claims after production-whether to ask the court to include their agreement in an order." FED. R. CIV. P. 26(f)(3)(C)&(D).

Fed. R.Civ. P. 34(a) was amended "to confirm that discovery of electronically stored information stands on equal footing with discovery of paper documents." FED. R. CIV. P. 34 advisory committee's note (2006). It provides in part as follows:

> (a) In General. A party may serve on any other party a request within the scope of Rule 26(b):
>
> (1) to produce and permit the requesting party or its representative to inspect, copy, test or sample the following items in the responding party's possession, custody, or control:
>
> (A) any designated documents or electronically stored information-including writings, drawings, graphs, charts, photographs, sound recordings, images and other data or data compilations-stored in any medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form;

FED. R. CIV. P. 34(a)(1)(A). The rule "is intended to be broad enough to cover all current types of computer-based information, and flexible enough to encompass future changes and developments." FED. R. CIV. P. 34 advisory committee's note (2006). Fed. R. Civ. P. 33(d) was amended to parallel Rule 34(a) "by recognizing the importance of electronically stored information." FED. R. CIV. P. 33 advisory committee's note (2006).

Addressing FED. R. CIV. P. 34(b), the advisory committee stated that the rule:

> permits the requesting party to designate the form or forms in which it wants electronically stored information produced . . . . In the written response to the production request that Rule 34 requires, the responding party must state the form it intends to use for producing electronically stored information if the requesting party does not specify a form or if the responding party objects to a form that the requesting party specifies . . . . The rule does not require a party to produce electronically stored information in the form in which it is ordinarily maintained, as long as it is produced in a reasonably usable form.

FED. R. CIV. P. 34 advisory committee's note (2006).

The 2006 amendments to the Federal Rules of Civil Procedure also acknowledged that "the routine alteration and deletion of information that attends ordinary use . . . may alter or destroy information, for reasons that have nothing to do with how that information might relate to litigation." FED. R. CIV. P. 37 advisory committee notes (2006). Therefore, a new rule was added which provides as follows:

> Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system.

FED. R. CIV. P. 37 (e). *See infra* notes 213-14 and accompanying text.

[194] *See* Suggested Protocol for Discovery of Electronically Stored Information ("ESI") §

the proposed protocol is "to facilitate the just, speedy and inexpensive conduct of discovery involving ESI in civil cases, and to promote, wherever possible, the resolution of disputes regarding the discovery of ESI without court intervention."[195]

The proposed protocol states that whether or not ordered by the court, parties should conduct a conference to discuss discovery of ESI and report the results of the conference to the court.[196] Before the Fed. R. Civ. P. 26(f) Conference of Parties, counsel should discuss the exchange of information about ESI and advise their respective clients of "substantive principles governing the preservation of relevant or discoverable ESI while the lawsuit is pending,"[197] including "the extent to which Meta-Data, deleted data, or fragmented data, will be subject to litigation hold."[198] At the Conference of Parties, the scope, objections and form of production of ESI should be discussed. [199] If meta-data is to be produced, "[p]ost-production assertion, and preservation or waiver of, the attorney-client privilege, work product doctrine, and other privileges . . ." should be discussed, as well as "procedures under which ESI that contains privileged information or attorney work product should be immediately returned to the Producing Party if the ESI appears on its face to have been inadvertently produced or if there is prompt written notice of inadvertent production by the Producing Party."[200] As to the discoverability of metadata, the proposed protocol sets forth the following principles:

A. Meta-Data is part of ESI . . . .

1, *available at* www.mdd.uscourts.gov/localrules/localrules.html. The suggested protocol "is a working model that has not been adopted by the court but may be of assistance to counsel." *Id.*

[195] *Id*. at 3.

[196] *Id*. at 4.

[197] *Id*. at 8.

[198] *Id*. at 9. "[W]here Meta-Data, or data that has been deleted but not purged, is to be preserved," there should be instructions in the litigation hold notice regarding a method to preserve such data. *Id.* at 11.

[199] *Id.* at 17. Included in the discussion should be whether production will be in Native File or Static Image format. "'Native File' means ESI in the electric format of the application in which such ESI is normally created, viewed and/or modified." *Id.* at 4. "'Static Image' means a representation of ESI produced by converting a Native File into a standard image capable of being viewed and printed on standard computer systems." *Id.* Any party wanting to redact contents of a Native File for privilege should indicate that fact, but retain an original, unmodified file during the pendency of the case. *Id*. at 18. Also, the volume and cost of metadata production and review should be discussed. *Id.* at 19.

[200] *Id.* at 20. The Proposed Protocol notes that "[t]his provision is procedural and return of materials pursuant to this Protocol is without prejudice to any substantive right to assert, or oppose, waiver of any protection against disclosure." *Id.*

> B. Meta-Data may generally be viewed as either System Meta-Data, Substantive Meta-Data, or Embedded Meta-Data . . . . System Meta-Data is less likely to involve issues of work product and/or privilege.
>
> C. . . . Meta-Data, especially substantive Meta-Data, need not be routinely produced, except upon agreement of the requesting and producing litigants, or upon a showing of good cause in a motion filed by the Requesting Party . . . .
>
> D. If a Producing Party produces ESI without some or all of the Meta-Data that was contained in the ESI, the Producing Party should inform all other parties of this fact . . . .
>
> E. Embedded Meta-Data is generally discoverable and in appropriate cases . . . should be produced as a matter of course . . . .[201]

Not addressed are substantive issues related to metadata, such as a duty to preserve meta-data, its authenticity or its admissibility.[202]

2. Alabama

The Disciplinary Commission in Alabama was next to consider the matter of metadata in an ethics opinion. They raised the following questions:

> 1. Does an attorney have an affirmative duty to take reasonable precautions to ensure that confidential metadata is properly protected from inadvertent or inappropriate production via an electronic document before it is transmitted?
>
> 2. Is it unethical for an attorney to mine metadata from an electronic document he or she received from another party?[203]

The Alabama Commission gave both inquiries an affirmative response. As to the first question, the Commission based its answer on a lawyer's duty under Rule 1.6.[204]

---

[201] *Id.* at 12. Mindful of the cost that may be involved in removing metadata, the Principles also state that "upon agreement of the parties, the Court will consider entry of an order approving an agreement that a party may produce Meta-Data in Native Files upon the representation of the recipient that the recipient will neither access nor review such data." *Id.* at 27.

[202] *Id.*

[203] Ala. Ethics Op. 2007-02, *supra* note 180.

[204] *Id.* Alabama Rule 1.6(a) follows the ABA Model Rule, which provides that "[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).

Calling for the exercise of reasonable care in taking reasonable precautions, the Commission noted that these "will, of course, vary according to the circumstances of each individual case."[205] Factors to be considered may include "steps taken by the attorney to prevent the disclosure of metadata, the nature and scope of the metadata revealed, the subject matter of the document, and the intended recipient."[206]

As to the second question, the Alabama Commission aligned its affirmative response with that of the New York position, finding "[a]bsent express authorization from a court, it is ethically impermissible for an attorney to mine metadata from an electronic document he or she inadvertently or improperly receives from another party."[207] However, the Commission distinguished situations involving electronic discovery, noting "that parties may be sanctioned for failing to provide metadata along with electronic discovery

---

[205] Ala. Ethics Op. 2007-02, *supra* note 180.

[206] *Id*. The Commission noted an attorney would need to exercise greater care when submitting documents to an opposing party than filing a pleading with a court: "[t]here is simply a much higher likelihood that an adverse party would attempt to mine metadata, than a neutral and detached court." *Id*. However, it has been noted that "[i]t is not just the opposing party with whom one shares an electronic document who can get access to a party's MS Word documents." Brian D. Zall, *Metadata: Hidden Information in Microsoft Word Documents and Its Ethical Implications*, 33 COLO. LAW. 53, 55 (2004). For instance, in the statewide electronic filing system of the Colorado State Courts, anyone with an account with the LexisNexis File & Serve service can access an original MS Word document, including metadata, when the MS Word document is uploaded to the Courts' website for conversion to PDF format. *Id*.

[207] Ala. Ethics Op. 2007-02, *supra* note 180. The Commission determined that the unauthorized mining of metadata to uncover confidential information would violate Rule 8.4, Misconduct, of the Alabama Rules of Professional Conduct, which provides:

> It is professional misconduct for a lawyer to:
>
> (a) Violate or attempt to violate the Rules of Professional Conduct, knowingly assist or induce another to do so, or do so through the acts of another;
> (b) Commit a criminal act that reflects adversely on the lawyer's honesty, trustworthiness or fitness as a lawyer in other respects;
> (c) Engage in conduct involving dishonesty, fraud, deceit or misrepresentation;
> (d) Engage in conduct that is prejudicial to the administration of justice;
> (e) State or imply an ability to influence improperly a government agency or official;
> (f) Knowingly assist a judge or judicial officer in conduct that is a violation of applicable Canons of Judicial Ethics or other law; or
> (g) Engage in any other conduct that adversely reflects on his fitness to practice law.

ALA. RULES OF PROF'L CONDUCT R. 8.4 (2008). The Model Rules of Professional Conduct are similar, but not identical, to Alabama Rule 8.4. Also, the Model Rule does not have Rule 8.4(g). *See* MODEL RULES OF PROF'L CONDUCT R. 8.4 (2009).

submissions."[208] The Commission cautioned that parties to litigation should seek direction from the court on whether to produce metadata during discovery.[209]

3. District of Columbia

When the District of Columbia Bar addressed metadata in electronic documents, it too distinguished "between electronic documents provided in discovery or pursuant to a subpoena from those electronic documents voluntarily provided by opposing counsel."[210] The D.C. Bar Legal Ethics Committee considered the metadata issue in a bifurcated fashion, analyzing the responsibilities of lawyers who send and receive electronic documents during discovery, separately from those who send and receive electronic documents outside the discovery context.

---

[208] Ala. Ethics Op. 2007-02, *supra* note 180. In support for this position, the Commission cited a case from Kansas and a case from Ohio. In the Kansas case, the defendant was ordered to disclose electronic documents in the form in which they were maintained. However, before providing the documents, the defendant scrubbed metadata from documents, allegedly to preclude the recovery of privileged and protected information. Defendant also locked data within spreadsheet cells before providing them to plaintiffs, allegedly to limit information in the spread sheets to that which was relevant to the underlying issues. Williams v. Sprint/United Mgnt Co., 230 F.R.D. 640, 646-47 (D. Kan. 2005). Regarding metadata, based on "emerging standards," the court in Kansas stated the following:

> [W]hen a party is ordered to produce electronic documents as they are maintained in the ordinary course of business, the producing party should produce the electronic documents with their metadata intact, unless that party timely objects to production of metadata, the parties agree that the metadata should not be produced, or the producing party requests a protective order. The initial burden with regard to the disclosure of metadata would therefore be placed on the party to whom the request or order to produce is directed. The burden to object to the disclosure of metadata is appropriately placed on the party ordered to produce its electronic documents as they are ordinarily maintained because that party already has access to the metadata and is in the best position to determine whether producing it is objectionable. Placing the burden on the producing party is further supported by the fact that metadata is an inherent part of an electric document, and its removal ordinarily requires an affirmative act by the producing party that alters the electronic document. (footnotes omitted)

Id. at 652. In the Ohio case, where plaintiffs sought sanctions for discovery abuse, among which was missing metadata, the court noted that in discovery, "people aren't allowed to go on a fishing expedition and at the same time they are certainly allowed to have material that may lead to relevant material." *In re* Telxon Corp. Sec. Litg., 2004 WL 3192729 *27 (N.D. Ohio 2004). Taking up on plaintiffs' suggestion that defendant withheld, or "improperly destroyed discoverable information," the court entered default judgment on liability issues against the defendant. *Id*. at *34-36.

[209] *See* Ala. Ethics Op. 2007-02, *supra* note 180.

[210] D.C. Bar Legal Ethics Comm., *supra* note 184.

Outside the context of discovery, the D.C. Bar Legal Ethics Committee sided with the generally held position on a sending lawyer's responsibilities.[211] According to the D.C. Bar Legal Ethics Committee, under Rule 1.6, a sending lawyer is obligated to take reasonable steps to maintain the confidentiality of documents, which "includes taking care to avoid providing electronic documents that inadvertently contain accessible information that is either a confidence or a secret" and "to employ reasonably available technical means to remove such metadata before sending the document."[212] However, the D.C. Bar Legal Ethics Committee took a different stance when it addressed the receiving lawyer's duty in a non-discovery context. While generally agreeing with New York and Alabama's position that Rule 8.4(c) is "implicated when a receiving lawyer wrongfully 'mines' an opponent's metadata," the D.C. Bar Legal Ethics Committee posited that "Rule 8.4 is implicated only when the receiving lawyer has an actual prior knowledge that the metadata was inadvertently provided."[213] Since the sending lawyer is obligated to avoid inadvertent production of metadata, "mere uncertainty by the receiving lawyer as to the inadvertence of the sender does not trigger an ethical obligation by the receiving lawyer to refrain from reviewing metadata."[214] Only when the receiving lawyer has actual knowledge that metadata was inadvertently sent is its review prohibited. According to the D.C. Bar Legal Ethics Committee, in this situation, "the receiving lawyer's duty of honesty requires that he refrain from reviewing the metadata until he has consulted with the sending lawyer to determine whether the metadata includes privileged or confidential information."[215]

With respect to electronic documents provided in discovery, the D.C. Bar Legal Ethics Committee noted that the Federal Rules of Civil Procedure provide steps to identify and address issues related to electronic discovery:

[P]arties are required to consult at the outset of a case about the nature of

---

[211] *Id.*

[212] *Id.* District of Columbia Rule 1.6(c)(2) permits a lawyer to reveal client confidences "to prevent the bribery or intimidation of witnesses, jurors, court officials, or other persons who are involved in proceedings before a tribunal if the lawyer reasonably believes" such acts will likely occur without revelation. Rule 1.6(h) applies the obligation of the Rule "to confidences and secrets learned prior to becoming a lawyer in the course of providing assistance to another lawyer." D.C. RULES OF PROF'L CONDUCT R. 1.6 (2004).

[213] D.C. Bar Legal Ethics Comm., *supra* note 184. District of Columbia Rule 8.4(c) follows the ABA Model Rule.

[214] D.C. Bar Legal Ethics Comm., *supra* note 184.

[215] *Id.* The opinion suggests that if the sending lawyer advises the receiving lawyer that "protected information is included in the metadata, then the receiving lawyer should comply with the instructions of the sender. The receiving lawyer may, however, reserve the right to challenge the claim of privilege and obtain an adjudication, where appropriate." *Id.*

> pertinent electronic documents in their possession and the manner in which they are maintained. This should include specific discussions as to whether a receiving lawyer wants to obtain the metadata, and if so, whether the sending party wishes to assert a claim of privilege as to some or all of the metadata.[216]

Focusing on applicable District of Columbia rules, the D.C. Bar Legal Ethics Committee noted that a lawyer shall not "obstruct another party's access to evidence or alter, destroy or assist another person to do so, if the lawyer reasonably should know that the evidence is or may be the subject of discovery or subpoena in any pending or imminent proceeding."[217] As far as the sending lawyer is concerned, "[b]ecause it is impermissible to alter electronic documents that constitute tangible evidence, the removal of metadata may, at least in some instances, be prohibited," leading to discovery sanctions and may under some circumstances constitute a crime.[218]

Looking next to the receiving lawyer, the D.C. Bar Legal Ethics Committee stated that "a receiving lawyer is generally justified in assuming that metadata was provided intentionally."[219] In fact, "when an electronic document constitutes tangible evidence, or potential tangible evidence, the receiving lawyer has an obligation competently and diligently to review, use and preserve the evidence."[220] It is only when the receiving lawyer has "actual knowledge that metadata containing protected information was inadvertently sent by the sending lawyer," that the metadata should not be reviewed "without first consulting with the sender and abiding by the sender's instructions."[221]

---

[216] *Id.* Federal Rule of Civil Procedure 26(b)(5)(B) also has a provision for "clawing back" a privileged document provided during discovery:

> If information is produced in discovery that is subject to a claim of privilege or of protection as trial-preparation material, the party making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has and may not use or disclose the information until the claim is resolved. A retrieving party may promptly present the information to the court under seal for a determination of the claim. If the receiving party disclosed the information before being notified, it must take reasonable steps to retrieve it. The producing party must preserve the information until the claim is resolved.

FED. R. CIV. P. 26(b)(5)(B).

[217] D.C. Bar Legal Ethics Comm., *supra* note 184 (citing D. C. RULES OF PROF'L CONDUCT R. 3.4(a)).

[218] *Id.* (citing D.C. RULES OF PROF'L CONDUCT R. 3.4 cmt. 4).

[219] *Id.*

[220] *Id.* Using an analogy to a fingerprint expert, the D.C. Bar Legal Ethics Committee notes that a lawyer "may consult with a computer expert to determine the means by which the metadata can be most fully revealed." *Id.*

[221] *Id.* The D.C. Bar Legal Ethics Committee notes that in such a situation "the receiving

4. Arizona

In November 2007, the Committee on the Rules of Professional Conduct of the State Bar of Arizona issued a *sua sponte* opinion on the metadata issue, "[g]iven the importance of the subject matter."[222] Identifying the relevant ethical rules as Rule 1.6(a),[223] Rule 4.4(b)[224] and Rule 8.4(a)-(d),[225] the Arizona Committee noted that when transmitting a communication, the sending lawyer "must take reasonable precautions to prevent the information from coming into the hands of unintended recipients."[226] Cautioning lawyers about the inclusion of comments on documents that are ultimately intended for transmission to opposing counsel, the Committee directed lawyers to use documents in '"clean' form and not a document that was used for another client."[227] Considering documents in litigation as a separate matter, the Arizona Committee stated that when "removing or restricting access to metadata," sending lawyers "must take care not to violate any duty of disclosure to which the lawyer or the lawyer's client is subject."[228]

When assessing the duty of a receiving lawyer, the Arizona Committee

lawyer is permitted to take protective measures to ensure that potential evidence is not destroyed and to preserve the right to challenge the claim that the information is privileged or otherwise not subject to discovery and obtain an adjudication on that point." *Id.*

[222] Ariz. State Bar Comm. on Rules of Prof'l Conduct, Ethics Op. 07-03 (2007), http://www.myazbar.org/Ethics/opinionview.cfm?id=695.

[223] ARIZ. RULES OF PROF'L CONDUCT R. 1.6(a) (2004) (following the ABA Model Rule). However, the Arizona Rule permits a lawyer to reveal the intention of a client to commit a crime and Rule 1.6(d)(5) applies only to "other law or a final order of a court or tribunal of competent jurisdiction directing the lawyer to disclose such information." *Compare id. with* MODEL RULES OF PROF'L CONDUCT R. 1.6(a) (2003).

[224] ARIZ. RULES OF PROF'L CONDUCT R. 4.4(b) (2004) (Arizona Rule 4.4(b) differs from the corresponding ABA Model Rule, in that it imposes an additional requirement on the lawyer who receives the inadvertently sent document to "preserve the status quo for a reasonable period of time in order to permit the sender to take protective measures."); *see* MODEL RULES OF PROF'L CONDUCT R. 4.4(b) (2003).

[225] ARIZ. RULES OF PROF'L CONDUCT R. 8.4 (following the ABA Model Rule). *Compare id. with* MODEL RULES OF PROF'L CONDUCT R. 8.4 (2009).

[226] Ariz. Ethics Op. 07-03, *supra* note 179 (citing ARIZ. R. PROF'L CONDUCT R. 1.6 cmt. 2). The Committee stated that what is '"reasonable' in the circumstances depends on the sensitivity of the information, the potential consequences of its inadvertent disclosure, whether further disclosure is restricted by statute, protective order, or confidentiality agreement, and any special instructions given by the client." *Id.*

[227] *Id.* The Committee further noted that sending lawyers should also "be aware that the electronic document may be received or distributed to a person who is not a lawyer and who therefore does not have the duties of a recipient lawyer with respect to such document." *Id.*

[228] *Id.* Effective January 1, 2008, the Arizona Rules of Civil Procedure include provisions relating to discovery and disclosure of ESI. *Id.*

noted that it "respectfully decline[d] to follow the ABA position" that a receiving lawyer is free to review and use embedded information contained in electronic documents.[229] Since "it may not be possible for the sending lawyer to be absolutely certain that all of the potentially harmful metadata has been 'scrubbed' from the document before it is transmitted electronically . . . the sending lawyer would be at the mercy of the recipient lawyer" should the ABA position be followed.[230] Instead, "reminded of the duty to take reasonable steps to prevent the inadvertent disclosure of confidential or privileged information . . . the recipient lawyer has a corresponding duty not to 'mine' the document for metadata that may be embedded therein."[231]

Just as the ABA looked to Rule 4.4(b) when analyzing this matter,[232] so did the Arizona Committee. However, Arizona's Rule 4.4(b) places a burden beyond mere notice to a sending lawyer that an inadvertent document was received. Under the Arizona Rule, a lawyer who receives an inadvertent document also must "preserve its status quo for a reasonable period of time in order to permit the sender to take protective measures."[233] The Committee points out, however, that it "expresses no opinion on whether any evidentiary privilege continues to exist once an inadvertent disclosure has occurred, or whether the lawyer has incurred civil liability as a result of such disclosure."[234]

5. Pennsylvania

The Pennsylvania Bar Association Committee on Legal Ethics and Professional Responsibility considered the matter of metadata in 2007, undertaking a review of the positions embraced by the bars in the various states.[235] Commenting that each of the different conclusions reached by the various states offered "a persuasive rationale," the Committee opined that it was "difficult to establish a rule applicable in all circumstances."[236] Therefore,

---

[229] *Id.; see supra* note 154 and accompanying text.

[230] Ariz. Ethics Op. 07-03, *supra* note 179.

[231] *Id*. The receiving lawyer is also cautioned not to "otherwise engage in conduct which amounts to an unjustified intrusion into the client-lawyer relationship that exists between the opposing party and his or her counsel." *Id.* However, "[a] lawyer who receives an electronic communication may attempt to discover the metadata that is embedded therein if he or she has the consent of the sender, or if such conduct is allowed by a rule, order, or procedure of a court or other applicable provision of law." *Id.*

[232] *See* MODEL RULES OF PROF'L CONDUCT 4.4(b) (2009).

[233] ARIZ. RULES OF PROF'L CONDUCT R. 4.4(b) (2004).

[234] Ariz. Ethics Op. 07-03, *supra* note 179.

[235] Due to the timing of the opinions, Arizona Ethics Op. 07-03 was not considered by the Pennsylvania Committee in 2007. *See* Pa. Bar Ass'n Comm. On Legal Ethics & Prof'l Resp. Formal Op. 2007-500 (2007).

[236] *Id*.

the Pennsylvania Committee took the position that "the final determination of how to address the inadvertent disclosure of metadata should be left to the individual attorney and his or her analysis of the applicable facts."[237]

The Pennsylvania Committee noted that there is no specific rule in Pennsylvania relating to inadvertently transmitted metadata, although the Committee considered Rules 1.6(a)[238] and 4.4(b),[239] along with selected commentary, in its analysis.[240] Noting that the "utilization of metadata by attorneys receiving electronic documents from an adverse party is an emerging problem," the Committee ultimately concluded that many factors will be involved in analyzing "the decision of how or whether a lawyer may use the information contained in metadata."[241] Included in those factors are the following:

- The judgment of the lawyer;

- The particular facts applicable to the situation;

- The lawyer's view of his or her obligations to the client under Rule of Professional Conduct 1.3, and the relevant Comments to this Rule;

- The nature of the information received;

- How and from whom the information was received;

- Attorney-client privilege and work product rules; and,

- Common sense, reciprocity and professional courtesy.[242]

---

[237] *Id.*

[238] *See* MODEL RULES OF PROF'L CONDUCT R. 1.6(a) (2003). Pennsylvania Rule 1.6(a) follows the Model Rule language. *See* 42 PA. CONS. STAT. ANN. § 1.6(a) (2008).

[239] *See* MODEL RULES OF PROF'L CONDUCT R. 4.4(b) (2009). Pennsylvania Rule 4.4(b). follows the Model Rule language. *See* 42 PA. CONS. STAT. ANN. § 4.4(b) (2008).

[240] Pa. Bar Ass'n Comm. on Legal Ethics & Prof'l Resp. Op. 2007-500 (2007).

[241] *Id.* The Committee noted that "[a]lthough a transmitting attorney has tools at his disposal that can minimize the amount of metadata contained in a document he or she is transmitting, those tools still may not remove all metadata." *Id.* For "metadata does not disappear with the click of a button." Daniel J. Siegel, *Scrub Your Documents! Removing Metadata Before E-mailing Can Help Maintain Client Confidences*, 68 THE PHILADELPHIA LAWYER 56, 57 (Fall 2005). It is suggested that lawyers should establish policies that address "under what circumstances electronic files may be sent to other counsel." *Id.* Should the transmission of electronic documents be approved, lawyers "should establish a procedure that assures that metadata is removed before a file is sent to opposing counsel or others, including the media." *Id.*

[242] Pa. Bar Ass'n Comm. on Legal Ethics & Prof'l Resp. Op. 2007-500 (2007) (footnotes omitted). Pennsylvania Rule 1.3 follows Model Rule 1.3, which states that "[a] lawyer shall act with reasonable diligence and promptness in representing a client." MODEL RULES OF

Although recognizing that waiver of attorney-client privilege is a matter for judicial determination, the Pennsylvania Committee stated that "the inadvertent transmissions of such materials should not constitute a waiver of the privilege, except in the case of extreme carelessness or indifference."[243]

In 2009, The Pennsylvania Committee revisited its 2007 position on metadata, stating that its 2007 opinion "provided insufficient guidance to recipients of documents containing metadata and did not provide correlative guidance to attorneys who send such documents."[244] With respect to the sending lawyer, the Pennsylvania Committee looked to Rules 1.1[245] and 1.6,[246] and their commentary, noting that "[c]ompetence includes the knowledge and skill to secure appropriate protection for documents to ensure that information that would negatively affect the client's case is not provided to an opposing party by any means, including by inadvertently embedded metadata."[247] Recognizing that the primary burden of keeping client confidences lies with the sending lawyer, the committee reiterated that "an attorney sending electronic materials has a duty of reasonable care to remove unwanted metadata."[248]

When addressing the duties of the receiving lawyer, the Pennsylvania Committee stated that Rule 4.4(b)[249] "requires that a lawyer accessing metadata evaluate whether the extra-textual information was intended to be deleted or scrubbed from the document prior to transmittal."[250] The result of this evaluation "determines the course of action required."[251] If metadata is inadvertently sent, Rule 4.4(b) calls for the sender to be promptly notified.[252]

PROF'L CONDUCT R. 1.3 (2009).

[243] Pa. Ethics Op. 2007-500 (2007).

[244] Pa. Bar Ass'n Comm. on Legal Ethics & Prof'l Resp. Op. 2009-100 n.3 (2009).

[245] *See* MODEL RULES OF PROF'L CONDUCT R. 1.1 (2009). Pennsylvania Rule 1.1 follows the ABA Model Rule. PA. CONS. STAT. ANN. § 1.1 (Comm. On Legal Ethics 2008).

[246] *See* MODEL RULES OF PROF'L CONDUCT R. 1.6 (2003). Pennsylvania adds a Rule 1.6(d) which states that "[t]he duty not to reveal information relating to representation of a client continues after the client-lawyer relationship has terminated." 42 PA. CONS. STAT. ANN. § 1.6(d) (2008). Also, a lawyer may reveal information relating to the representation of a client that the lawyer reasonably believes necessary to "effectuate the sale of a law practice consistent with Rule 1.17." *Id.* at § 1.6(c)(6).

[247] Pa. Bar Ass'n Comm. on Legal Ethics & Prof'l Resp. Op. 2009-100 n.3 (2009).

[248] *Id.*

[249] *See* MODEL RULE OF PROF'L CONDUCT R. 4.4(b) (2003); *see also supra* text accompanying note 144.

[250] Pa. Bar Ass'n Comm. on Legal Ethics & Prof'l Resp. Op. 2009-100 (2009).

[251] *Id.*

[252] *Id.; see* MODEL RULE OF PROF'L CONDUCT R. 4.4(b) (2009); *see also supra* text accompanying note 144.

Focusing on the lawyer's duty to the lawyer's client, competent representation of the client under Rule 1.1 calls for the lawyer first to determine:

> whether the tribunal in which the matter is or will be proceeding may find an impropriety in the review or use of inadvertently transmitted metadata, or whether its use may unduly impact future dealings with opposing counsel, resulting in adverse consequences to the client. In such an instance, competent representation may require that the attorney refrain from disclosing or using the information. Conversely, if the inadvertently received material is beneficial to the client's case and can be viewed and/or used without adverse consequences, then Rule 1.1 may require that the attorney do so.[253]

Pursuant to Rule 1.4[254] on communication, "a lawyer has an obligation to keep the client fully appraised of important developments in the client's case so that the client may make informed decisions concerning the representation."[255] One such important event could be "potentially useful metadata."[256] Lawyers have a duty to advise their clients and respect a client's authority to control the objectives of the representation.[257] Even if the attorney judges the metadata is

---

[253] Pa. Bar Ass'n Comm. on Legal Ethics & Prof'l Resp. Op. 2009-100 (2009).

[254] The Pennsylvania rule on communication comports with Model Rule 1.4 Communication, which provides that:

> (a) A lawyer shall:
>
> (1) promptly inform the client of any decision or circumstance with respect to which the client's informed consent, as defined in Rule 1.0(e), is required by these Rules;
>
> (2) reasonably consult with the client about the means by which the client's objectives are to be accomplished;
>
> (3) keep the client reasonably informed about the status of the matter;
>
> (4) promptly comply with reasonable requests for information; and
>
> (5) consult with the client about any relevant limitation on the lawyer's conduct when the lawyer knows that the client expects assistance not permitted by the Rules of Professional Conduct or other law.
>
> (b) A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation.

MODEL RULES OF PROF'L CONDUCT R. 1.4 (2009).

[255] Pa. Bar Ass'n Comm. on Legal Ethics & Prof'l Resp. Op. 2009-100 (2009).

[256] *Id.*

[257] *Id.* The committee references a lawyer's duty "to respect the client's authority to control the objectives and means of pursuit under Rule 1.2." The Pennsylvania Rule comports with Model Rule 1.2, Scope of Representation and Allocation of Authority between Lawyer and Client, which provides in part as follows:

> (a) . . . a lawyer shall abide by a client's decision concerning the objectives of representation and, as required by Rule 1.4, shall consult with the client as to the

not useful to the client's case, "there will in most instances remain a duty to advise the client of the receipt of the metadata and the reason for nondisclosure."[258]

Continuing to focus on the duty of lawyers to their clients, the Pennsylvania Committee posited that "the lawyer's duty to the lawyer's own client trumps any theoretical responsibility to protect the right of confidentiality as between another lawyer and that lawyer's client."[259] As a general premise, a lawyer who receives inadvertently transmitted information, may "examine and use the metadata for the client's benefit without violating the [Rules of Professional Conduct]."[260] However, the receiving lawyer must determine whether the metadata can be used as a matter of substantive law; consider the potential effect on the client if the metadata is used; and consult with the client about the appropriate course of action.[261]

6. Colorado

The Ethics Committee of the Colorado Bar Association issued an opinion addressing metadata, setting forth obligations of sending and receiving lawyers who transmit electronic documents.[262] As an initial premise, the Colorado Committee asserted that "[t]he ultimate responsibility for control of metadata rests with the lawyers who send the electronic documents."[263]

Regarding Rule 1.6(a),[264] Rule 1.1,[265] and Rules 5.1 and 5.3,[266] the

> means by which they are to be pursued. A lawyer may take such action on behalf of the client as is impliedly authorized to carry out the representation.

MODEL RULES OF PROF'L CONDUCT R. 1.2(a) (2009).

[258] Pa. Bar Ass'n Comm. on Legal Ethics & Prof'l Resp. Op. 2009-100 (2009).

[259] *Id.*

[260] *Id.*

[261] *Id.*

[262] *See* Colo. Bar Ass'n Ethics Comm., Formal Op. 119 (2007).

[263] *Id.*

[264] *See* MODEL RULES OF PROF'L CONDUCT R. 1.6(a) (2009). Generally speaking, the Colorado Rules of Professional Conduct follow the ABA Model Rules and Colorado's Rule 1.6(a) comports with the ABA Model Rule. COLO. RULES OF PROF'L CONDUCT R. 1.6 (2008). *But see infra* note 284, and accompanying text.

[265] See MODEL RULES OF PROF'L CONDUCT R. 1.1 (2009).

[266] Colorado Rules of Professional Conduct 5.1 and 5.3 follow the ABA Model Rules. Rule 5.1 requires that lawyers with managerial authority in law firms and associations "make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that all lawyers in the firm conform to the Rules of Professional Conduct." MODEL RULES OF PROF'L CONDUCT R. 5.1(a) (2003). Rule 5.3 requires that lawyers with managerial authority "make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that [the conduct of nonlawyers employed by, retained by, or

Committee noted that:

> [A] Sending Lawyer must act competently to avoid revealing a client's Confidential Information, and to ensure that others at the Sending Lawyer's firm similarly avoid revealing a client's Confidential Information. This requires a Sending Lawyer to use reasonable care to ensure that metadata that contain Confidential Information are not disclosed to a third party.[267]

The obligations of the receiving lawyer are addressed by the Colorado Committee as two distinct issues, the initial issue being whether it is ethical for a receiving lawyer to review metadata.[268] To this inquiry the Colorado Committee gave an affirmative response. Siding with the positions taken by the ABA,[269] Maryland[270] and the District of Columbia,[271] rather than those of New York,[272] Arizona,[273] Alabama[274] and Florida,[275] the Colorado Committee concluded that generally, a receiving lawyer "may ethically search for and review metadata embedded in an electronic document that the Receiving Lawyer receives from opposing counsel or other third party."[276] The Colorado Committee arrived at this decision for three primary reasons. First, it opined that "there is nothing inherently deceitful or surreptitious about searching for metadata," so "[r]eferring to searching for metadata as 'mining' or

associated with a lawyer] is compatible with the professional obligations of the lawyer." MODEL RULES OF PROF'L CONDUCT R. 5.3(a) (2003). Pursuant to these rules, the Colorado Committee notes that "[a] supervising lawyer has a duty to make reasonable efforts to make sure that the lawyer's firm has appropriate technology and systems in place so that subordinate lawyers and nonlawyer assistants can control transmission of metadata." Colo. Ethics Op. 119, *supra* note 178.

[267] Colo. Bar Ass'n Ethics Comm., Formal Op. 119 (2007). What would constitute "reasonable care will depend on the facts and circumstances." *Id*. However, "[t]he duty to provide competent representation requires a lawyer to ensure that he or she is reasonably informed about the types of metadata that may be included in an electronic document or file and the steps that can be taken to remove metadata . . . ." *Id*.

[268] *Id*.

[269] *See* ABA Comm. on Ethics and Prof'l Responsibility Formal Op. 06-442 (2006) (Review and Use of Metadata).

[270] *See* Comm. on Ethics of Md. State Bar Ass'n Op. 2007-09 (2007).

[271] *See* D. C. Bar Ethics Op. 341 (2007).

[272] *See* N. Y. State Bar Ass'n Op. 749 (Dec. 14, 2001); N. Y. State Bar Ass'n Op. 782 (Dec. 8, 2004).

[273] *See* Ariz. State Bar Comm. on Rules of Prof'l Conduct Op. 07-03 (2007).

[274] *See* Ala. Office of Gen. Counsel, Ethics Op. 2007-02 (2007).

[275] *See* Fla. Bar Op. 06-02 (Sept. 15, 2006).

[276] Colo. Bar Ass'n Ethics Comm., Formal Op. 119 (2007).

'surreptitiously get[ting] behind' a document is, therefore, misleading."[277] Second, in many cases there is no confidential information in metadata. Third, "metadata [is] often of no import."[278]

The second issue the Colorado Committee considered was the appropriate response for a lawyer receiving metadata that appears to contain confidential information. In such a situation, the Colorado Committee indicated that the receiving lawyer "should assume that the Confidential Information was transmitted inadvertently."[279] The Colorado Committee stated that the receiving lawyer "must promptly notify the Sending Lawyer," and the lawyers may "discuss whether a waiver of privilege or confidentiality has occurred."[280] However, the "Receiving Lawyer's only duty upon viewing confidential metadata is to notify the Sending Lawyer. There is no rule that prohibits the Receiving Lawyer from continuing to review the electronic document or file and its associated metadata."[281] In contrast, in situations "where the Receiving Lawyer has prior notice from the sender of the inadvertent transmission of confidential metadata," the lawyer is prohibited from reviewing the material.[282] Rule 4.4(c) of the Colorado Rules is controlling, and provides:

> Unless otherwise permitted by court order, a lawyer who receives a document relating to the representation of the lawyer's client and who, before reviewing the document, receives notice from the sender that the document was inadvertently sent, shall not examine the document and shall abide by the sender's instructions as to its disposition.[283]

There is no comparable Model Rule to this provision.

---

[277] *Id.*

[278] *Id.*

[279] *Id.* This is the case, "unless the Receiving Lawyer knows that confidentiality has been waived." *Id.*

[280] *Id.* "If this is not possible, then the Sending Lawyer or the Receiving Lawyer may seek a determination from a court or other tribunal as to the proper disposition of the electronic documents or files, based on the substantive law or waiver." *Id.*

[281] *Id.* The Colorado Committee disagrees with the approach taken by the District of Columbia Committee, that a receiving lawyer must stop reviewing an electronic document when the receiving lawyer has actual knowledge that the sending lawyer did not intend to disclose confidential information. *Id.* Nor does the Colorado Committee agree with the position taken by the California Supreme Court in *Rico v. Mitsubishi Motors Corp.*, 42 Cal. 4th 807 (Cal. 2007), that a receiving lawyer must stop reviewing material when it becomes "reasonably apparent" that the disclosure of confidential information was not intended. Colo. Bar Ass'n Ethics Comm., Formal Op. 119 (2007).

[282] *Id.*

[283] COLO. RULES OF PROF'L CONDUCT R. 4.4(c) (2008).

7. Maine

The professional Ethics Commission of the Maine Board of Overseers of the Bar was asked by Bar Counsel to give an opinion concerning "the ethical duties of lawyers involving the transmission, retrieval and use of metadata embedded in documents which may reveal client confidences or other legally privileged information."[284] To that end the Maine Commission considered the duties of receiving and sending lawyers separately, concluding as follows:

> 1. Without authorization from a court, it is ethically impermissible for an attorney to seek to uncover metadata, embedded in an electronic document received from counsel for another party, in an effort to detect confidential information that should be reasonably known not to have been intentionally communicated.
>
> 2. A sending attorney has an ethical duty to use reasonable care when transmitting an electronic document to prevent the disclosure of metadata containing confidential information.[285]

With respect to the receiving lawyer, the Maine Commission sided with the New York position and characterized "purposefully seeking" to uncover confidential information of another party as "dishonest," striking "at the foundational principles that protect attorney-client confidences," which "prejudices the administration of justice."[286] With respect to the sending lawyer, the Commission followed "the consensus approach on the subject," calling for "reasonable measures" to be taken "to avoid the communication of confidential information, regardless of the mode of transmission."[287]

Addressing the scope of reasonable measures the sending lawyer should take, the Commission did not find it reasonable that an attorney should be "ignorant of the standard features and capabilities of word processing and other software used by that attorney, including their reasonably known capacity for transmitting certain types of data that may be confidential."[288] In fact, "a basic understanding of the existence of metadata embedded in electronic documents, the features of the software used by the attorney to generate the document and practical measures that may be taken to purge documents of sensitive metadata where appropriate to prevent the disclosure of confidential information" is called for in undertaking a lawyer's duty.[289]

---

[284] Me. Prof'l Ethics Comm'n of the Bd. of Bar Overseers Op. 196 (2008).

[285] *Id.* (footnotes omitted).

[286] *Id.*

[287] *Id.*

[288] *Id.* This, however, would not dictate the retention of a computer expert in routine work. *Id.*

[289] *Id.*

8. New Hampshire

Most recently, the Ethics Committee of the New Hampshire Bar Association considered the duties of lawyers with respect to metadata, outside the context of litigation.[290] The Committee determined that both sending lawyers and receiving lawyers "share ethical obligations to preserve confidential information relating to the representation of clients."[291] With respect to sending lawyers, there is a "duty to use reasonable care to guard against disclosure of metadata that might contain confidential information."[292] Looking to Rules 1.1,[293] 5.1 and 5.3[294] the Committee asserted that "lawyers should be reasonably informed about the types of metadata that may be included in documents when they are transmitted electronically and the steps that can be taken to remove it."[295]

With respect to lawyers who receive metadata from opposing counsel, the New Hampshire Committee determined that they "have an ethical obligation not to search for, review or use metadata containing confidential information that is associated with transmission of electronic materials from opposing counsel."[296] Any confidential information contained in electronic material is inadvertently sent, triggering Rule 4.4(b) obligations. New Hampshire Rule

---

[290] N.H. Bar Ass'n Ethics Comm. Op. 2008-2009/4 (2009).

[291] *Id.*

[292] *Id.*

[293] *See* MODEL RULES OF PROF'L CONDUCT R. 1.1 (2009). New Hampshire Rule 1.1 defines competence in detail, providing a list of requirements a lawyer must follow to achieve "legal competence." N.H. RULES OF PROF'L CONDUCT R. 1.1 (2008).

[294] *See* MODEL RULES OF PROF'L CONDUCT R. 5.1(a) (2009). New Hampshire Rules 5.1 & 5.3 impose a duty on "each" lawyer with managerial authority to emphasize that this is an obligation of all managers which cannot be delegated to one manager. *See* N.H. RULES OF PROF'L CONDUCT R. 5.1 & 5.3 (2008).

[295] N.H. Bar Ass'n Ethics Comm. Op. 2008-2009/4 (2009). The New Hampshire Committee noted the following:

> [A]s a result of rapid technological advances, some lawyers are generally unaware of the myriad of ways that client confidences may be disclosed in the form of metadata that accompanies electronic documents and files. However, unless lawyers obtain a reasonable understanding of the risks inherent in the use of technology in transmitting and receiving electronic materials that may contain confidential information, they risk violating their ethical obligations to clients. Of course, this does not mean that lawyers must necessarily purchase expensive computer software to ensure that metadata is removed or "scrubbed" from documents in all cases. In most circumstances, lawyers can limit the likelihood of transmitting metadata containing confidential information by avoiding its creation during document drafting or subsequently deleting it, as well as by sending a different version of the document without the embedded information through hard copy, scanned or faxed versions.

Id.

[296] *Id.* at 1.

4.4(b), Respect for Rights of Third Persons, varies from the Model Rule, and provides as follows:

> A lawyer who receives materials relating to the representation of the lawyer's client and knows that the material was inadvertently sent shall promptly notify the sender and shall not examine the materials. The receiving lawyer shall abide by the sender's instructions or seek determination by a tribunal.[297]

Regarding metadata, the New Hampshire Committee posits that "all circumstances, with the exception of express waiver and mutual agreement on review of metadata, lead to a necessary conclusion that metadata is 'inadvertently sent.'"[298] The New Hampshire Committee seems to champion a shared responsibility on both the sending and receiving lawyer to protect the attorney-client privilege. With respect to a receiving lawyer, "unless receiving lawyers have a sound basis to believe that the information was intentionally sent or there has been an express waiver of confidentiality, receiving lawyers should not take steps to review or to use metadata embedded in documents received from opposing counsel."[299]

V. PROPOSED TREATMENT OF METADATA

The last fifteen years have seen the proliferation of electronic communications within the practice of law. Adversaries exchange electronic documents on a routine basis and within the context of civil litigation, electronic discovery is commonplace. 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. What impact this has, along with the concomitant duties and responsibilities it brings to legal practitioners, is a matter of significant concern.

A. Responsibilities of Sending Lawyers

As jurisdictions consider the issues surrounding metadata, the tendency has been to distinguish between transmissions that are subject to discovery in litigation and those which are not. This is primarily because within the context of litigation, rules and procedures may require that certain metadata be produced, and failure to do so could subject lawyers to some type of sanction

---

[297] N.H. RULES OF PROF'L CONDUCT R. 4.4(b) (2008). New Hampshire's Rule 4.4(b) was amended in 2008 "to provide guidance to lawyers who receive confidential information from opposing counsel or third persons." N.H. Bar Ethics Op. 2008-2009, *supra* note 182, at 4.

[298] N.H. Bar Ass'n Ethics Comm. Op. 2008-2009/5 (2009).

[299] *Id.* at 6.

or censure. However, with respect to material that could be subject to privilege, there should be no distinction between the responsibility of a sending lawyer, whether during litigation or otherwise. Across the board, whether outside or within the context of discovery, a sending lawyer has a duty to use reasonable care when transmitting documents to prevent the disclosure of metadata containing information which could be subject to privilege. Not surprisingly, what constitutes reasonable care will vary with the circumstances. One factor that has been considered is whether the lawyer has stayed abreast of technological advances regarding the transmission of electronic information.[300]

1. Outside the Discovery Context

Both outside and within the context of discovery, the sending lawyer has a duty to use reasonable care to see that no material which could be subject to privilege is included in documents that are transmitted to a third party. However, ethical mandates indicate that outside of litigation, information relating to the representation of a client would also be included in this prohibition.[301] The Model Rules call for a lawyer to provide competent representation to a client,[302] and with limited exceptions, not to reveal information relating to the client's representation.[303] While described by some as "stringent," "unworkable and unrealistic,"[304] a lawyer's ethical duty to maintain client confidentiality is very broad. It has been posited that *no* imbedded information should accompany documents sent to anyone outside one's firm.[305] Couching commercial scrubbers as "cheap and effective," many feel they "should be considered essential equipment for fulfilling lawyers' duties of competence and care."[306]

It may be that a lawyer intends to include embedded information when transmitting an electronic document to a third party. Perhaps embedded data is included for a third party's review or perhaps costs associated with conversion of particular files are significant, and since most metadata is harmless, a decision is made to send a file in its native format.[307] In such situations, conscious decisions to include metadata are involved. If sending lawyers do

[300] *See supra* notes 168, 173, 268, 289 and accompanying text.

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

[302] *See* FED. R. CIV. P 26(b)(3)(A)&(B).

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

[304] *See supra* note 4; *supra* note 101 and accompanying text.

[305] Whittaker, *supra* note 146, at 307 (emphasis added).

[306] *Id.* The effectiveness of commercial scrubbers is a matter on which different views are held. *See* Pa. Bar Ass'n Comm. on Legal Ethics & Prof'l Resp. Op. 2007-500 (2007); Siegel, *supra* note 242. Also, a forensic technologist can often retrieve information that has been scrubbed.

[307] *See, e.g.*, Suggested Protocol, *supra* note 147.

not intend to include metadata, it should be blocked or removed. Lawyers need to be mindful that it is inappropriate, if not dangerous, for a lawyer unintentionally to transmit information related to the representation of a client, especially that which could be considered sensitive. Lawyers must be aware of what is in the documents they transmit and how, or whether, embedded data can be accessed. Transmitting electronic documents to third parties that contain embedded information relating to the representation of a client could constitute a breach of a lawyer's ethical duty. Furthermore, in addition to being an ethical breach, lawyers might subject themselves to malpractice liability. "An attorney's failure to use the skill and knowledge ordinarily used by attorneys for communicating with or about a client could conceivably result in malpractice liability if the breach of duty proximately causes injury to the client."[308]

While a lawyer's ethical obligation to maintain the confidentiality of client information is clear, it is recognized that information may be mistakenly or inadvertently sent.[309] This can be the case even when reasonable care is used. To fulfill the lawyer's responsibility to exercise care to guard against such disclosure, lawyers should establish procedures to analyze, and where appropriate, cleanse, documents before sending files to a third party. Furthermore, should a sending lawyer determine that material was sent that should not have been, he or she should immediately notify the recipient of this fact and ask that remedial steps be taken. Such steps could include the immediate return of the information or its destruction.

2. Within the Context of Discovery

Both within and outside the context of discovery, a sending lawyer has the responsibility not to transmit information which could be subject to a claim of privilege. However, particularly within the context of discovery, a systematic removal of metadata may be both inappropriate and dangerous. Before removing metadata from a document that might be subject to discovery, sending lawyers must take care not to violate any duty of disclosure to which the lawyers or their clients are subject. The Model Rules specifically carve an exception to the lawyer's duty of confidentiality for compliance "with other law or a court order."[310]

Under mandates in new federal rules,[311] as well as under various state

[308] ABA/BNA Lawyers' Manual on Professional Conduct Electronic Communications Practice Guide, 55:401, LMPC 55:401 (Westlaw) (citing R. MALLEN & J. SMITH, LEGAL MALPRACTICE, § 8.12, 18.2 (4th ed. 1996)).

[309] *See, e.g.*, MODEL RULES OF PROF'L CONDUCT R. 4.4 cmt. 2 (2009).

[310] MODEL RULES OF PROF'L CONDUCT R. 1.6(b)(6) (2009).

[311] *See* FED. R. CIV. P. 16(b)(3)(iii), (iv); FED. R. CIV. P. 26(f)(C), (D); FED. R. CIV. P. 34(a)(1)(A); FED. R. CIV. P. 37(e).

provisions,[312] mechanisms are outlined by which prior to document production, the parties discuss the production of electronic documents, including metadata, and the assertion of any claims of privilege, and challenges thereto. Anticipating that information may be mistakenly or inadvertently sent, included in such discussions may also be procedures for asserting any such claims after information has been provided. For those matters on which counsel cannot agree, adjudication typically is available. Removing, or failing to preserve, metadata prior to the implementation of any outlined procedures could lead to sanctions being imposed on counsel and amount to a breach of a duty. Before removing or blocking embedded information in documents that might be subject to discovery, counsel should obtain direction from the court, or mutually work out how to proceed. Metadata which is determined to be confidential, or trial preparation material, may be protected. However, material that would constitute tangible evidence must be produced. While fishing expeditions are not allowed in discovery, access to "material that may lead to relevant material" is allowed.[313]

B. Responsibilities of Receiving Lawyers

It is the responsibility of the sending lawyer to take reasonable measures to avoid the disclosure of information which could be subject to a claim of privilege or protection, and outside the context of discovery, information relating to client representation. This notwithstanding, even with the employment of measures that are reasonable, material containing this information can be mistakenly or inadvertently sent. Given the volume and incidence of the exchange of electronic documents in law practice today, such an instance is contemplated in the Model Rules, which call for the receiving lawyer to notify the sender of inadvertently sent documents.[314] While jurisdictions are in general accord as to the sending lawyers' ethical obligations in this regard, disparate views are taken on the receiving lawyers' responsibilities.

Some jurisdictions take the position that a receiving lawyer is free to review and use embedded information which is transmitted in an electronic document.[315] Especially within the context of discovery, it has been asserted that not only is this permissible, but a receiving lawyer has an obligation to

---

[312] *See, e.g.*, Suggested Protocol *supra* note 147; Ariz. Ethics Op. 07-03, *supra* note 179.

[313] *In re* Telxon Corp. Sec. Litg., 2004 WL 3192729 *27 (N.D. Ohio 2004).

[314] MODEL RULE OF PROF. CONDUCT R. 4.4(b) (2009).

[315] *See* ABA Formal Op. 06-442, *supra* note 174 and accompanying text; MODEL RULE OF PROF. CONDUCT R. 4.4(b) (2009); Md. Ethics Op. 2007-09, *supra* note 188 and accompanying text; Pa. Ethics Op. 2009-100, *supra* note 261 and accompanying text; Whittaker, *supra* note 261 at 305 and accompanying text; Colo. Ethics Op. 119, *supra* note 277 and accompanying text.

competently and diligently review this material.[316] Perhaps this follows from the premise that because the presence of embedded data in documents is well known,[317] sending a document with metadata raises a presumption that it was intentional. Or perhaps this follows from the premise that given the duty of sending lawyers to remove unintended embedded information, metadata which is sent should be presumed to be intentional. Other jurisdictions, conversely, take the position that a receiving lawyer should not try to obtain information from metadata.[318] To these divergent points of view are variations, one of which calls for there to be actual knowledge of inadvertent disclosure for review to be precluded.[319]

1. Within the Context of Discovery

Within the context of discovery, as with the sending lawyer, procedural or evidentiary rules suggest mechanisms which help chart the receiving lawyer's responsibilities with respect to embedded information in documents that are subject to discovery. Either by agreement of the parties, or court order, the receiving lawyer's access to embedded information should often be pre-determined. It may be that metadata which is sent is tangible evidence which the receiving lawyer is free, if not obligated, to carefully review. Then again, because of the cost involved in the conversion of some files, a party may send documents in Native format with metadata intact, when such information is deemed to be inconsequential or irrelevant. And yet again, because of the cost involved in the conversion of some files, the parties may agree that files will be sent in Native format with metadata intact, which the receiving lawyer will agree not to access.[320]

In those situations where no rule, protocol or agreement exists for the handling of electronic documents, direction should be sought from the court. If direction is not forthcoming from the court, it seems reasonable to infer that information, including metadata which is produced in discovery, should be presumed to have been intentionally provided. Therefore, a lawyer who receives a document that contains metadata should be free to view and use this

[316] *See* D.C. Ethics Op. 341, *supra* note 221 and accompanying text.

[317] *See* Hricik, *supra* note 114. There are many types of metadata, some of which may not be removed by conventional means. *See* Pa. Bar Ass'n Comm. on Legal Ethics & Prof'l Responsibility, Formal Op. 2009-100 (2009). However, lawyers generally are aware of the existence of metadata and the problems associated with it. *See* Hricik, *supra* note 114.

[318] *See* N.Y. State Bar Ass'n Op. 749, *supra* note 162 and accompanying text; Ala. Ethics Op. 2007-02, *supra* note 207 and accompanying text; Ariz. Ethics Op. 07-03, *supra* note 232 and accompanying text; Me. Ethics Op. 196, *supra* note 287 and accompanying text; N.H. Ethics Op. 2008-2009/4, *supra* note 297 and accompanying text.

[319] *See* D.C. Ethics Op. 341, *supra* notes 214-15 and accompanying text.

[320] *See* Suggested Protocol, *supra* note 147 §§ 8(A) & 11.

information. However, this presumption of intentional submission is rebuttable. If a sending lawyer notifies opposing counsel that protected information was inadvertently sent, it should not be examined by the receiving lawyer. Also, if upon reviewing metadata, the receiving lawyers know, or should know, that the metadata was not intended for them, review should stop, the material should be treated as protected information which was not meant to be sent and the sending lawyer should be notified. Requiring receiving lawyers to comply with a standard of "actual knowledge," rather than one of "reasonably knows or should know," is inappropriate. Such a standard works against the confidentiality doctrine itself. As to what the receiving lawyer should do next, the information at issue should be returned or sequestered, until resolution of the issue by the means employed in the jurisdiction, or by the means decided upon in that particular litigation.

2. Outside the Discovery Context

A sending lawyer is obligated to take reasonable precautions to avoid the inadvertent transmission of documents, including metadata. Because lawyers should be familiar with this duty,[321] it seems reasonable to presume that most metadata which is transmitted in a document is done so intentionally by the sending lawyer. Most embedded data is inconsequential.[322] Thus lawyers who receive documents with embedded information should be free to review it, if they so desire. However, if the receiving lawyer obtains notice from the sending lawyer that metadata was inadvertently provided, the information should not be reviewed by the receiving lawyer. Additionally, if upon review of the metadata, the receiving lawyers know, or should know, that the metadata was not intended for them, it should be treated as protected information which was not meant to be sent, and the receiver should notify the sender. As with the situation where discovery is ongoing, calling for receiving lawyers to comply with a standard of "actual knowledge," rather than one of "reasonably knows or should know," is inappropriate.

It has been noted that no lawyer intentionally transmits confidential information to a third party, so any confidential information included in metadata to an adversary would be inadvertent.[323] It has also been noted that

[321] A 2004 study revealed that 43% of respondents were aware of the existence of embedded data. Warnings about embedded data have been released since 2006. *See* David Hricik, *Mining for Embedded Data: Is it Ethical to Take Intentional Advantage of Other People's Failures?*, 8 N.C. J. L. & TECH. 231, 246 (2007).

[322] *See* ABA Comm. on Ethics and Prof'l Responsibility Formal Op. 06-442 (2006) (Review and Use of Metadata). It has been noted that while most metadata is harmless, some of it can be useful. Elizabeth W. King, *The Ethics of Mining for Metadata Outside of Formal Discovery*, 113 PENN STATE L. REV. 801, 807 (2009).

[323] *See* Hricik, *supra* note 321, at 246-47; N.H. Bar Ass'n Ethics Comm. Op. 2008-

since a receiving lawyer's decision to review metadata is an intentional act, and a sending lawyer's inclusion of confidential information an inadvertent one, a receiving lawyer's search for metadata would be a dishonest act, taking advantage of a sending lawyer's mistake.[324] This proposition, while interesting, would be better grounded if most of the information contained in metadata were confidential information or sensitive. The converse is true; most metadata does not fall into this category.[325] The review of metadata by a receiving lawyer should not be considered a dishonest act. Furthermore, permitting the review of metadata does not put confidentiality at risk.[326] Embedded information which is confidential is afforded protection since review is precluded once the lawyer knows, or should know, its character.

One suggested approach to the metadata issue, couched as "a proactive stance," is for the receiving lawyer to reserve the right to its review.[327] Just as lawyers use disclaimers related to legal advice, client representation, and the like, assertions related to embedded information could be used. Lawyers may want to represent that they "reserve the right to use whatever readily available tools and techniques are available to examine any and all documents" that are transmitted.[328]

C. Inadvertent Disclosure as Waiver of Attorney-Client Privilege

Various jurisdictions have examined the transmission of metadata in electronic documents with an eye toward the obligations that attach to lawyers who send and receive these communications. However, in addition to

2009/4 (2009).

[324] *See* Hricik, *supra* note 321, at 241, 247. It has also been asserted that "searching for metadata is unethical because it is an intentional intrusion into the attorney-client relationship and constitutes conduct that is dishonest and prejudicial to the administration of justice." King, *supra* note 322, at 828.

[325] The following are examples of metadata categories: author's name; author's initials; author's company or organization name; name of network server or hard disc where author saved document; other file properties and summary information; non-visible portions of OLE objects; names of previous document authors; document revisions; document versions; template information; hidden text; comments to documents; and time spent editing documents. *See* Zall, *supra* note 206, at 54; David Hricik & Robert Jueneman, *The Transmission and Receipt of Invisible Confidential Information*, 15 PROF. LAW. 18 (2004-05). Often metadata simply acts as a bookmark and directs a reader where to look, similar to a "post-it" on a paper document.

[326] Some feel that "[a] rule allowing receiving attorneys to search for metadata wrongfully favors the duty of diligence over the duty of confidentiality." King, *supra* note 322, at 833.

[327] Hricik & Jueneman, *supra* note 325, at 20.

[328] *Id.*

attending to the ethical obligations of lawyers is the poignant question of whether the transmission of metadata, containing confidential or trial preparation material, results in the waiver of any protection or privilege that might attach. The trend has been toward a resolution of non-waiver.

When considering whether inadvertent disclosure waives attorney-client privilege, most jurisdictions apply a balancing test.[329] Typically, balancing factors relating to the care taken by the client and sending lawyer both before and after transmission, as well as fairness to the recipient, a judicial determination is made. Attempting to resolve resulting conflicting decisions, new Federal Rule of Evidence 502 comes down on the side of non-waiver when disclosure is inadvertent and the sending lawyer acted with reasonable care.[330] The scope of waiver is also narrow under Rule 502. If it is determined that the privilege is waived for an inadvertently sent document, Rule 502 limits the extent of the waiver to the actual material disclosed, in lieu of extending the waiver to other material on the covered subject.[331] This tendency toward non-waiver should be reflected in the treatment of metadata.

When metadata is sent in a document, it should be presumed that it was done so intentionally. This follows from our understanding of the sending lawyer's responsibility to use reasonable care to see that unintended metadata is not transmitted. However, this presumption of intent is not absolute. As has been noted, no lawyer intentionally transmits confidential information to a third party, so if material that is subject to privilege or protection is sent, the presumption is rebutted and the transmission is considered to be an inadvertent one.[332] For the purpose of evaluating waiver of attorney-client privilege, when metadata which is confidential is included in a document, it should constitute an inadvertent disclosure, even if the electronically transmitted document which included the imbedded information was intentionally sent.

As with other technologies used for communication in the practice of law, lawyers cannot ignore their responsibility to maintain the confidentiality of client information when transmitting documents electronically. However, as with facsimile transmissions, e-mail, and the like,[333] there is no indication that

---

[329] *See* Walkowiak, Lemons & Leach, *supra* note 38, at 319, 321 and accompanying text; Mackintosh & Angus, *supra* note 8, at 45 n.87.

[330] *See* Lindeman, *supra* note 54, at 646; Lindeman, *supra* note 55, at 496 and accompanying text.

[331] *See* Mackintosh & Angus, *supra* note 8, at 43 n.58; Pub. L. No. 110-322, §1(b), 122 Stat. 3537 (2008); s*upra* note 59 and accompanying text.

[332] *See* Hricik, *supra* note 321, at 246-47; N.H. Bar Ass'n Ethics Comm. Op. 2008-2009/4 (2009); *supra* note 324 and accompanying text.

[333] *See* ABA/BNA Lawyers' Manual on Professional Conduct Electronic Communications Practice Guide, 55:401, LMPC 55:401 (Westlaw); David Hricik, *Confidentiality & Privilege in High-Tech Communications*, 60 TEX. B.J. 104, 110 (Feb.

a lack of expectation of privacy should be associated with the mere use of electronic document transmission. As a profession, we contemplate, if not expect, some documents to be mistakenly or inadvertently transmitted, particularly electronic ones. Ethics opinions, rules and protocols address these inadvertent transmissions of documents, providing procedures for lawyers to follow as remedial steps.[334] When evaluating whether inadvertent disclosure waives a privilege or protection, the profession has focused on the reasonable care that was used both before and after transmission. Lawyers must be aware of the perils associated with electronic transmission of documents and have a mechanism in place to guard against transmitting information unintentionally. Depending on the situation, to comply with the lawyer's duty to use reasonable care, this may necessitate the retention of a computer expert, especially in particularly sensitive situations. Just as unusual circumstances involving extraordinarily sensitive information might warrant enhanced security measures with e-mail,[335] circumstances may call for the retention of technological specialists with the transmission of certain electronic documents.

While the standard of reasonable care has been embraced when evaluating waiver of privilege with inadvertent communications, perhaps it is time for the profession to explore a more liberal approach. Continuing with the current tendency toward non-waiver, and emphasizing the duty owed to one's client, perhaps a standard similar to that used in the subjective intent test should be employed.[336] Concomitant with this, it should not go unnoticed that the policy behind privilege, at common law, was grounded on subjective considerations.[337] Since the privilege is for the welfare of the client, it has been noted that "more than the attorney's negligence should be required before the client loses the privilege."[338] Opponents to this point of view opine that this approach does little to encourage care of privileged documents.[339] However, this is not necessarily the case. Although privilege may not be lost when an intent standard is employed, the lawyer would still have an ethical duty to protect client information. Should this duty be breached, the lawyer would be subject to discipline, or liability, in certain circumstances. Such an

1997) and text accompanying note 114.

[334] *See, e.g.*, *supra* notes 144, 200, 215, & 217; MODEL RULES OF PROF'L CONDUCT R. 4.4(b) (2009); Suggested Protocol, *supra* note 147, §. 8(D); D.C. Ethics Op. 341, *supra* note 184; FED. R. CIV. P. 26(B)(5)(B), *supra* note 216 and accompanying text.

[335] *See* discussion *supra* note 143 and accompanying text.

[336] *See* Walowiak et al., *supra* note 38; *supra* text accompanying note 42; *see also supra* note 190.

[337] *See supra* note 20.

[338] Walkowiak, Lemons & Leach, *supra* note 38, at 318 (quoting Mendenhall v. Barber-Greene Co., 531 F. Supp. 951, 955 (N.D. Ill. 1982)).

[339] *See* Walowiak et al., *supra* note 38; *supra* text accompanying note 47.

approach would work to hold the lawyer in check, while protecting privilege for the client.

IV. CONCLUSION

It is aptly stated that "[t]echnology is wonderful, but failing to understand it can lead to disastrous results."[340] Sending lawyers, both within and outside the context of discovery, must guard against transmitting information that is protected. Be it within or outside discovery, there is no distinction between the duty owed a client as it relates to information which could be subject to privilege. There is a distinction, however, with how counsel should proceed in furthering this mandate, depending on the setting. Outside of litigation, the sending lawyer also has a duty to see that metadata relating to the representation of a client is not available to a third party, unless there is an intent to transmit this information. Accomplishing this typically will involve employing some type of technological means. However, within the litigation context, counsel must employ these technological means very cautiously. Before removing or blocking embedded information in documents that might be subject to discovery, counsel should obtain direction from the court, or arrive at a mutual agreement, as to how they both will proceed.

As to lawyers who receive embedded information in electronic documents, in light of the duty imposed upon the sending lawyer, it is reasonable to assume that imbedded data that is sent in an electronic file usually is intentional. Lawyers receiving such information should be free to review it, unless the lawyers know, or should know, that it was not intended for them. In the situation where material is sent which is not intended for the receiving lawyer, the sending lawyer should be notified of its transmission and the receiving lawyer should follow the sending lawyer's directions.

In situations where confidential material is mistakenly or inadvertently sent, such act of the sending lawyer should not, in and of itself, amount to a waiver of attorney-client privilege. Typically, the standard of reasonable care is employed when determining if privilege has been waived. However, since privilege is for the welfare of the client, perhaps the profession should reconsider whether a mistaken or inadvertent act on the part of the lawyer, or even lawyer negligence, should deprive the client of privilege. While the majority of jurisdictions call for reasonable care on behalf of the sender, along with fundamental fairness, when determining waiver of privilege with inadvertent transmissions, it seems that the fate of the client should not solely rest on the action of the lawyer. Instead, perhaps the intent to disclose should be the linchpin for waiver of privilege as it relates to the client, especially in light of today's digital document exchange. We anticipate mistakes with

[340] Hricik & Jueneman, *supra* note 327, at 20.

electronic transmissions, and implement rules to help protect client information. Perhaps we should take protection of the client a step further, so clients do not lose privilege because their lawyers make mistakes or act in a careless manner.