



**PENNSYLVANIA BAR ASSOCIATION
COMMITTEE ON LEGAL ETHICS AND PROFESSIONAL RESPONSIBILITY**

**FORMAL OPINION
2009 – 100**

**ETHICAL OBLIGATIONS ON THE
TRANSMISSION AND RECEIPT OF METADATA**

I. Introduction

In Formal Opinion 2007-500, this Committee considered whether a lawyer has a duty to protect client confidentiality by removing metadata from electronic materials provided to opposing counsel, and whether opposing counsel is permitted to examine and use the metadata that was contained within the electronic materials. Since that opinion issued, other state bar ethics committees and commentators have reviewed this issue and presented further guidance on the topic. The Committee has carefully reviewed the available guidance and determined that the prior opinion provided insufficient guidance to recipients of documents containing metadata and did not provide correlative guidance to attorneys who send such documents. The conduct of attorneys in each of these capacities implicates several Rules of Professional Conduct affecting the attorney's responsibilities and options when metadata embedded in documents is transmitted inadvertently in conjunction with electronic communications.

As outlined in this Formal Opinion, this Committee concludes that an attorney has an obligation to avoid sending electronic materials containing metadata, where the disclosure of such metadata would harm the client's interests. In addition, an attorney who receives such 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. The substantive law governing whether the recipient may use the metadata received in legal proceedings or negotiations is outside the scope of this Opinion.¹

¹ This opinion assumes that the receiving lawyer did not obtain the electronic documents in a manner that was criminal, fraudulent, deceitful, or otherwise improper, for example, by making a false statement of material fact to opposing counsel or to any other third person (PA RPC 4.1(a)), using a method of obtaining evidence that violated the legal rights of a third person (PA RPC 4.4(a)), or otherwise engaging in misconduct (PA RPC 8.4). Such scenarios are beyond the scope of this opinion.

While no Pennsylvania Rule of Professional Conduct specifically addresses metadata, the Committee's conclusion is consistent with the treatment of inadvertent communications under Rule 4.4(b). Thus, the primary burden of keeping client confidences lies with the sending attorney: an attorney sending electronic materials has a duty of reasonable care to remove unwanted metadata consistent with Rule 1.1 (Competence) and Rule 1.6 (Client Confidentiality). However, the receiving attorney, while potentially under duties to the client under Rules 1.1, 1.2, 1.3, and 1.4 to review, communicate and utilize such information, must, if the receiver knows or reasonably should know that the document was inadvertently sent, treat such metadata as an inadvertent communication under Rule 4.4(b) and promptly notify the sender of the receipt of the materials.

II. Background

Metadata, which means "information about data," is data contained within electronic materials that is not ordinarily visible to those viewing the information.² Although most commonly found in documents created in Microsoft Word, metadata is also present in a variety of other formats, including spreadsheets, PowerPoint presentations and Corel WordPerfect documents.³ Metadata generally contains seemingly harmless information such as editing of spelling or punctuation. Metadata may also contain privileged and/or confidential information, such as previously deleted text, notes and tracked changes, which may provide information about, *e.g.*, legal issues, legal theories and other information that was not intended to be disclosed to opposing counsel. *See, e.g.*, Daniel J. Siegel, "Scrub Your Documents," *The Philadelphia Lawyer*, Fall 2005.^{4,5}

² Although metadata appears in various types of materials such as documents, spreadsheets and presentations created by computer programs such as Microsoft Word, Microsoft Excel, Microsoft PowerPoint and Corel WordPerfect, this Opinion refers to these materials collectively as "documents."

³ 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. Additional information about metadata and removing it from Microsoft documents may be found on Microsoft's website at <http://support.microsoft.com/kb/290945>, <http://support.microsoft.com/kb/q223790/>, and <http://office.microsoft.com/en-us/help/HA010776461033.aspx>.

⁴ The Microsoft Office website contains detailed information about metadata, and provides examples of metadata that may be stored in materials created by Microsoft

Attorneys who receive electronic documents from other attorneys can easily use a variety of software to discover and utilize this metadata, with potentially disastrous consequences to the other side. *See*, David Hricik and Robert B. Jueneman, “The Transmission and Receipt of Invisible Confidential Information,” 15 *The Professional Lawyer* No. 1, p. 18 (Spring 2004). For example, in a products liability lawsuit involving the prescription drug Vioxx, the metadata contained within documents produced by Merck, the manufacturer of the drug, revealed that Merck had edited out negative information from a drug study. *See* Eileen B. Libby, “What Lurks Within: Hidden Metadata in Electronic Documents Can Win or Lose Your Case,” http://www.abanet.org/cpr/about/Hidden_Metadata.html. Because the problems with metadata have become increasingly common, and because the software that permits review of the data is inexpensive and easy to use, the ability to discover and utilize metadata presents serious challenges to the protection of the confidentiality of information provided by counsel.

III. Discussion

A. Pennsylvania Rules of Professional Conduct: Mandatory and Prohibited Conduct

The Rules implicated by these circumstances include portions of Rule 1.0 (“Definitions”); Rule 1.1 (“Competence”); Rule 1.2 (“Scope of Representation and Allocation of Authority Between Client and Lawyer”); Rule 1.3 (“Diligence”); Rule 1.4 (“Communication”); Rule 1.6 (“Confidentiality of Information”); and Rule 4.4 (“Respect for Rights of Third Persons”). The Rules define the requirements and limitations on an attorney’s conduct that may subject the attorney to disciplinary sanctions; while the Comments may assist an attorney in understanding or arguing the intention of the Rules, they are not enforceable in disciplinary proceedings.

B. Duties of the Transmitting Lawyer

In the absence of a specific Rule addressing the handling of metadata, the inadvertent disclosure of metadata is analogous to the inadvertent disclosure of a document and not an act consciously undertaken by counsel.

applications, and explains how to remove this data from a document. Examples of metadata that may be hidden in documents include the name of the author, information about the computer on which the document was typed, the names of previous authors of the document, as well as the number of revisions to the document and the contents of those revisions.

⁵ Of course, when responding to discovery, a lawyer must not alter a document when it would be unlawful or unethical to do so. *See, e.g.*, Rule 3.4(a) (“A lawyer shall not: (a) unlawfully obstruct another party’s access to evidence or unlawfully alter, destroy or conceal a document or other material having potential evidentiary value. A lawyer shall not counsel or assist another person to do any such act[.]”).

Rule 1.1 (“Competence”) 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.

Competent representation necessitates that an attorney disclose only that client confidential information that the attorney believes is appropriate to advance the client’s cause, in the manner which does so most effectively. Competence includes the knowledge and skill to secure appropriate protection for documents to insure 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.

An attorney is also generally prohibited from revealing information “relating to representation” pursuant to Rule 1.6 (“Confidentiality of Information”), which states:

(a) A lawyer shall not reveal information relating to representation of a client unless the client gives informed consent, except for disclosures that are impliedly authorized in order to carry out the representation, and except as stated in paragraphs (b) and (c).

As noted in Comment [4] to the Rule, this duty to protect client information extends beyond the information disclosed by a client or otherwise learned in the course of the representation to material which provides access to such protected content. Except in situations in which metadata is intentionally included in a transmitted document, metadata will generally fall within this category.

[4] Paragraph (a) prohibits a lawyer from revealing information relating to the representation of a client. This prohibition also applies to disclosures by a lawyer that do not in themselves reveal protected information but could reasonably lead to the discovery of such information by a third person. A lawyer’s use of a hypothetical to discuss issues relating to the representation is permissible so long as there is no reasonable likelihood that the listener will be able to ascertain the identity of the client or the situation involved.

This Comment is particularly pertinent to metadata, which may contain source material, work product, references or other content that may reveal protected information, thereby underscoring the obligation of the lawyer to take all available steps to avoid the transmittal of metadata and to ensure that the lawyer is promptly advised of the receipt of any inadvertently transmitted metadata.

As stated in Comment [23] to Rule 1.6 (“Acting Competently to Preserve Confidentiality”), protection of a client’s confidential information under Rule 1.6 is one element of competent representation under Rule 1.1:

[23] A lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rule 1.1, 5.1 and 5.3.

Comment [24], without reference to the term "metadata," speaks clearly to the lawyer's duty to protect the client's information in transmitting electronic documents:

[24] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule.

C. Duties of the Receiving Lawyer

Two facets of the Rules apply to the conduct of the receiving lawyer. The first is the duty of the lawyer to the lawyer's client. The second is the duty to the opposing party. While, in the view of this Committee, the former takes precedence, this Opinion will address these issues in order.

As noted, for the purpose of this Opinion, the Committee views unintentionally embedded metadata as an inadvertent disclosure. Rule 4.4(b) ("Respect for Rights of Third Persons"), which outlines the duty of a lawyer who receives an inadvertent disclosure, states:

(b) 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.

The rule must be read in conjunction with the following definitions under Rule 1.0:

(f) "Knowingly," "Known," or "Knows" denotes actual knowledge of the fact in question. A person's knowledge may be inferred from circumstances.

(h) “Reasonable” or “Reasonably” when used in relation to conduct by a lawyer denotes the conduct of a reasonably prudent and competent lawyer.

(j) “Reasonably should know” when used in reference to a lawyer denotes that a lawyer of reasonable prudence and competence would ascertain the matter in question.

(l) “Substantial” when used in reference to degree or extent denotes a material matter of clear and weighty importance.

Rule 1.2 states:

(a) Subject to paragraphs (c) and (d), a lawyer shall abide by a client’s decisions concerning the objectives of representation and, as required by Rule 1.4, shall consult with the client as to 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.

When applied to metadata, Rule 4.4(b) 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. In many instances, the process may be relatively simple, such as where the information does not appear on the face of the document sent but is accessible only by means such as viewing tracked changes or other mining techniques, or, in the alternative, where a covering document may advert to the intentional inclusion of metadata. The resulting conclusion or state of knowledge determines the course of action required. The foregoing again presumes that the mere existence of metadata confirms inadvertence, which is not warranted. This conclusion taken to its logical conclusion would mean that the existence of any and all metadata must be reported to opposing counsel in every instance.

Rule 4.4(b) and the Comments to the Rule demonstrate that attorneys in Pennsylvania who receive inadvertently disclosed documents have an ethical obligation to promptly notify the sender. The Comment to Rule 4.4 makes clear that any action other than reporting is purely a matter of intraprofessional courtesy and the lawyer’s sound judgment or substantive law, unless other Rules are implicated. The Comments to Rule 4.4 state:

[2] Paragraph (b) recognizes that lawyers sometimes receive documents that were mistakenly sent or produced by opposing parties or their lawyers. If a lawyer knows or reasonably should know that a document was sent inadvertently, then this Rule requires the lawyer to promptly notify the sender in order to permit that person to take protective measures. Whether the lawyer is required to take additional steps, such as returning the original document, is a matter of law beyond the scope of these Rules, as is the question of whether the privileged status of a

document has been waived. Similarly, this Rule does not address the legal duties of a lawyer who receives a document that the lawyer knows or reasonably should know may have been wrongfully obtained by the sending person. For purposes of this Rule, “document” includes e-mail or other electronic modes of transmission subject to being read or put into readable form.

[3] Some lawyers may choose to return a document unread, for example, when the lawyer learns before receiving the document that it was inadvertently sent to the wrong address. Where a lawyer is not required by applicable law to do so, the decision to voluntarily return such a document is a matter of professional judgment ordinarily reserved to the lawyer. See Rules 1.2 and 1.4.

These Comments do not mention other duties that the receiving attorney may have relating to receipt of such information, specifically, the lawyer’s duties to the client, which may require the attorney to either disclose to or withhold from the client the fact and content of the inadvertently transmitted document, which duties must be evaluated in light of relevant substantive and procedural law. These duties lie under Rules 1.1, 1.2 and 1.4.

A lawyer’s duty to competently represent that client under RPC 1.1 requires that the lawyer first 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 this information. Conversely, if the inadvertently received material is beneficial to the client’s case and can be viewed and/or used without adverse consequence, then Rule 1.1 may require that the attorney do so.

Generally, a lawyer has an obligation to keep the client fully apprised of important developments in the client’s case so that the client may make informed decisions concerning the representation. The receipt of a transmission including potentially useful metadata may be a significant event in the progress of the legal matter. Rule 1.4, which requires a lawyer to keep a client informed about such significant events and to provide enough information to permit the client to make informed decisions concerning the representation, provides:

(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; ...

(b) A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation.

A lawyer must generally abide by the client's decisions concerning the objectives of representation, and the lawyer is to consult with the client as to the means of achieving them. These communications are necessary to effectuate the allocation of authority between client and lawyer under Rule 1.2(a).

Upon making a determination as to the potential consequences of disclosure to the client and use of the materials, the lawyer will be in a position to comply with his or her duty to communicate with the client under Rule 1.4 and to respect the client's authority to control the objectives and means of pursuit under Rule 1.2.

If the attorney determines that disclosure of the substance of the metadata to the client may negatively affect the process or outcome of the case, there will in most instances remain a duty to advise the client of the receipt of the metadata and the reason for nondisclosure. The client may then make an informed decision whether the advantages of examining or utilizing the metadata outweigh the disadvantages of so doing.

D. Differing Opinions of Other Ethics Committees

Various Ethics Committees have considered whether reviewing the metadata contained within documents produced by opposing counsel is ethically permissible, and have reached varying conclusions.⁶

The American Bar Association Standing Committee on Ethics and Professional Responsibility considered the review and use of metadata in Formal Opinion 06-442 (August 5, 2006), concluding that the ABA Model Rules of Professional Conduct "generally permit" a lawyer to review and use metadata contained in e-mail and other electronic documents, "whether [they are] received from opposing counsel, an adverse party or an agent of an adverse party." Finding Model Rule 4.4(b) most closely applicable, the Committee stated that, although Rule 4.4(b) provides that "[a] lawyer who receives a document relating to the representation of the lawyer's client and knows or

⁶ See, also, Elizabeth W. King, "The Ethics of Mining for Metadata Outside of Formal Discovery," *Penn State Law Review*, Vol. 113:3, p. 801 (2009), which provides a review of the various Ethics Committee opinions, and concludes that, "outside of formal discovery, a lawyer who receives electronic documents should not be ethically permitted to search for inadvertently disclosed metadata" *Id.*, p. 804.

reasonably should know that the document was inadvertently sent shall promptly notify the sender,” the rule is silent on the issue of whether or not an attorney can review or use such information. The Committee therefore concluded that the Rule’s sole requirement of promptly notifying the sender of inadvertently sent documents was “evidence of the intention to set no other specific restrictions on the receiving lawyer’s conduct...” The Committee suggested several methods by which counsel could protect himself or herself from inadvertently disclosing metadata, including negotiation of a confidentiality agreement or protective order that allows the transmitting attorney to “pull back” transmitted documents. These methods of protection, however, will not always adequately protect an attorney, such as when the transferred metadata contains information about a client’s willingness to settle and/or the terms by which the client may be willing to do so.

The Maryland State Bar Association Committee on Ethics issued Opinion 2007-09, in which it concluded that lawyers who produce electronic materials in discovery have a duty to take reasonable measures to avoid the disclosure of confidential information embedded in the metadata within the documents. Citing the recent amendments to the Federal Rules of Civil Procedure, the Committee further concluded that lawyers who receive electronic discovery materials have no ethical duty to refrain from viewing or using metadata.

Several Ethics Opinions have concluded, contrary to the ABA Opinion, that a party may not use inadvertently disclosed metadata. However, some of these Opinions are based upon different rules of conduct than those in effect in Pennsylvania, and those that are based upon similar rules do not take into consideration the duty of the lawyer to the lawyer’s client, as discussed in § III(c), *supra*. See, e.g., New York Committee on Professional Ethics, *Opinion 749* (December 14, 2001) and *Opinion 782* (December 8, 2004). In *Opinion 749*, the Committee addressed the use of computer software to surreptitiously examine metadata contained in emails and other electronic documents.⁷

⁷ Opinion 782 concluded:

Lawyers have a duty under DR 4-101 to use reasonable care when transmitting documents by e-mail to prevent the disclosure of metadata containing client confidences or secrets.

Effective April 1, 2009, New York has adopted a modified version of the Model Rules of Professional Conduct, including Rule 4.4(b), which states:

(b) 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.

Each of the New York Committee’s opinions was based upon prior Disciplinary Rule 4-101. As the Committee noted in *Opinion 782*:

The Lawyer’s Code of Professional Responsibility (the "Code") prohibits lawyers from “knowingly” revealing a client confidence or secret, DR 4-101(B)(1), except when permitted under one of five exceptions enumerated in DR 4-101(C). DR 4-101(D) states that a lawyer “shall exercise reasonable care to prevent his or her employees, associates, and

The New York Committee concluded that such a use of metadata “constitutes an impermissible intrusion on the attorney-client relationship in violation of the [Code of Professional Responsibility].” *Id.* Noting that the Code “prohibits a lawyer from engaging in conduct ‘involving dishonesty, fraud, deceit or misrepresentation...’ and ‘conduct that is prejudicial to the administration of justice...’” the Committee opined that “in light of the strong public policy in favor of preserving confidentiality as the foundation of the lawyer-client relationship,” such a use of metadata would go against the spirit of the Code. *Id.* The Committee paralleled the use of inadvertently transmitted metadata to the use of inadvertently transmitted communications in general, which the Committee had previously found impermissible under the Code because the conduct involved “dishonesty, fraud, deceit or misrepresentation, [was] prejudicial to the administration of justice” and would “undermine confidentiality and the attorney-client relationship.” *Id.*

The Committee concluded that the use of software to examine metadata was more impermissible than the use of inadvertently transmitted communication in general noting that, whereas in the latter scenario the transmitting attorney’s carelessness caused the inadvertent transmission, in the former scenario, the transmitting attorney unwillingly and unknowingly transmitted the metadata, which the receiving attorney then secretly and deceitfully accessed. *Id.* This Committee is of the opinion 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.

In *Opinion 782*, the New York Committee addressed the emailing of documents that may contain metadata “reflecting client confidences and secrets.” The Committee concluded that “Lawyers must exercise reasonable care to prevent the disclosure of confidences and secrets contained in ‘metadata’ in documents they transmit electronically to opposing counsel or other third parties.” *Id.* Identifying the various rules under the Lawyer’s Code of Professional Responsibility that provide guidance in these situations, the Committee stated:

The Lawyer’s Code of Professional Responsibility (the “Code”) prohibits lawyers from “knowingly” revealing a client confidence or secret, DR 4-101(B)(1), except when permitted under one of five exceptions enumerated in DR 4-101(C). DR 4-101(D) states that a lawyer “shall exercise reasonable care to prevent his or her employees, associates, and others whose services are utilized by the lawyer from disclosing or using confidences or secrets of a client.” See also EC 4-5 (“Care should be exercised by a lawyer to prevent the disclosure of the confidences and secrets of one client to another”). Similarly, a lawyer who uses technology

others whose services are utilized by the lawyer from disclosing or using confidences or secrets of a client.”

This Committee believes that the New York Committee’s opinion is unlikely to change as a result because its primary concerns were the protection of client confidences and the preservation of the attorney-client relationship, both of which remain embodied in the Model Rules.

to communicate with clients must use reasonable care with respect to such communication, and therefore must assess the risks attendant to the use of that technology and determine if the mode of transmission is appropriate under the circumstances. See N.Y. State 709 (1998) (“an attorney must use reasonable care to protect confidences and secrets”); N.Y. City 94-11 (lawyer must take reasonable steps to secure client confidences or secrets).

Id. The Committee opined that “Reasonable care may, in some circumstances, call for the lawyer to stay abreast of technological advances and the potential risks in transmission in order to make an appropriate decision with respect to the mode of transmission,” implying that attorneys have the responsibility to take steps to prevent the transmission of metadata when emailing documents. *Id.* The Committee noted, however, that “Lawyer-recipients also have an obligation not to exploit an inadvertent or unauthorized transmission of client confidences or secrets.” *Id.* Therefore, while finding that attorneys may have to take steps to prevent the transmission of metadata, the Committee continued to hold that it is unethical for receiving attorneys to use technology to secretly view and use metadata.

The Professional Ethics Committee of the Florida Bar and Alabama State Bar Office of General Counsel have reached similar conclusions. In *Professional Ethics of the Florida Bar Opinion 06-2* (September 15, 2006), the Florida Committee addressed the duties of both transmitting and receiving attorneys with respect to metadata contained in electronic documents. With respect to transmitting attorneys, the Committee examined Fl.R.P.C. 4-1.6(a), which is virtually identical to Pa.R.P.C. 1.6, for guidance. The Committee concluded that “Florida lawyers must take reasonable steps to protect confidential information in all types of documents and information ... including electronic documents and electronic communications with other lawyers and third parties” in order to maintain confidentiality as required by Rule 4-1.6(a). *Id.* With respect to receiving attorneys, the Committee relied on Fl.R.P.C. 4-4.4(b), which is substantially similar to Pa.R.P.C. 4.4(b), for guidance, concluding:

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. *See*, Ethics Opinion 93-3 and Rule 4-4.4(b), Florida Rules of Professional Conduct, effective May 22, 2006.

...If the recipient lawyer inadvertently obtains information from metadata that the recipient knows or should know was not intended for the recipient, the lawyer must “promptly notify the sender.” *Id.*

Id. (footnote omitted) The Committee concluded that the duties of transmitting and receiving attorneys mentioned above “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 under Rule 4-1.6(a),” noting that Rule 4-1.6’s Comment addressing competency states that a lawyer “should engage in continuing study and education” to maintain the skills and knowledge necessary for competent representation. *Id.*

In *Alabama Bar Formal Ethics Opinion 2007-02* (March 14, 2007), the Alabama State Bar Office of General Counsel, concluded that “an attorney has an ethical duty to exercise reasonable care when transmitting electronic documents to ensure that he or she does not disclose his or her client's secrets and confidences,” noting that what constitutes reasonable care will vary based on the circumstances of each case. *Id.* Relying upon Ala. R. Prof. C. 1.6 and 8.4, which are substantially similar to Pa.R.P.C. 1.6 and 4.4, the Opinion also concluded that “Just as a sending lawyer has an ethical obligation to reasonably protect the confidences of a client, the receiving lawyer also has an ethical obligation to refrain from mining an electronic document.” *Id.* The Alabama Bar specifically agreed with New York *Opinion 749* that the use of computer technology to view and utilize metadata “constitutes an impermissible intrusion on the attorney-client relationship in violation of the Alabama Rules of Professional Conduct,” noting that the protection of the confidence of the client is “a fundamental tenet of the legal profession.” *Id.*

The State Bar of Arizona Ethics Committee made similar conclusions in its *Ethics Opinion 07-03* adopted in November of 2007. It determined that sending attorneys have a duty of reasonable care to avoid disclosing client confidences, and it further concluded that the receiving lawyer cannot mine or use metadata, as that is “an unjustified intrusion into the client-lawyer relationship that exists between the opposing party and his or her counsel.” *Id.* Additionally, though it disfavors the mining of metadata, the Arizona Ethics Committee requires that the receiving attorney notify the sending attorney if metadata conveys any confidential information. *Id.*

In its Opinion, the Colorado Bar Association Ethics Committee permitted a receiving attorney to mine for metadata, but with a caveat: if the transmitting attorney notifies the receiving attorney that metadata was inadvertently sent, the receiving attorney cannot view or use the metadata as long as the receiving attorney has not already seen it. Colorado Bar Association Ethics Committee, Formal Opinion 119 (May 17, 2008). The Colorado Bar further requires a sending attorney to take reasonable care that no client confidences are transmitted to third parties, including through metadata. *Id.* Finally, the receiving attorney must assume that any confidential information received was sent inadvertently unless he or she knows otherwise, and the receiving attorney must therefore notify the sending attorney that the information was sent. *Id.*

The Maine Board of Overseers of the Bar Professional Ethics Commission, in *Opinion 196*, adopted October 21, 2008, has also concluded that a sending attorney owes his or her client a duty of reasonable care to avoid disclosing client confidences. Although the Committee determined that mining a received document for metadata is unethical, it did

not render an opinion whether a receiving attorney must notify the sending attorney when confidential information is conveyed. *Id.*

The District of Columbia Bar Association differed with the ABA in Ethics Opinion 341 in September 2007, concluding:

A receiving lawyer is prohibited from reviewing metadata sent by an adversary only where he has actual knowledge that the metadata was inadvertently sent. In such instances, the receiving lawyer should not review the metadata before consulting with the sending lawyer to determine whether the metadata includes work product of the sending lawyer or confidences or secrets of the sending lawyer's client.

The D.C. Bar further stated:

We recognize that other ethics opinions take a different view and have concluded that neither Rule 8.4(c) nor any other ethics rule prohibits the review of metadata. In Formal Opinion 06-442, the ABA noted that there is no rule expressly prohibiting such conduct. The ABA discussed Model Rule 4.4(b), which relates to the inadvertent production of documents, as "the most closely applicable rule," but it declined to state that it directly applied to metadata transmitted within an electronic document. The ABA nevertheless noted that under Model Rule 4.4(b), where it applies, a receiving lawyer has no obligation under the ethics rules beyond notifying the sender.[5]

Notably, however, the version of Rule 4.4(b) adopted by the D.C. Court of Appeals, effective February 1, 2007, is more expansive than the ABA version. Indeed, the D.C. Rule largely codified Opinion No. 256 regarding inadvertent production of privileged documents. See D.C. Rule 4.4, Comments [2] & [3]. D.C. Rule 4.4(b) provides:

A lawyer who receives a writing relating to the representation of a client and knows, before examining the writing, that it has been inadvertently sent, shall not examine the writing, but shall notify the sending party and abide by the instructions of the sending party regarding the return or destruction of the writing

These various opinions reach different conclusions, and each offers a persuasive rationale.

IV. Conclusion

The use of metadata by attorneys receiving electronic documents from an adverse party is a continuing problem and source of confusion as to appropriate conduct. A transmitting attorney has tools at his or her disposal that can minimize the amount of metadata

contained in a document he or she is transmitting, but those tools still may not remove all metadata.

This Committee believes that the Pennsylvania Rules of Professional Conduct require that the responsibility of keeping client confidences is primarily that of the sending attorney, but recognizes that technological challenges require the offsetting duty of the receiving lawyer to notify the sender of the possible error. Therefore, this Committee concludes that, under the Pennsylvania Rules of Professional Conduct:

- (1) A transmitting attorney has a duty of reasonable care to remove unwanted metadata from electronic documents before sending them to a third party;
- (2) If the receiving lawyer concludes that the disclosure of metadata was inadvertent, the lawyer must promptly notify the sender of the receipt of the materials containing metadata; and,
- (3) The receiving lawyer:
 - (a) must then determine whether he or she may use the data received as a matter of substantive law;
 - (b) must consider the potential effect on the client's matter should the lawyer do so; and,
 - (c) should advise and consult with the client about the appropriate course of action under the circumstances.

CAVEAT: The foregoing opinion is advisory only and is not binding on the Disciplinary Board of the Supreme Court of Pennsylvania or any other Court. This opinion carries only such weight as an appropriate reviewing authority may choose to give it.