ELECTRONIC EXCHANGE OF DOCUMENTS:
THE ETHICS OF METADATA

HANS P. SINHA

INDEX

NEW YORK ETHICS OPINION 749 (12/14/01) ................................................................. 2
AMERICAN BAR ASSOCIATION ETHICS OPINION 06-442 (8/5/06) ......................... 6
FLORIDA ETHICS OPINION 06-02 (9/15/06)) ............................................................... 11
MARYLAND ETHICS OPINION 2007-09 (10/19/06) ...................................................... 15
ALABAMA ETHICS OPINION 2007-02 (3/14/07) ............................................................ 18
DISTRICT OF COLUMBIA ETHICS OPINION 341 (9/07) ............................................. 22
PENNSYLVANIA ETHICS OPINION 2007-500 (11/20/07) ......................................... 29
PENNSYLVANIA ETHICS OPINION 2009-100 (4/09) .................................................... 39
ARIZONA ETHICS OPINION 07-03 (11/07) .................................................................. 54
COLORADO ETHICS OPINION 119 (5/17/08) ............................................................... 59
MAINE ETHICS OPINION 196 (10/21/08) ................................................................. 67
NEW HAMPSHIRE ETHIC’S OPINION 2008-2009/4 (4/16/09) ................................. 75
WEST VIRGINIS ETHICS OPINION 2009-1 (6/10/09) ............................................. 84
VERMONT ETHICS OPINION 2009-1 (9/09) ................................................................. 89
New York State Bar Association Ethics Opinion 749

USE OF COMPUTER SOFTWARE TO SURREPTITIOUSLY EXAMINE AND TRACE E-MAIL AND OTHER ELECTRONIC DISCOVERY

December 14, 2001

BACKGROUND

Modern computer technology enables sophisticated users who receive documents by electronic transmission to “get behind” what is visible on the computer screen and determine, among other things, revisions made at various stages, and sometimes even the authors of the revisions. Use of this technology would enable a lawyer who receives e-mail and electronic documents from counsel for an opposing party to obtain various kinds of information that the sender has not intentionally made available to the lawyer. For example, a lawyer who has received the final draft of a contract from counsel for a party with whom the lawyer is negotiating would be able to see prior drafts of the contract and, perhaps, learn the identity of those who made the revisions, without the knowledge or consent of the sending lawyer. How to effectively “block” recipients from access to deletions and prior versions of the “visible” document appears to be unclear and a matter of debate among sophisticated computer users. See, e.g., M. David Stone, “Deleting Your Deletions,” P.C. Magazine November 20, 2000.

It is also possible for an e-mail sender to determine the subsequent route of the e-mail, including comments on the e-mail written by its ultimate recipients. Through use of this application a lawyer can place a “bug” in e-mail he or she sends to opposing counsel and learn the identity of those with whom the first recipient shares the message and comments that these persons may make about it. Even if a user can avoid applications that make it possible to place a bug in the user’s e-mail, the recipient’s forwarded messages can still be traced if the user forwards the message to someone who has not taken these measures. Accordingly, it is virtually impossible to render one’s e-mail system “bug-proof”. See www.privacyfoundation.org/privacywatch, “E-Mail Wiretapping”, posted February 5, 2001.

QUESTION

May a lawyer ethically may use available technology to surreptitiously examine and trace e-mail and other electronic documents in the manner described?

OPINION

This new technology permits a user to access confidential communications relating to another lawyer’s representation of a client, including “confidences” and “secrets” within the scope of DR 4-101 of the Lawyer’s Code of Professional Responsibility (“Code”). For this reason, we conclude that the use of computer technology in the manner described above constitutes an impermissible intrusion on the attorney-client relationship in violation of the Code. The protection of the confidences and secrets of a client are among the most significant obligations imposed on a lawyer. As explained in EC 4-1:
Both the fiduciary relationship existing between lawyer and client and the proper function of the legal system require the preservation by the lawyer of confidences and secrets of one who has employed or sought to employ the lawyer. A client must feel free to discuss anything with his or her lawyer and a lawyer must be equally free to obtain information beyond that volunteered by the client. . . . The observance of the ethical obligation of a lawyer to hold inviolate the confidences and secrets of a client not only facilitates the full development of facts essential to proper representation of the client but also encourages non-lawyers to seek early legal assistance.

Although the precise question presented in this inquiry has not previously been answered by this Committee or, to our knowledge, by other ethics authorities, we believe the circumstances described are substantively analogous to less technologically sophisticated means of invading the attorney-client relationship that we and other authorities have addressed and rejected as inconsistent with the ethical norms of the profession. For example, the strong public policy in favor of protecting attorney-client confidentiality is expressed in the prohibition against lawyers (1) soliciting the disclosure of unauthorized communications, see, e.g., Dubois v. Gradco Sys., Inc., 136 F.R.D. 341, 347 (D. Conn. 1991) (Cabranes, J.) (Although former employees of adverse corporate party are not within reach of the no-contact rule “it goes without saying that plaintiff’s counsel must take care not to seek to induce or listen to disclosures by the former employees of any privileged attorney-client communications to which the employee was privy’’); see also ABA Formal Op. 91-359; (2) exploiting the willingness of others to undermine the confidentiality principle, see N.Y. State 700 (1997); ABA Formal Op. 94-382; and (3) making use of inadvertent disclosures of confidential communications, see ABA Formal Op. 92-368.

The Code prohibits a lawyer from engaging in conduct “involving dishonesty, fraud, deceit or misrepresentation,” DR 1-102(A)(4) and “conduct that is prejudicial to the administration of justice.” DR 1-102(A)(5). 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. Accord MMR/Wallace Power & Indus. Inc. v. Thames Assocs., 764 F. Supp. 712, 718-19 (D. Conn. 1991) (spirit if not the letter of ethical rules precludes an attorney from acquiring, inadvertently or otherwise, confidential information about his adversary’s litigation strategy); In re Wisehart, 721 N.Y.S. 2d 356, 281 A.D. 2d 23, (1st Dep’t 2001) (respondent suspended for two years for using documents purloined by his client from opposing counsel); N.Y. City 1989-1 (client’s interception of adversary’s communications with counsel involved dishonesty and deceit; lawyer may not help client take advantage of such wrongdoing).

In the present inquiry, although counsel for the other party intends the lawyer to receive the “visible” document, absent an explicit direction to the contrary counsel plainly does not intend the lawyer to receive the “hidden” material or information about the authors of revisions to the document. To some extent, therefore, the “inadvertent” and “unauthorized” disclosure cases provide guidance in the present inquiry.

In N.Y. State 700 (1997), we concluded that a lawyer who receives an unsolicited and
Unauthorized communication from a former employee of an adversary’s law firm may not seek information from that person if the communication would exploit the adversary’s confidences or secrets. Despite the fact that the Code does not expressly require a lawyer to refrain from encouraging a breach of client confidentiality by opposing counsel’s staff, we determined that because use of such information would undermine confidentiality and the attorney-client relationship, it was conduct “involving dishonesty, fraud, deceit or misrepresentation,” DR 1-102(A)(4), and “conduct prejudicial to the administration of justice.” DR 1-102(A)(5).

In N.Y. State 700 we cited ABA Formal Op. 92-368 in support of our conclusion that the strong public policy in favor of confidentiality outweighed what might be seen as the competing principles of zealous representation (Canon 7) and encouraging more careful conduct. ABA 92-368 concluded that a lawyer who receives confidential materials under circumstances where it is clear that they were not intended for the receiving lawyer (a) should not examine the materials once the inadvertence is discovered, (b) should notify the sending lawyer of their receipt, and (c) should abide by the sending lawyer’s instructions as to their disposition.

The circumstances of the present inquiry present an even more compelling case against surreptitious acquisition and use of confidential or privileged information than that presented by the “inadvertent” or “unauthorized” disclosure decisions. First, to the extent that the other lawyer has “disclosed”, it is an unknowing and unwilling, rather than inadvertent or careless, disclosure. In the “inadvertent” and “unauthorized” disclosure decisions, the public policy interest in encouraging more careful conduct had to be balanced against the public policy in favor of confidentiality. No such balance need be struck here because it is a deliberate act by the receiving lawyer, not carelessness on the part of the sending lawyer, that would lead to the disclosure of client confidences and secrets.

Nor need we balance the protection of confidentiality against the principles of zealous representation expressed in Canon 7. Our Code carefully circumscribes factual and legal representations a lawyer can make, people a lawyer may contact, and actions a lawyer can take on behalf of a client. Prohibiting the intentional use of computer technology to surreptitiously obtain privileged or otherwise confidential information is entirely consistent with these ethical restraints on uncontrolled advocacy.

Although our jurisdiction does not extend to questions of law, we note that the misuse of some aspects of this technology, particularly the use of e-mail “bugs,” may violate federal or state law prohibiting unauthorized interception of e-mail content. See, e.g., The Electronic Communications Privacy Act, 18 U.S.C. §§2510 et. seq. In that event, such conduct would, of course, be unethical per se. DR 7-102(A)(8) (“In the representation of a client, a lawyer shall not . . .[k]nowingly engage in other illegal conduct or conduct contrary to a Disciplinary Rule”).

Finally, the inquiry that has prompted this opinion underscores the need for all lawyers to exercise care in using Internet based e-mail. Accordingly, we reiterate the admonition we offered in N.Y. State 709 (1998) that “lawyers must always act reasonably in choosing e-mail for confidential communications, as with any other means of communication.” 2
CONCLUSION

A lawyer may not make use of computer software applications to surreptitiously “get behind” visible documents or to trace e-mail.

Footnotes

1 The Code defines “confidence” as “information protected by the attorney-client privilege under applicable law”; the term “secret” includes all “other information gained in the professional relationship that the client has requested be held inviolate or the disclosure of which would be embarrassing or would be likely to be detrimental to the client.” DR 4-101(A).

2 As noted in N.Y. State 709 (1998), “in circumstances in which a lawyer is on notice for a specific reason that a particular e-mail transmission is at heightened risk of interception, or where the confidential information at issue is of such an extraordinarily sensitive nature that it is reasonable to use only a means of communication that is completely within the lawyer’s control, the lawyer must select a more secure means of communication than unencrypted Internet e-mail.”

NOTES

______________________________________________________________________________

______________________________________________________________________________

______________________________________________________________________________

______________________________________________________________________________

______________________________________________________________________________

______________________________________________________________________________

______________________________________________________________________________

______________________________________________________________________________

______________________________________________________________________________

______________________________________________________________________________

______________________________________________________________________________
American Bar Association Formal Opinion 06-442

REVIEW AND USE OF METADATA

August 5, 2006

The Model Rules of Professional Conduct do not contain any specific prohibition against a lawyer's reviewing and using embedded information in electronic documents, whether received from opposing counsel, an adverse party, or an agent of an adverse party. A lawyer who is concerned about the possibility of sending, producing, or providing to opposing counsel a document that contains or might contain metadata, or who wishes to take some action to reduce or remove the potentially harmful consequences of its dissemination, may be able to limit the likelihood of its transmission by "scrubbing" metadata from documents or by sending a different version of the document without the embedded information.

In modern legal practice, lawyers regularly receive e-mail, sometimes with attachments such as proposed contracts, from opposing counsel and other parties. Lawyers also routinely receive electronic documents that have been made available by opponents, such as archived e-mail and other documents relevant to potential transactions or to past events. Receipt may occur in the course of negotiation, due diligence review, litigation, investigations, and other circumstances.

E-mail and other electronic documents often contain "embedded" information. Such embedded information is commonly referred to as "metadata." [FN1] This opinion [FN2] addresses whether the ABA Model Rules of Professional Conduct permit a lawyer to review and use embedded information contained in e-mail and other electronic documents, whether received from opposing counsel, an adverse party [FN3] or an agent of an adverse party. The Committee concludes that the Rules generally permit a lawyer to do so. [FN4]

Metadata is ubiquitous in electronic documents. For example:

- Electronic documents routinely contain as embedded information the last date and time that a document was saved, and data on when it last was accessed. Anyone who has an electronic copy of such a document usually can "right click" on it with a computer mouse (or equivalent) to see that information.

- Many computer programs automatically embed in an electronic document the name of the owner of the computer that created the document, the date and time of its creation, and the name of the person who last saved the document. [FN5] Again, that information might simply be a "right click" away.

- Some word processing programs allow users, when they review and edit a document, to "redline" the changes they make in the document to identify what they added and deleted. The redlined changes might be readily visible, or they might be hidden, but even in the latter case, they often will be revealed simply by clicking on a software icon in the program.
- Some programs also allow users to embed comments in a document. The comments may or may not be flagged in some manner, and they may or may not "pop up" as a cursor is moved.
over their locations.

Other types of metadata may or may not be as well known and easily understandable as the foregoing examples. Moreover, more thorough or extraordinary investigative measures sometimes might permit the retrieval of embedded information that the provider of electronic documents either did not know existed, or thought was deleted.

Not all metadata, it should be noted, is of any consequence; most is probably of no import. In ordinary day-to-day circumstances, the embedded information that is found in most documents, such as when they were saved, or who the authors were, is unlikely to be of any interest, much less material to a matter. In some instances, however, such as when a party to a lawsuit is attempting to establish "who knew what when," the date and time that a critical document was created or who drafted it may be a critical piece of information. If a payment amount is being negotiated, then a redlined change or a comment in a draft agreement that suggests how much more the opposing party is willing to pay or how much less they might take likely is of the highest importance.

The Committee first notes that the Rules do not contain any specific prohibition against a lawyer's reviewing and using embedded information in electronic documents. [FN6] The most closely applicable rule, Rule 4.4(b), relates to a lawyer's receipt of inadvertently sent information. Even if transmission of "metadata" were to be regarded as inadvertent, [FN7] Rule 4.4(b) is silent as to the ethical propriety of a lawyer's review or use of such information. The Rule provides only that "[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." [FN8] Comment [3] to Model Rule 4.4 indicates that, unless other law requires otherwise, a lawyer who receives an inadvertently sent document ordinarily may, but is not required to, return it unread, as a matter of professional judgment. [FN9]

Some authorities have addressed questions related to a lawyer's search for, or use of, metadata under the rubric of a lawyer's honesty, and have found such conduct ethically impermissible. [FN10] The Committee does not share such a view, but instead reads the recent addition of Rule 4.4(b) identifying the sole requirement of providing notice to the sender of the receipt of inadvertently sent information, as evidence of the intention to set no other specific restrictions on the receiving lawyer's conduct found in other Rules. [FN11] 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. [FN12]

The Committee observes that counsel sending or producing electronic documents may be able to limit the likelihood of transmitting metadata in electronic documents. Computer users can avoid creating some kinds of metadata in electronic documents in the first place. For example, they often can choose not to use the redlining function of a word processing program or not to embed comments in a document. Simply deleting comments might be effective to eliminate them. Computer users also can eliminate or "scrub" some kinds of embedded information in an electronic document before sending, producing, or providing it to others. [FN13] Methods to
avoid or eliminate embedded information have been, and no doubt will continue to be, discussed in many legal programs, practice guides, and articles, [FN14] as well as in general office software publications and support web sites. The specifics of any such software are beyond the scope of this opinion.

A lawyer who is concerned about the possibility of sending, producing, or providing to opposing counsel a document that contains or might contain metadata also may be able to send a different version of the document without the embedded information. For example, she might send it in hard copy, create an image of the document and send only the image (this can be done by printing and scanning), or print it out and send it via facsimile.

Finally, if a lawyer is concerned about risks relating to metadata and wishes to take some action to reduce or remove the potentially harmful consequences of its dissemination, then before sending, producing, or otherwise making available any electronic documents, she may seek to negotiate a confidentiality agreement or, if in litigation, a protective order, that will allow her or her client to "pull back," or prevent the introduction of evidence based upon, the document that contains that embedded information or the information itself. [FN15] Of course, if the embedded information is on a subject such as her client's willingness to settle at a particular price, then there might be no way to "pull back" that information.

Footnotes

FN1. Creation of metadata is not a new phenomenon. For example, for decades, documents saved on personal computers typically have contained embedded information recording the last date and time that the documents were saved.

FN2. This opinion is based on the Model Rules of Professional Conduct as amended by the ABA House of Delegates through August 2003. The laws, court rules, regulations, rules of professional conduct and opinions promulgated in the individual jurisdictions are controlling.

FN3. 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 (Model Rule 4.1(a)), using a method of obtaining evidence that violated the legal rights of a third person (Model Rule 4.4(a)), or otherwise engaging in misconduct (Model Rule 8.4). Such scenarios are beyond the scope of this opinion.

FN4. Comment [16] to Model Rule 1.6 states, "[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 Rules 1.1, 5.1, and 5.3." Addressing whether the sending or producing lawyer acted competently in any given factual scenario is beyond the scope of this opinion. See also New York State Bar Ass'n Committee on Prof'l Eth. Op. 782 (Dec. 8, 2004), (E-mailing documents that may contain hidden data reflecting client confidences and secrets), available at http://www.nysba.org/Content/NavigationMenu/Attorney_Resources/Ethics_

FN5. The names generally are automatically derived from the name of the owner of the computer on which the document is created or from the name associated with the user identification of the person who accessed the computer program. If a document is copied and altered, it still might contain the name of the creator of the original document. Thus, the embedded information about the creator of a document or who last saved it might or might not identify the person(s) who actually created or saved it.

FN6. As stated earlier, this opinion assumes that the receiving lawyer acted lawfully and ethically in obtaining the electronic documents.

FN7. The Committee does not characterize the transmittal of metadata either as inadvertent or as advertent, but observes that the subject may be fact specific. As noted in Formal Opinion 06-440 (May 13, 2006) (Unsolicited Receipt of Privileged or Confidential Materials: Withdrawal of Formal Opinion 94-382 (July 5, 1994)), there is no Model Rule that addresses the duty of a recipient of advertently transmitted information.

FN8. Comment [2] to Rule 4.4 confirms that the word "document" includes e-mail and other electronic documents. The Comment also indicates that the notification requirement exists "in order to permit [the sender] to take protective measures," and includes a recognition that applicable other law (outside of the applicable rules of professional conduct) may require the lawyer to take additional steps beyond notification.

FN9. Rule 4.4(b) was added to the Model Rules in 2002. The clarity of its requirements provided the basis for the Committee to withdraw two of its past formal ethics opinions. First, the Committee, in Formal Opinion 05-437 (Oct. 1, 2005) (Inadvertent Disclosure of Confidential Materials: Withdrawal of Formal Opinion 92-368 (Nov. 10, 1992)), withdrew its Formal Opinion 92-368 (Nov. 10, 1992) (Inadvertent Disclosure of Confidential Materials). Formal Opinion 92-368 opined that a lawyer who receives materials that on their face appear to be subject to the attorney-client privilege or otherwise confidential under Model Rule 1.6, under circumstances where it is clear they were not intended for the receiving lawyer, should refrain from examining the materials, notify the sending lawyer, and abide by the instructions of the sending lawyer. Second, the Committee, in Formal Opinion 06-440 (May 13, 2006) (Unsolicited Receipt of Privileged or Confidential Materials: Withdrawal of Formal Opinion 94-382 (July 5, 1994)), withdrew its Formal Opinion 94-382 (July 5, 1994) (Unsolicited Receipt of Privileged or Confidential Materials). Formal Opinion 94-382 addressed the obligations under the Rules of a lawyer who is offered, or is provided, by a person not authorized to offer them, materials of an adverse party that the lawyer knows to be, or on their face appear to be, subject to the attorney-client privilege or otherwise confidential under Rule 1.6.

FN10. The Committee notes that New York State Bar Ass'n Committee on Prof'l Eth. Op. 749 (Dec. 14, 2001) (Use of computer software to surreptitiously examine and trace e-mail and other
electronic documents), available at http://www.nysba.org/Content/NavigationMenu/Attorney_Resources/Ethics_Opinions/Committee_on_Professional_Ethics_Opinion_749.htm (last visited Sept. 15, 2006) took the position that under New York's Code of Professional Responsibility, a lawyer may not "intentionally use... computer technology to surreptitiously obtain privileged or otherwise confidential information" of an opposing party. The New York committee reaffirmed that view in the opinion cited in footnote 4, supra. The Committee recognizes that Opinion 749 relies in part on language contained in present Rule 8.4(c) and (d) that prohibits engaging in conduct "involving dishonesty, fraud, deceit, or misrepresentation" or "that is prejudicial to the administration of justice." However, the Committee does not believe that a lawyer, by acting within the circumstances assumed by the instant opinion, would violate either of those paragraphs of Rule 8.4. The Committee views similarly an opinion issued for comment at the request of the Florida Bar Board of Governors by the Florida Bar Professional Ethics Committee. See Proposed Adv. Op. 06-02 (June 23, 2006), available at http://www.floridabar.org/TFB/TFBResources.nsf/Attachments/53ED6DC5599019138525719A006DCE1B/$FILE/062pao.pdf?OpenElement#search=Florida%2Bopinion%2Bmetadata (last visited Sept. 15, 2006).

FN11. We note that this interpretation was intended by the Commission on Evaluation of the Rules of Professional Conduct ("Ethics 2000 Commission"), as reported in the Reporter's Explanation of Changes, available at http://www.abanet.org/cpr/e2k/e2krule44rem.html (last visited Sept. 15, 2006), regarding this amendment.

FN12. One of the facts that might be relevant is whether the metadata is a privileged communication.

FN13. Of course, when responding to discovery, a lawyer must not alter a document when it would be unlawful or unethical to do so, 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[.]")

FN14. For example, the 2006 ABA Techshow included a roundtable program on metadata, and a number of publications and items available on ABA web site pages of the ABA General Practice, Solo & Small Firm Division and the ABA Law Practice Management Section have addressed metadata from practical and ethical perspectives.

FN15. On April 12, 2006, the Supreme Court of the United States approved extensive amendments to the Federal Rules of Civil Procedure relating to discovery of electronic documents, available at http://www.uscourts.gov/rules/newrules6.html#cv0804 (last visited September 15, 2006). Among other provisions, certain of the amendments allow a producing party to pull back privileged information and work product under certain circumstances. The amendments will be effective on December 1, 2006, unless Congress enacts legislation to reject, modify, or defer them.
Florida Ethics Opinion 06-02

September 15, 2006

A lawyer who is sending an electronic document should take care to ensure the confidentiality of all information contained in the document, including metadata. A lawyer receiving an electronic document should not try to obtain information from metadata that the lawyer knows or should know is not intended for the receiving lawyer. A lawyer who inadvertently receives information via metadata in an electronic document should notify the sender of the information’s receipt. The opinion is not intended to address metadata in the context of discovery documents.

RPC: 4-1.1, 4-1.2, 4-1.4, 4-1.6, 4-4.4(b)

The Board of Governors of The Florida Bar has directed the committee to issue an opinion to determine ethical duties when lawyers send and receive electronic documents in the course of representing their clients. These ethical responsibilities are now becoming issues in the practice of law where lawyers may be able to “mine” metadata from electronic documents. Lawyers may also receive electronic documents that reveal metadata without any effort on the part of the receiving attorney. Metadata is information about information and has been defined as “information describing the history, tracking, or management of an electronic document.”

Metadata can contain information about the author of a document, and can show, among other things, the changes made to a document during its drafting, including what was deleted from or added to the final version of the document, as well as comments of the various reviewers of the document. Metadata may thereby reveal confidential and privileged client information that the sender of the document or electronic communication does not wish to be revealed.

This opinion does not address metadata in the context of documents that are subject to discovery under applicable rules of court or law. For example, the opinion does not address the role of the
lawyer acting as a conduit to produce documents in response to a discovery request.

The Florida Rules of Professional Conduct require lawyers to protect information that relates to the representation of a client. Rule 4-1.6(a) provides as follows:

(a) Consent Required to Reveal Information. A lawyer shall not reveal information relating to representation of a client except as stated in subdivisions (b), (c), and (d), unless the client gives informed consent.

The Comment to Rule 4-1.6 further provides:
A fundamental principle in the client-lawyer relationship is that the lawyer maintain confidentiality of information relating to the representation. The client is thereby encouraged to communicate fully and frankly with the lawyer even as to embarrassing or legally damaging subject matter.

In order to maintain confidentiality under Rule 4-1.6(a), Florida lawyers must take reasonable steps to protect confidential information in all types of documents and information that leave the lawyers’ offices, including electronic documents and electronic communications with other lawyers and third parties.

Rule 4-4.4(b) addresses inadvertent disclosure of information and provides as follows:
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 comment to rule 4-4.4 provides additional guidance:

Subdivision (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 such 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.

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 4-1.2 and 4-1.4.

The duties of a lawyer when sending an electronic document to another lawyer and when receiving an electronic document from another lawyer are as follows:
(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 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. See, Ethics Opinion 93-3 and Rule 4-4.4(b), Florida Rules of Professional Conduct, effective May 22, 2006.

(3) 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.

The foregoing 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 under Rule 4-1.6(a). As set forth in the Comment to Rule 4-1.1, regarding competency:

To maintain the requisite knowledge and skill [for competent representation], a lawyer should engage in continuing study and education.

Footnotes

1 The Sedona Guidelines: Best Practice Guidelines and Commentary for Managing Information and Records in the Electronic Age, Appendix F (The Sedona Conference Working Group Series, Sept. 2005 Series), available at http://www.thesedonaconference.org. The Microsoft Word and Microsoft Office online sites also contain detailed information about metadata, showing examples of metadata that may be stored in Microsoft applications and explaining how to remove this information from a final document. Examples of metadata that may be hidden in Microsoft documents include the name of the author, the identification of the computer on which the document was typed, the names of previous document authors and revisions to the document, including prior versions of a final document.

The ethical implications of such hidden information in electronic documents have been discussed in legal journals and ethics opinions in other states. The New York Bar Association has issued Opinion 749 (2001), which concluded that attorneys may not ethically use computer software applications to surreptitiously “mine” documents or to trace e-mail. New York Ethics Opinion 782 (2004), further concluded that New York 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. Legal commentators have published articles about ethical issues involving metadata. David Hricik and Robert B. Jueneman, “The Transmission and Receipt of Invisible Confidential Information,” 15 The Professional Lawyer No. 1, p. 18 (Spring 2004). See also, Brian D. Zall, “Metadata: Hidden Information in Microsoft Work Documents and its Ethical Implications,” 33 Colo. Lawyer No.10, p. 53 (Oct. 2004).

NOTES
You have raised several questions, in the context of litigation, concerning the ethics of viewing and/or using metadata under The Maryland Lawyers' Rules of Professional Conduct ("Maryland Rules of Professional Conduct" or "Maryland Rule"). For purposes of this Opinion, the Ethics Committee adopts your definition of "metadata" as being information within programs (e.g., Microsoft Word/Excel/Power Point, Corel Word Perfect/Quattro Pro, Adobe Acrobat, etc.) which is not readily visible but which is accessible and which may include data such as author, dates of creation/printing, number of revisions, content of those revisions/previous versions, editing time, etc.

You raise three questions in your inquiry: first, whether it is ethical for the attorney recipient to view or use metadata in documents produced by another party; second, whether the attorney sender has any duty to remove metadata from the files prior to sending them; and third, whether the attorney recipient has any ethical duty not to view or otherwise use the metadata without first ascertaining whether the sender intended to include such metadata in the produced documents. By referring to "attorney," we include non-lawyer assistants over whom the attorney has supervisory responsibility. See Maryland Rule 5.3.

The questions you raise have not previously been considered by the Ethics Committee. Because of the relatively recent growth of electronic discovery, technology associated therewith, and developing rules of procedure and case law, there is not a lot of precedent and, furthermore, it is impossible to cover every conceivable situation which may arise with respect to the issues raised by your inquiries. Accordingly, the scope of this Opinion will be general in nature, recognizing that some of the general principles discussed below may be subject to modification depending upon specific factual situations and/or legal requirements.

The Committee believes that your first and third inquiries can be discussed together, namely whether the recipient attorney of electronic discovery containing metadata may view or use that metadata without first ascertaining whether the sender attorney inadvertently or intentionally included the metadata in the production of the electronic discovery. Subject to any legal standards or requirements (case law, statutes, rules of procedure, administrative rules, etc.), this Committee believes that there is no ethical violation if the recipient attorney (or those working under the attorney's direction) reviews or makes use of the metadata without first ascertaining whether the sender intended to include such metadata. The Committee's opinion in this regard is heavily influenced by the difference between the Maryland Rules of Professional Conduct and the American Bar Association's Model Rules of Professional Conduct. In February 2002, the ABA Model Rules of Professional Conduct were amended to add Rule 4.4(b), which states that "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." In Formal Opinion 05-437, the ABA Standing Committee on Ethics and Professional Responsibility pointed out that while Rule 4.4(b) obligated the receiving lawyer to
notify the sender of the inadvertent transmission promptly, the Rule did "not require the receiving lawyer either to refrain from examining the materials or to abide by the instructions of the sending lawyer." Comment 2 to Model Rule 4.4 explains that "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."

The Maryland Rules of Professional Conduct, however, have not been amended to include Model Rule 4.4(b). Accordingly, the Maryland Rules of Professional Conduct do not require the receiving attorney to notify the sending attorney that there may have been an inadvertent transmittal of privileged (or, for that matter, work product) materials. Of course, the receiving lawyer can, and probably should, communicate with his or her client concerning the pros and cons of whether to notify the sending attorney and/or to take such other action which they believe is appropriate. See generally Rule 1.4 (communications with client concerning certain matters involving the representation).[1]

Although this Committee does not opine on legal issues, the Committee believes it is appropriate in this instance to point out how the lack of an ethical obligation to notify the sender or to return the privileged or work-product documents to the sender may be impacted, at least in terms of federal court litigation, by certain amendments to the Federal Rules of Civil Procedure which go into effect on December 1, 2006 and which pertain to electronic discovery. Recognizing the complexity of electronic discovery and, perhaps, anticipating that inadvertent production of privileged or work product material may well be an ongoing problem, proposed Federal Rule 16(b)(5) and (6) as part of the requirement that the parties confer and work out an initial scheduling order, encourages the parties to meet and discuss possible provisions for disclosure or discovery of electronically stored information, and try to reach agreements concerning the assertion of claims of privilege or protection as to trial-preparation materials even after production of such documents. Any such agreements would supersede the ethical standard described above because the parties, and their counsel, would be obligated to conduct themselves in accordance with the terms of any such agreement; otherwise, the attorney could well be in violation of Rule 8.4(b) by engaging in conduct that is prejudicial to the administration of justice.

Proposed Federal Rule 26(b)(5) provides as follows:
"Information produced. If information is produced in discovery that is subject to a claim of privilege or 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 receiving 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."

Accordingly, the lack of any ethical prohibition concerning the review and/or use of metadata discussed earlier in this Opinion would, at least in the arena of federal litigation, be superseded by the legal requirements set forth in the Federal Rules which go into effect on December 1, 2006, and any violation of those Federal Rules would in all likelihood constitute a violation of
Finally, you inquire as to whether the attorney sending the electronic discovery has a duty to remove metadata from the files prior to production thereof. The Committee believes that, absent an agreement with the other parties (such as is contemplated in proposed Federal Rules 16(b)(5) and (6), the sending attorney has an ethical obligation to take reasonable measures to avoid the disclosure of confidential or work product materials imbedded in the electronic discovery. The Committee believes that this ethical obligation arises out of a combination of Rule 1.1, which provides that a lawyer shall provide competent representation to a client, together with Rule 1.6, which obligates the lawyer not to reveal confidential information relating to the representation of a client. See generally, New York State Bar Association Committee on Professional Ethics Opinion 782 (2004), concluding that attorneys have an obligation to "stay abreast of technological advances" and to behave reasonably in accordance with the risks involved in the technology they use. This is not to say, however, that every inadvertent disclosure of privileged or work product material would constitute a violation of Rules 1.1 and/or 1.6 since each case would have to be evaluated based on the facts and circumstances applicable thereto.

We thank you for your inquiry and hope that the foregoing is responsive thereto. Opinions of the Committee may be obtained from the MSBA web site: www.msba.org.

Footnotes

1] Comment 3 to ABA Model Rule 4.4 states that where an attorney is not required by applicable law to return an inadvertently produced document, "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."


NOTES
Alabama State Bar Ethics Opinion 2007-02

DISCLOSURE AND MINING OF METADATA

March 14, 2007

QUESTION #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?

ANSWER:
Lawyers have a duty under Rule 1.6 to use reasonable care when transmitting electronic documents to prevent the disclosure of metadata containing client confidences or secrets.

QUESTION #2:
Is it unethical for an attorney to mine metadata from an electronic document he or she receives from another party?

ANSWER:
Absent 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.

DISCUSSION:
The recent proliferation of electronic discovery, e-filing, and use of e-mail has created an ethical dilemma surrounding the disclosure and mining of metadata. For the purposes of this Opinion, metadata may be loosely defined as data hidden in documents that is generated during the creation of those documents.1 Metadata is most often generated by software programs, such as Microsoft Word and Corel WordPerfect.2 These programs are frequently used by attorneys in the creation and drafting of legal documents.

The act of deliberately seeking out and viewing metadata embedded in a document is most often referred to as “mining” the document. Mining metadata allows a person to learn a variety of information about the history and evolution of an electronic document, including: the author, the name of previous document authors, template information, and hidden text.3 By mining an electronic document, a recipient attorney could also view revisions made to the document, comments added by other users that reviewed the document, and whether the document was drafted from a template. The disclosure of metadata contained in an electronic submission to an opposing party could lead to the disclosure of client confidences and secrets, litigation strategy, editorial comments, legal issues raised by the client, and other confidential information.

For example, say your firm is filing a motion to summarily dismiss a lawsuit and the motion is electronically distributed among the firm’s attorneys for review and comments. In reviewing the motion, the other attorneys insert comments critiquing the firm’s position and discussing the strengths and weaknesses of various legal positions. The motion is then electronically
transmitted to opposing counsel. If you failed to “scrub” or remove the hidden metadata prior to transmission, the opposing party could mine the document’s metadata and discover which attorneys reviewed the motion, the critiques about the viability or strength of certain arguments, and the subsequent revisions made to the document.4

Another example demonstrating the inherent danger of electronically transmitting documents involves the use of templates. Many attorneys routinely recycle templates for common filings, in which the current client’s name is substituted in place of a prior client’s name. If the document is later electronically transmitted to the opposing party, the opposing party could mine the document and discover the original client’s name and information. Such disclosure of client identity and information could constitute a violation of Rule 1.6, Alabama Rules of Professional Conduct. The protection of the confidences and secrets of a client are among the most significant obligations imposed on a lawyer. Rule 1.6, Ala. R. Prof. C., provides that: “(a) A lawyer shall not reveal information relating to representation of a client unless the client consents after consultation, except for disclosures that are impliedly authorized in order to carry out the representation, and except as stated in paragraph (b)."

The Comment to Rule 1.6, Ala. R. Prof. C., states, in pertinent part: “The observance of the ethical obligation of a lawyer to hold inviolate confidential information of the client not only facilitates the full development of facts essential to proper representation of the client but also encourages people to seek early legal assistance.

Almost without exception, clients come to lawyers in order to determine what their rights are and what is, in the maze of laws and regulations, deemed to be legal and correct. The common law recognizes that the client’s confidences must be protected from disclosure. Based upon experience, lawyers know that almost all clients follow the advice given, and the law is upheld.

A fundamental principle in the client-lawyer relationship is that the lawyer maintains confidentiality of information relating to the representation. The client is thereby encouraged to communicate fully and frankly with the lawyer even as to embarrassing or legally damaging subject matter.”

As such, the Commission believes 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.

The determination of whether an attorney exercised reasonable care will, of course, vary according to the circumstances of each individual case. Factors in determining whether reasonable care was exercised 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. For example, an attorney would need to exercise greater care in submitting an electronic document to an opposing party than he or she would if e-filing a pleading with the court. There is simply a much higher likelihood that an adverse party would attempt to mine metadata, than a neutral and detached court.

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. In N.Y. State Bar Opinion 749, the New York State Bar concluded that the use of
computer technology to access client confidences and secrets revealed in metadata constitutes
The Commission agrees that the use of computer technology in the manner described above
constitutes an impermissible intrusion on the attorney-client relationship in violation of the
Alabama Rules of Professional Conduct. As discussed earlier, the protection of the confidences
and secrets of a client is a fundamental tenet of the legal profession.

The unauthorized mining of metadata by an attorney to uncover confidential information would
be a violation of the Alabama Rules of Professional Conduct. Rule 8.4, Ala. R. Prof. C., provides
that it is misconduct for an attorney to, among other things:
“(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;”

In Formal Opinion 749, the New York State Bar adroitly observed 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.” (2001)
The Disciplinary Commission agrees. The mining of metadata constitutes a knowing and
deliberate attempt by the recipient attorney to acquire confidential and privileged information in
order to obtain an unfair advantage against an opposing party.

One possible exception to the prohibition against the mining of metadata involves electronic
discovery. Recent court decisions indicate that parties may be sanctioned for failing to provide
metadata along with electronic discovery submissions.5 In certain cases, metadata evidence may
be relevant and material to the issues at hand. For example, the mining of an email may be vital
in determining the original author, who all received a copy of the email, and when the email was
viewed by the recipient. In Enron type litigation, the mining of metadata may be a valuable tool
in tracking the history of accounting decisions and financial transactions.

The production of metadata during discovery will ordinarily be a legal matter within the sole
discretion of the courts. The Commission advises attorneys, however, to be cognizant of the
issue of disclosing metadata during discovery. Both parties should seek direction from the court
in determining whether a document’s metadata is to be produced during discovery.

This opinion is consistent with Formal Opinions 749 and 782 of the New York State Bar and
some of the language herein is derived from that opinion.
Footnotes


3 Brian D. Zall , Metadata: Hidden Information in Microsoft Documents and Its Ethical Implications, 33 The Colorado Lawyer 83 (October 2004)


District of Columbia Ethics Opinion 341

REVIEW AND USE OF METADATA IN ELECTRONIC DOCUMENTS

September, 2007

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.

Applicable Rules

Rule 1.6 (Confidentiality of Information)
Rule 3.4 (Fairness to Opposing Party and Counsel)
Rule 4.4 (Respect For Rights of Third Persons)
Rule 8.4 (Misconduct)

Inquiry. We have received numerous inquiries concerning a lawyer’s obligations regarding metadata that is imbedded in electronic documents received from opposing counsel. Metadata is electronically stored information, typically not visible from the face of the document as printed out or as initially shown on the computer screen, but which is imbedded in the software and retrievable by various means. Often described as "data about data," metadata provides information regarding the creation and modification of a document, and sometimes includes comments by persons participating in the creation or modification of the document.[1] To the uninitiated, metadata is hidden and perhaps unknown, but to competent computer-users, the existence of metadata is well known and may be a simple "click" or two away. The information that is embedded is often mundane and of little or no interest, but in some instances it may reveal significant information.

In assessing the ethical obligations of both the sending and receiving lawyer with respect to metadata, we find it useful to distinguish between electronic documents provided in discovery or pursuant to a subpoena from those electronic documents voluntarily provided by opposing counsel. Although the Florida and Alabama Bars have recognized a similar distinction, see Florida Bar Op. 06-2; Alabama State Bar, Office of Gen. Counsel Op. No. R0-2007-02, the distinction has not been universally recognized in other ethics opinions addressing metadata. See ABA Formal Op. 06-442; Maryland Bar Ass’n Ethics Docket No. 2007-09.
Analysis

A. Electronic Documents Provided Outside of Discovery

1. The Sending Lawyer

Lawyers sending electronic documents outside of the context of responding to discovery or subpoenas have an obligation under Rule 1.6 to take reasonable steps to maintain the confidentiality of documents in their possession. This 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. See N.Y. State Bar Ass’n Committee Op. 782. Accordingly, lawyers must either acquire sufficient understanding of the software that they use or ensure that their office employs safeguards to minimize the risk of inadvertent disclosures. [2]

2. The Receiving Lawyer

More often than not, the exchange of metadata between lawyers is either mutually helpful or otherwise harmless. Lawyers routinely exchange contracts, stipulations, and other documents that include “track changes” or other software features which highlight suggested modifications. Similarly, spreadsheets include necessary metadata such as formulas for the columns and rows, thereby providing a useful understanding of the calculations made.

But when a receiving lawyer has actual knowledge that the sender inadvertently included metadata in an electronic document, we believe that the principles stated in Opinion Nos. 256 and 318 relating to inadvertent production of privileged material should be used in determining the receiving lawyer’s obligations. In Opinion No. 256, we stated that, where a lawyer knows that a privileged document was inadvertently sent, it is a dishonest act under D.C. Rule 8.4(c) for the lawyer to review and use it without consulting with the sender. We reached a similar conclusion in Opinion No. 318, regarding the receipt of documents from third parties. However, we noted in Opinion 318 that, where the privileged nature of the document is not apparent on its face, there is no obligation to refrain from reviewing it, and the duty of diligent representation under D.C. Rule 1.3 may trump confidentiality concerns.

Consistent with Opinion No. 256, we agree generally with the New York and Alabama Bars to the extent that they have found Rule 8.4(c) to be implicated when a receiving lawyer wrongfully “mines” an opponents’ metadata. See N.Y. State Bar Ass’n Committee Op. 749 (concluding that lawyers have an obligation not to exploit an inadvertent or unauthorized transmission of client confidences or secrets and that “use of such information ... [is] conduct ‘involving dishonesty, fraud, deceit or misrepresentation’”); and Alabama State Bar, Office of Gen. Counsel Op. No. R0-2007-02 (finding that “[t]he unauthorized mining of metadata by an attorney to uncover confidential information would be a violation of ... Rule 8.4”).

In our view, however, Rule 8.4 is implicated only when the receiving lawyer has actual prior knowledge that the metadata was inadvertently provided. Given the ubiquitous exchange of
electronic documents and the sending lawyers’ obligation to avoid inadvertent productions of metadata, we believe that 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 the metadata. This standard is consistent with our conclusion in Opinion No. 256.[3]

Where there is such actual prior knowledge by the receiving lawyer as to the inadvertence of the sender, then notwithstanding the negligence or even ethical lapse of the sending lawyer, 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.[4] If the sending lawyer advises that such 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 his right to challenge the claim of privilege and obtain an adjudication, where appropriate.

A receiving lawyer may have such actual prior knowledge if he is told by the sending lawyer of the inadvertence before the receiving lawyer reviews the document. Such actual knowledge may also exist where a receiving lawyer immediately notices upon review of the metadata that it is clear that protected information was unintentionally included. These situations will be fact-dependent, but can arise, for example, where the metadata includes a candid exchange between an adverse party and his lawyer such that it is “readily apparent on its face,” D.C. Ethics Op. 318, that it was not intended to be disclosed. As we stated in Opinions 256 and 318, a prudent receiving lawyer who is uncertain whether the sender intended to include particular information should contact the sending lawyer to inquire.

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.

Although the purpose of Rule 4.4(b) was to address the inadvertent disclosure of entire documents (whether electronic or paper),[6] we see no reason why it would not also apply to an inadvertently transmitted portion of a writing that is otherwise intentionally sent.
B. Electronic Documents Provided in Discovery or Pursuant to a Subpoena

When metadata is provided in discovery or pursuant to a subpoena, the rules of professional conduct are not the only rules of which lawyers must be aware. Although such other rules lie outside our jurisdiction, we note that the Federal Rules of Civil Procedure now provide steps to identify and address issues related to electronic discovery. See F. R. Civ. P. 16(b), 26 (f), 33(d), 34(a) and 37(f) (effective Dec. 1, 2006). Under these new rules, parties are required to consult at the outset of a case about the nature of pertinent electronic documents in their possession and the manner in which they are maintained. This should include specific discussions as to whether a receiving party 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.

Although decided prior to the implementation of the amended federal rules, the case of Williams v. Sprint/United Mgt., 230 F.R.D. 640 (D. Kan. 2005), illustrates how metadata may be considered probative evidence in litigation. In Williams, plaintiff employees brought a class action claiming age discrimination in connection with a reduction-in-force ("RIF"), and they sought and obtained from the defendant electronic versions of Excel spreadsheets that were created and used by the defendant to identify pools of employees subject to the RIF. The defendant "scrubbed" the metadata from these spreadsheets before producing them, and plaintiffs objected. They moved to compel production of the metadata as originally maintained. The court held that because the metadata could be relevant in determining whether defendants had manipulated the employee pools as alleged, defendants had to provide the metadata to plaintiffs.[7]

1. The Sending Lawyer in the Discovery/Subpoena Context

D.C. Rule 3.4(a) provides the relevant guidance for lawyers providing access to tangible evidence in discovery:

A lawyer shall not ...Obstruct another party’s access to evidence or alter, destroy, or conceal evidence, or counsel 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. Unless prohibited by law, a lawyer may receive physical evidence of any kind from the client or from another person.

Because it is impermissible to alter electronic documents that constitute tangible evidence, the removal of metadata may, at least in some instances, be prohibited as well.[8] In addition to issues regarding discovery sanctions, the alteration or destruction of evidence can, under some circumstances, also constitute a crime. See D.C. Rule 3.4, Comment [4].

2. The Receiving Lawyer in the Discovery/Subpoena Context

In view of the obligations of a sending lawyer in providing electronic documents in response to a discovery request or subpoena, a receiving lawyer is generally justified in assuming that metadata was provided intentionally. Moreover, when a document is sought in discovery or
through subpoena, the scope of what is protected is narrowed from anything that is a confidence or secret to that material which falls within an evidentiary privilege. See D.C. Rule 1.6(e)(2)(A); Adams v. Franklin, No. 05-CV-233, slip op. at 5 (D.C. May 10, 2007) (“the lawyer’s ethical duty to preserve a client’s confidences and secrets is broader [than] the attorney-client privilege”).

In addition, 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. See D.C. Rules 1.1, 1.3. The electronic document is similar to any other tangible evidence that the lawyer is expected to review in order to advance her client’s interests. Where useful, for example, the lawyer in such instances may consult with a computer expert to determine the means by which the metadata can be most fully revealed and reviewed, much as a lawyer does with a finger-print expert.[9]

Notwithstanding all this, even in the context of discovery or other judicial process, if a receiving lawyer has actual knowledge that metadata containing protected information was inadvertently sent by the sending lawyer, the receiving lawyer, under Rule 8.4(c), should advise the sending lawyer and determine whether such protected information was disclosed inadvertently. See D.C. Ethics Op. 256 (“The line we have drawn between an ethical and an unethical use of inadvertently disclosed information is based on the receiving lawyer’s knowledge of the inadvertence of the disclosure.”). If the sender advises that protected information was unintentionally provided, then the receiving lawyer should follow the directives of the sending lawyer regarding the disposition of the electronic document. Under these circumstances, however, the receiving 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. Of course, this is all subject to applicable rules of procedure and court orders that may otherwise govern.[10]

Conclusion

We conclude that when a receiving lawyer has actual knowledge that an adversary has inadvertently provided metadata in an electronic document, the lawyer should not review the metadata without first consulting with the sender and abiding by the sender’s instructions. In all other circumstances, a receiving lawyer is free to review the metadata contained within the electronic files provided by an adversary.

Footnotes

1. The Federal Judicial Center recently issued a publication on electronic discovery that defined the term “metadata” as

[i]Information about a particular data set or document which describes how, when, and by whom the data set or document was collected, created, accessed, or modified; its size; and how it is formatted. Some metadata, such as file dates and sizes, can easily be seen by users; other metadata can be hidden from users but are still available to the operating system or the program
used to process the data set or document.


3. By stating that the standard for a violation is “actual knowledge,” we do not condone a situation in which a lawyer employs a system to mine all incoming electronic documents in the hope of uncovering a confidence or secret, the disclosure of which was unintended by some hapless sender. The Rules of Professional Conduct are “rules of reason,” Scope [1], and a lawyer engaging in such a practice with such intent cannot escape accountability solely because he lacks “actual knowledge” in an individual case. Moreover, as stated in Rule 1.0(f), “[a] person’s knowledge may be inferred from circumstances.”

4. In Opinion No. 256, we discussed the analogous situation of a lawyer who finds a wallet in the street. Here, the more appropriate analogy may be to a lawyer who inadvertently leaves his briefcase in opposing counsel’s office following a meeting or a deposition. The one lawyer’s negligence in leaving the briefcase does not relieve the other lawyer from the duty to refrain from going through that briefcase, at least when it is patently clear from the circumstances that the lawyer was not invited to do so.

5. In its Opinion No. 2007-09, the Maryland Bar also concluded that Rule 8.4(c) is not implicated by a receiving lawyer’s accessing metadata. But the Maryland Bar relied on its version of Rule 4.4, which has not been amended to impose any obligation on the lawyer who receives an inadvertently produced document. The Maryland Bar stated that its opinion was “heavily influenced by the difference between the Maryland Rules of Professional Conduct and [ABA Model Rule 4.4].” D.C. Rule 4.4(b), by contrast, imposes upon the receiving lawyer an obligation not only to contact the sending lawyer (as the Model Rule requires), but also to abide by the sending lawyer’s instructions regarding the return or destruction of the document.

6. Under D.C. Rule 1.0(o), a “writing” is defined as “a tangible or electronic record of a communication or representation, including handwriting, typewriting, printing, photostating, photography, audio or video recording, and e-mail.”

7. By citing Williams, we do not necessarily mean to endorse its holding or to provide any guidance with respect to the rules of discovery. See Speedway v. NASCAR, Inc., 2006 U.S. Dist. LEXIS 92028 (E.D. Ky. Dec. 18, 2006) (criticizing the specific holding in Williams). Rather, we cite Williams merely to illustrate that courts have required the production of metadata as probative evidence, and we discuss below the implications of this conclusion for the responsibilities of lawyers under the rules of professional conduct.
8. This is not to suggest that all metadata should be treated alike. For example, a Joint Court-Bar Committee of the United States District Court for the District of Maryland has issued a suggested protocol that defines and distinguishes between different kinds of metadata, only some of which are subject to routine production. See Suggested Protocol for Discovery of Electronically Stored Information, In re: Electronically Stored Information, ¶11 (D. Md.), www.mdd.uscourts.gov/localrules/localrules.html. The purpose of the protocol is “to facilitate the just, speedy, and inexpensive conduct of discovery involving [electronically stored information or ‘ESI’] in civil cases, and to promote, whenever possible, the resolution of disputes regarding the discovery of ESI without Court intervention.” Id. ¶1.

9. In concluding that a lawyer may review metadata in documents produced in discovery (that is, unless and until the lawyer has actual knowledge that the metadata contains protected information), we do not intend to suggest that a lawyer must undertake such a review. Whether as a matter of courtesy, reciprocity, or efficiency, “a lawyer may decline to retain or use documents that the lawyer might otherwise be entitled to use, although (depending on the significance of the documents) this might be a matter on which consultation with the client may be necessary.” D.C. Ethics Op. 256, n.7 (citing D.C. Rules 1.2(a) and 1.4(b)); see also D.C. Ethics Op. 318, n.5.

10. When in litigation, an attorney must comply with the applicable rules of procedure of the court in which the litigation resides. In this regard, for example, Rule 26(b)(5)(B) of the Federal Rules of Civil Procedure requires a lawyer who is informed by opposing counsel that an allegedly privileged document was produced, to return, sequester or destroy the document until the court adjudicates the claim of privilege. See also D.C. Rule 3.4(c) (requiring a lawyer to comply with the rules of a presiding tribunal).

NOTES
I. Introduction

This Formal Opinion provides ethical guidance to lawyers on the subject of metadata received from opposing counsel in electronic materials, including documents, spreadsheets and PowerPoint presentations under circumstances in which it is clear that the materials were not intended for the receiving lawyer. As more fully set forth below, it is the opinion of this Committee that each attorney must, as the Preamble to the Rules of Professional Conduct states, "resolve [the issue] through the exercise of sensitive and moral judgment guided by the basic principles of the Rules" and determine for himself or herself whether to utilize the metadata contained in documents and other electronic files based upon the lawyer's judgment and the particular factual situation.

In reaching this conclusion, the Committee notes that there is no specific Pennsylvania Rule of Professional Conduct determining the ethical obligations of a lawyer receiving inadvertently transmitted metadata from another lawyer, his client or other third person; and, there is no specific Pennsylvania Rule of Professional Conduct requiring the receiving lawyer to assess whether the opposing lawyer has violated any ethical obligation to the lawyer's client. Thus, the decision of how or whether a lawyer may use the information contained in the metadata will depend upon many factors, including:

- 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\(^1\);

\(^1\) Comment 1 to R.P.C. 1.3 states:

[1] A lawyer should pursue a matter on behalf of a client despite opposition, obstruction or personal inconvenience to the lawyer, and take whatever lawful and ethical measures are required to vindicate a client's cause or endeavor. A lawyer must also act with commitment and dedication
• 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.

Although the waiver of the attorney-client privilege with respect to privileged and confidential materials is a matter for judicial determination, the Committee believes that the inadvertent transmissions of such materials should not constitute a waiver of the privilege, except in the case of extreme carelessness or indifference.

II. **Background**

Metadata, which means “information about data,” is data contained within electronic materials that is not ordinarily visible to those viewing the information. 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. Metadata generally contains seemingly harmless information. However, 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.

---

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 Version X3 permits a user to easily remove all or specific metadata. Microsoft Office products do not permit the easy removal of this information. 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/290945) and [http://support.microsoft.com/kb/223790](http://support.microsoft.com/kb/223790).

4 The Microsoft Office website contains detailed information about metadata, provides examples of metadata that may be stored in materials created by Microsoft applications, and explains how to remove this data from a document. Examples of metadata that may
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

Pa.R.P.C. 1.6 ("Confidentiality of Information") governs an attorney’s disclosure of information relating to the representation of a client. The Rule 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).

The Comment to Rule 1.6 states in relevant part:

[2] A fundamental principle in the client-lawyer relationship is that, in the absence of the client’s informed consent, the lawyer must not reveal information relating to the representation. See Rule 1.0(c) for the definition of informed consent. This contributes to the trust that is the hallmark of the client-lawyer relationship. The client is thereby encouraged to seek legal assistance and to communicate fully and frankly with the lawyer even as to embarrassing or legally damaging subject matter. The lawyer needs this information to represent the client effectively and, if necessary, to advise the client to refrain from wrongful conduct. Almost without exception, clients come to lawyers in order to determine their rights and what is, in the complex of laws and regulations, deemed to be legal and correct. Based upon experience, lawyers know that almost all clients follow the advice given, and the law is upheld.

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.
[3] The principle of client-lawyer confidentiality is given effect by related bodies of law: the attorney-client privilege, the work product doctrine and the rule of confidentiality established in professional ethics. The attorney-client privilege and work-product doctrine apply in judicial and other proceedings in which a lawyer may be called as a witness or otherwise required to produce evidence concerning a client. The rule of client-lawyer confidentiality applies in situations other than those where evidence is sought from the lawyer through compulsion of law. The confidentiality rule, for example, applies not only to matters communicated in confidence by the client but also to all information relating to the representation, whatever its source. A lawyer may not disclose such information except as authorized or required by the Rules of Professional Conduct or other law. See also Scope.

[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.

The Comment, “Acting Competently to Preserve Confidentiality,” further states:

[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.

[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.
In addition, Rule 4.4(b) ("Respect for Rights of Third Persons") 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 Comment to Rule 4.4 states:

[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.

When Rule 4.4(b) and the Comments to the Rule are read in conjunction with Rule 1.6, it is possible to conclude that the Pennsylvania Supreme Court has determined that attorneys in Pennsylvania who receive inadvertently disclosed documents have an ethical obligation to promptly notify the sender in order to permit that person to take protective measures. The absence of a specific Rule addressing the inadvertent disclosure of metadata may also be viewed as analogous to the inadvertent disclosure of a document and not an act consciously undertaken by counsel.

Various Ethics Committees have considered whether it is ethically permissible to review the metadata contained within documents produced by opposing counsel.

The American Bar Association Standing Committee on Ethics and Professional Responsibility considered the review and use of metadata in Formal Opinion 96-442 (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.” Id. 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 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. Id. 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...” Id. 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. Id. 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.

Consistent with the ABA Opinion, the District of Columbia Bar Association issued Ethics Opinion 341 in September 2007, in which it concluded:

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 works product of the sending lawyer or confidences or secrets of the sending lawyer’s client.

The D.C. Bar further opined that, “In all other circumstances, a receiving lawyer is free to review the metadata contained within the electronic files provided by an adversary.”

Several Ethics Opinions issued by various states have concluded, contrary to the ABA and D.C. Committees, that a party may not use inadvertently disclosed metadata. 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. 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

34
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.

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 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 “Lawyers- 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 F.C.R.P.C. 41.6(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 41.6(a). Id. With respect to receiving attorneys, the Committee relied on F.C.R.P.C. 44.4(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 44.4(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 41.6(a),” noting that Rule 41.6’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.
In a similar vein, the Maryland State Bar Association Committee on Ethics issues 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.

These various opinions reach different conclusions, although each offers a persuasive rationale. This Committee believes, however, that it would be difficult to establish a rule applicable in all circumstances and that, consequently, 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.

IV. Conclusion

The utilization of metadata by attorneys receiving electronic documents from an adverse party is an emerging problem. Although 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.

Therefore, this Committee concludes that, under the Pennsylvania Rules of Professional Conduct, each attorney must determine for himself or herself whether to utilize the metadata contained in documents and other electronic files based upon the lawyer’s judgment and the particular factual situation. This determination should be based upon 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. Although the waiver of the attorney-client privilege with respect to privileged and confidential materials is a matter for judicial determination, the Committee believes that the inadvertent transmissions of such materials should not constitute a waiver of the privilege, except in the case of extreme carelessness or indifference.

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.
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. 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. 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.

---

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. 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 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(c), is required by these Rules;
46

(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.2

---

2 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(D)(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.
While modern electronic communications are often greatly beneficial to the client, lawyers who use them to send or receive documents or other communications on behalf of clients must be aware that they carry certain risks. Lawyers must take reasonable precautions to prevent inadvertent disclosure of confidential information.

Except in the specific circumstances described in this opinion, a lawyer who receives an electronic communication may not examine it for the purpose of discovering the metadata embedded in it.

FACTS

This opinion addresses the ethical duties of lawyers who send and receive electronic communications. Such communications may contain metadata. Metadata is information describing the document’s history, tracking, and management. Metadata may also include hidden information, such as track changes, comments, and other information. By “mining” the metadata in a document, it may be possible to identify the author of the document, the changes made to the document during the various stages of its preparation and revision, comments made by the persons who prepared or reviewed the document, and other documents embedded within the document.

For example, a lawyer who is preparing a document may electronically circulate the document in draft form among other lawyers in the firm for their review and comment. The other lawyers may insert their suggested revisions and other comments, some of which might address the strengths and weaknesses of the client’s position. If the final version of the document is electronically transmitted to opposing counsel, it may be possible for opposing counsel to discover the comments.

The sender of the document may not be aware of the metadata embedded within the document or that it remains in the electronic document despite the sender’s good faith belief that it was “deleted.” In most cases, metadata is inconsequential or otherwise known to the recipient of the document. In some situations, though, the metadata in the electronic document may permit the recipient of the document to obtain information that is confidential or privileged from disclosure. Given the importance of this subject matter, the Committee has determined that it is appropriate to issue a sua sponte opinion for the guidance of lawyers in Arizona.

QUESTIONS PRESENTED

1. If a lawyer sends an electronic communication, what ethical duty does the lawyer have to
prevent the disclosure, through metadata embedded therein, of confidential or privileged information?

2. May a lawyer who receives an electronic communication examine it for the purpose of discovering the contents of the metadata that may be embedded within it?

RELEVANT ETHICAL RULES

ER 1.6  Confidentiality of Information
(a) 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 or required by paragraphs (b), (c) or (d), or ER 3.3(a)(3).

. . . .

ER 4.4  Respect for Rights of Others
. . . .
(b) A lawyer who receives a document and knows or reasonably should know that the document was inadvertently sent shall promptly notify the sender and preserve the status quo for a reasonable period of time in order to permit the sender to take protective measures.

ER 8.4  Misconduct
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;

. . . .

RELEVANT ETHICS OPINIONS

OPINION

Duties of the Sender

“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.” ER 1.6, cmt 20. 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. See also Ala. Op. RO-2007-02 (March 14, 2007); Fla. Op. 06-2 (September 15, 2006); N.Y. State Bar Op. 782 (December 8, 2004). In the case of a lawyer who is employed by a corporation or by a governmental or other entity, “special instructions given by the client” might include the client’s informed consent to forego, for financial or other reasons, the acquisition or use of software that is designed to
remove metadata from an electronic document. If a lawyer is asked to comment on a document prepared by another lawyer in the firm, and the commenting lawyer knows or reasonably should know that the document is ultimately intended for transmission to opposing counsel, he or she should consider whether the comment is the type that should be included within the draft. A lawyer who prepares a pleading, contract, or other document should use a “clean” form and not a document that was used for another client. The lawyer who sends an electronic document should 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.

When removing or restricting access to metadata in documents produced or disclosed in litigation, the lawyer must take care not to violate any duty of disclosure to which the lawyer or the lawyer’s client is subject. For a recent discussion relating to the duty to preserve and disclose metadata in a litigation context, see Wyeth v. Impax Laboratories, Inc., 2006 WL 3091331 (D. Del. October 26, 2006). See also the Arizona Supreme Court’s order dated September 5, 2007, on rule-change petition R-06-0034 (amending, effective January 1, 2008, the Arizona Rules of Civil Procedure to include provisions relating to discovery and disclosure of “electronically stored information”).

Duties of the Recipient

A fundamental principle of the client-lawyer relationship is that, in the absence of the client’s informed consent, the lawyer must not reveal information relating to the representation…. This contributes to the trust that is the hallmark of the client-lawyer relationship. The public is better protected if full and open communication by the client is encouraged than if it is inhibited. The client is thereby encouraged to seek legal assistance and to communicate fully and frankly with the lawyer even as to embarrassing or legally damaging subject matter. The lawyer needs this information to represent the client effectively and, if necessary, to advise the client to refrain from wrongful conduct. Almost without exception, clients come to lawyers in order to determine their rights and what is, in the complex of laws and regulations, deemed to be legal and correct. Based upon experience, lawyers know that almost all clients follow the advice given, and the law is upheld.

ER 1.6, cmt 2 (internal citations omitted).

Lawyers, in light of this fundamental principle, and in keeping with their status as members of a learned profession, should refrain from conduct that amounts to an unjustified intrusion into the client-lawyer relationship that exists between the opposing party and his or her counsel. ER 8.4(a)-(d). See also Ala. Op. RO-2007-02.

Florida, in Op. 06-2, concluded that “[a] lawyer receiving an electronic document should not try to obtain information from metadata that the lawyer knows or should know is not intended for the receiving lawyer.” The New York State Bar Association, in Op. 749 (December 14, 2001), determined that a lawyer may not “intentional[ly] use . . . computer technology to surreptitiously obtain privileged or other confidential information” of an opposing party. Alabama, in Op. RO-2007-02, has adopted the New York position.
The American Bar Association (ABA), in Formal Op. 06-442 (August 5, 2006), concluded that the Model Rules of Professional Conduct do not prohibit such conduct. We respectfully decline to follow the ABA position. Despite the most reasonable and thorough precautions, and even with the best of intentions, 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. Under the ABA position, the sending lawyer would be at the mercy of the recipient lawyer. Under such circumstances, the sending lawyer might conclude that the only ethically safe course of action is to forego the use of electronic document transmission entirely. We do not think that is realistic or necessary. Under the position adopted by Florida, New York, Alabama, and now Arizona, the sending lawyer is alerted to the potential problem and is reminded of the duty to take reasonable steps to prevent the inadvertent disclosure of confidential or privileged information. At the same time, except in the specific circumstances described below, the recipient lawyer has a corresponding duty not to “mine” the document for metadata that may be embedded therein or 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.[1]

We also note that there is a significant difference between the Model Rules of Professional Conduct as promulgated by the ABA and the Rules of Professional Conduct as adopted by the Arizona Supreme Court. Under Arizona’s version of ER 4.4(b), a “lawyer who receives a document and knows or reasonably should know that the document was inadvertently sent shall promptly notify the sender and preserve the status quo for a reasonable period of time in order to permit the sender to take protective measures.” While it might be argued that ER 4.4(b) is inapplicable because the document was not inadvertently sent, only the metadata embedded therein, we think that is an insubstantial distinction. If the document as sent contains metadata that reveals confidential or privileged information, it was not sent in the form in which it was intended to be sent, and the harm intended to be remedied by ER 4.4(b) is the same. Therefore, a lawyer who receives an electronic document from another party, and who discovers metadata embedded in the document that the lawyer knows or reasonably should know is revealing confidential or privileged information, has a duty to notify the sender and to preserve the status quo for a reasonable period of time in order to permit the sender to take protective measures. ER 4.4(b). We express 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 the result of such disclosure. Those are questions of substantive law. Whether the sending lawyer has transgressed ER 1.6 will depend on what was reasonable in the circumstances.

We recognize that some metadata embedded within an electronic document may be discovered by the recipient through inadvertent or relatively innocent means, such as right-clicking a mouse or by holding the cursor over certain text in the document. We do not mean to imply that all such activity necessarily rises to a level of ethical concern. If, however, the recipient discovers metadata by any means, and knows or reasonably should know that the sender did not intend to transmit the information, the recipient has a duty to follow the procedures set forth in ER 4.4(b).

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. Even so, if the lawyer comes across information that the lawyer knows or reasonably should know was not intended to be transmitted by the sender, the recipient has a duty to follow the procedures set forth in ER 4.4(b).

CONCLUSION

Lawyers who send communications or other documents electronically must be aware that such activity has inherent risks. Therefore, the lawyer must take reasonable measures to prevent the inadvertent disclosure of confidential client information. At the same time, and except in the specific circumstances set forth above, a lawyer who receives an electronic communication may not examine it for the purpose of discovering the metadata embedded in it. A recipient lawyer who discovers metadata embedded within an electronic communication and who knows or reasonably should know that the metadata reveals confidential or privileged information has a duty to comply with the procedures set forth in ER 4.4(b).

Formal opinions of the Committee on the Rules of Professional Conduct are advisory in nature only and are not binding in any disciplinary or other legal proceedings. © State Bar of Arizona 2007

Footnotes

[1] The District of Columbia, in Op. 341 (September 2007), held that “[a] receiving lawyer is prohibited from reviewing metadata sent by an adversary only where he has actual knowledge that the metadata was inadvertently sent.” (Emphasis added). While Op. 341 may reflect an effort to reach a middle ground between the position of the ABA, on the one hand, and the positions of Alabama, Florida, and New York on the other hand, we respectfully disagree with the District of Columbia. Subject to the specific exceptions described elsewhere in this opinion, a lawyer who receives an electronic communication should not be engaged in the intentional examination of the document’s metadata in the first place and, in our view, would bear the burden of establishing that any such intentional examination was for a proper purpose and not for the purpose of attempting to discover any confidential or privileged information that might be contained therein.

NOTES
Colorado Ethics Opinion 119

Disclosure, Review, and Use of Metadata.

November, 2007

Introduction

Lawyers routinely send and receive documents or computer files in electronic form, whether in email correspondence, in the course of civil discovery, or otherwise. An electronic document typically includes data that may or may not be visible when viewing the document on the computer screen or as printed out. These hidden data are called “metadata.” Metadata embedded in a document can include such information as the dates and times that the document was created, modified, and accessed, and the names of the persons who created the document and who last edited the document. Metadata can also include embedded user comments or the edit history of a document, including redlined changes showing additions and deletions of text. Metadata in spreadsheets include the formulas used to arrive at the numbers displayed in a table. This list of types of metadata is not complete. Moreover, common types of metadata are likely to change and multiply over time as computer software and technology change.

Much metadata is of little or no practical significance. For example, it may be of no importance when a document was created and edited or by whom. Other metadata, such as formulas in a spreadsheet, may be important but not confidential. Some metadata, however, particularly metadata such as hidden comments or redlines, can be Confidential Information. “Confidential Information” is used in this Opinion to include information that is subject to a legally recognized exemption from discovery and use in a civil, criminal, or administrative action or proceeding, even if it is not “privileged.” See Op. 108.

This opinion addresses the ethical obligations of a lawyer (the “Sending Lawyer”) who transmits electronic documents containing metadata to a third party, including the lawyer for an adverse party. This opinion also addresses the ethical obligations of a lawyer (the “Receiving Lawyer”) who receives electronic documents containing metadata from a third party, including the lawyer for an adverse party or a non-lawyer third party.

Syllabus

A Sending Lawyer who transmits electronic documents or files has a duty to use reasonable care to guard against the disclosure of metadata containing Confidential Information. What constitutes reasonable care will depend on the facts and circumstances. The duty to provide competent representation requires a Sending 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 if necessary. Within a law firm, a supervising lawyer has a duty to ensure that appropriate systems are in place so that the supervising lawyer, any subordinate lawyers, and any nonlawyer assistants are able to control the transmission of metadata.
A Receiving Lawyer who receives electronic documents or files generally may search for and review metadata. If a Receiving Lawyer knows or reasonably should know that the metadata contain or constitute Confidential Information, the Receiving Lawyer should assume that the Confidential Information was transmitted inadvertently, unless the Receiving Lawyer knows that confidentiality has been waived. The Receiving Lawyer must promptly notify the Sending Lawyer. Once the Receiving Lawyer has notified the Sending Lawyer, the lawyers may, as a matter of professionalism, discuss whether a waiver of privilege or confidentiality has occurred. In some instances, the lawyers may be able to agree on how to handle the matter. 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 of waiver.

If, before examining metadata in an electronic document or file, the Receiving Lawyer receives notice from the sender that Confidential Information was inadvertently included in metadata in that electronic document or file, the Receiving Lawyer must not examine the metadata and must abide by the sender’s instructions regarding the disposition of the metadata.

**Opinion**

Metadata are not really different from any other sort of information. In Formal Opinion 108, the Committee addressed a lawyer’s obligations with respect to receipt of inadvertently transmitted documents. In Formal Opinion 90, the Committee addressed a lawyer’s obligations to be aware of disclosure of Confidential Information using new technology. In most respects, this opinion is an application of those two previous opinions and the underlying Rules. The Committee believes that this separate opinion regarding metadata is appropriate because there is a split among other jurisdictions over the application of familiar rules to a type of data that is new and mysterious to some.

**1. The Sending Lawyer’s Obligations to Guard Against Disclosure of Metadata Containing Confidential Information.**

Under the Colorado Rules of Professional Conduct, a Sending Lawyer has an ethical duty to take steps to reduce the likelihood that metadata containing Confidential Information would be included in an electronic document transmitted to a third party. This duty arises out of several interrelated rules.

First, Rule 1.6(a) 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 [otherwise] permitted ….” Second, Rule 1.1 provides that “A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.” Third, Rules 5.1 and 5.3 generally require a lawyer to make reasonable efforts to ensure that the lawyer’s firm, including lawyers and non-lawyers, conform to the Rules.

Under these Rules, 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. See DC Ethics Op. 341 (2007); Maryland State Bar Ass’n Formal Ethics Op. 2007-09, “Ethics of Viewing and/or Using Metadata,” (“the sending attorney has an ethical obligation to take reasonable measures to avoid the disclosure of confidential or work product materials imbedded in the electronic discovery”); Arizona Ethics Op. 07-03, “Confidentiality; Electronic Communications; Inadvertent Disclosure” (same); Alabama Ethics Op. RO-2007-02, “Disclosure and Mining of Metadata” (same); Florida Ethics Op. 06-2 (same); New York State Bar Ass’n Comm. on Prof’l Ethics, Op. 782 (2004) (same); see also CBA Formal Ethics Op. 90, “Preservation of Client Confidences in View of Modern Communications Technology” (1992) (“A lawyer must exercise reasonable care when selecting and using communications devices in order to protect the client’s confidences or secrets from unintended disclosure.”).

What constitutes reasonable care will depend on the facts and circumstances. For example, a Sending Lawyer could avoid creating certain types of metadata by choosing not to use redlining or hidden comments in a document that may be transmitted to third parties. In addition, software is available to “scrub” files of some types of metadata. In a circumstance where it is vital that no metadata be transmitted, a Sending Lawyer could print out an electronic document to ensure absolutely that no unseen metadata of any kind are included. Other methods of controlling or preventing disclosure of metadata exist.

In many instances, it would be appropriate for a lawyer to retain persons with expertise in computer software and hardware, either through an in-house computer systems department in a larger firm, or through outside contract vendors for a smaller firm or solo practice. These computer experts can set up systems to control or prevent the transmission of metadata. 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. RPC 5.1; RPC 5.3.

The ultimate responsibility for control of metadata rests with the Sending Lawyer. A Sending Lawyer may not limit the duty to exercise reasonable care in preventing the transmission of metadata that contain Confidential Information by remaining ignorant of technology relating to metadata or failing to obtain competent computer support. The 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. See DC Ethics Op. 341 (2007) (“lawyers must either acquire sufficient understanding of the software that they use or ensure that their office employs safeguards to minimize the risk of inadvertent disclosures”); New York State Bar Ass’n Comm. on Prof’l Ethics, Op. 782 (2004) (same).

2. The Receiving Lawyer’s Obligations Upon Receiving Metadata

There are two distinct issues relating to a Receiving Lawyer’s obligations regarding metadata. The first issue is whether the Receiving Lawyer ethically may review metadata. The second issue is what a Receiving Lawyer must do when he or she receives metadata that appear to contain Confidential Information.
a. May a Receiving Lawyer Ethically Review Metadata?

The authorities are split on whether a Receiving Lawyer ethically may review metadata in electronic documents received from adversaries or other third parties. The American Bar Association Ethics Committee concluded that the Model Rules of Professional Conduct generally do not prohibit a lawyer from searching for or reviewing embedded metadata in electronic documents or files received from opposing counsel, an adverse party, or other third party. ABA Formal Op. 06-442, “Review and Use of Metadata.” The Maryland State Bar Association Ethics Committee followed the ABA on this point. Maryland State Bar Ass’n Formal Ethics Op. 2007-09, “Ethics of Viewing and/or Using Metadata.” The District of Columbia Bar Association concluded that a Receiving Lawyer generally may review metadata included in an electronic document unless the Receiving Lawyer has actual knowledge that metadata containing Confidential Information were transmitted inadvertently. DC Ethics Op. 341 (2007).

The New York State Bar Association Committee on Professional Ethics concluded that a lawyer may not search for or review metadata in electronic documents received from third parties. The New York Committee stated that “A lawyer may not make use of computer software to surreptitiously ‘get behind’ visible documents.” New York State Bar Ass’n Comm. on Prof’l Ethics, Op. 749 (2001). The New York opinion relied on a lawyer’s ethical obligation under the New York Code of Professional Responsibility to refrain from dishonest, fraudulent, or deceitful conduct. New York’s lead was followed by the bar association ethics committees of Arizona, Alabama, and Florida. Arizona Ethics Op. 07-03, “Confidentiality; Electronic Communications; Inadvertent Disclosure”; Alabama Ethics Op. RO-2007-02, “Disclosure and Mining of Metadata”; Florida Ethics Op. 06-2; see also D. Hricik, Mining for Embedded Data: Is It Ethical to Take Intentional Advantage of Other People’s Failures?, N. Car. J. of Law & Tech. 231 (Spring 2007) (reaching the same conclusion). The Alabama decision relied on Alabama’s version of Colorado Rule of Professional Conduct 8.4 which prohibits “conduct involving dishonesty, fraud, deceit, or misrepresentation.” These opinions -- as evidenced by their use of such language as “mining” -- appear to be based on an implied premise that searching for metadata is surreptitious or otherwise involves procedures that are difficult or complicated. They also seem to assume that metadata generally contain Confidential Information and that any metadata transmitted to a third party must, therefore, have been transmitted inadvertently.

The Committee concludes that the ABA, Maryland, and District of Columbia opinions are better reasoned, and that the New York, Arizona, Alabama, and Florida opinions are based on incorrect factual premises regarding the nature of metadata. Thus, the Committee concludes that a Receiving Lawyer generally may ethically search for and review metadata embedded in an electronic document that the Receiving Lawyer receives from opposing counsel or other third party. This conclusion is supported by the following.

First, there is nothing inherently deceitful or surreptitious about searching for metadata. Some metadata can be revealed by simply passing a computer cursor over a document on the screen or right-clicking on a computer mouse to open a drop-down menu that includes the option to review certain metadata. Typical word processing software can be configured so that files are routinely opened to show redlines or embedded comments. Referring to searching for metadata as
“mining” or “surreptitiously ‘get[ting] behind’” a document is, therefore, misleading.

Second, an absolute ethical bar on even reviewing metadata ignores the fact that, in many circumstances, metadata do not contain Confidential Information. To the contrary, in some circumstances metadata are intended to be searched for, reviewed, and used. For example, in discovery in a civil case, a party is entitled to discover pre-existing files in electronic form to enable review of metadata to trace the history of a document, its authors, edits, and comments. See, e.g., Fed. R. Civ. P. 34 (explicitly requiring production of electronically stored information). As another example, when opposing parties are negotiating a document, a Sending Lawyer may specifically intend a Receiving Lawyer to review some metadata, such as redlines or comments in a draft of the document. Similarly, when a Sending Lawyer transmits a spreadsheet, the Sending Lawyer may intend that the Receiving Lawyer be able to see the formulas used in the spreadsheet so that the Reviewing Lawyer may understand and rely upon the numbers in the rows and columns of the spreadsheet.

Third, metadata are often of no import. In many circumstances it is of no significance who created a document, when the document was created, or the like.

Once one discards the notions that it is dishonest or deceitful to search for or look at metadata or that metadata typically contain significant Confidential Information, there is no Rule in the Colorado Rules of Professional Conduct that contains any prohibition on a lawyer generally reviewing or using information received from opposing counsel or other third party. Therefore, a Receiving Lawyer generally may search for and review any metadata included in an electronic document or file.

b. The Receiving Lawyer’s Obligations On Discovering that He or She Has Received Metadata that Appear to Contain Confidential Information.

If a Receiving Lawyer knows or reasonably should know that a Sending Lawyer (or non-lawyer) has transmitted metadata that contain Confidential Information, the Receiving Lawyer should assume that the Confidential Information was transmitted inadvertently, unless the Receiving Lawyer knows that confidentiality has been waived. The Receiving Lawyer must promptly notify the Sending Lawyer (or non-lawyer sender). Once the Receiving Lawyer has notified the Sending Lawyer, the lawyers may, as a matter of professionalism, discuss whether a waiver of privilege or confidentiality has occurred. In some instances, the lawyers may be able to agree on how to handle the matter. 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 of waiver.

If, before examining metadata in an electronic document or file, the Receiving Lawyer receives notice from the sender that Confidential Information was inadvertently included in metadata in that electronic document or file, then the analysis changes. In this scenario, the Receiving Lawyer must not examine the metadata and must abide by the Sending Lawyer’s instructions regarding the disposition of the metadata.
We reach these conclusions as follows.

It is reasonable to expect that a Sending Lawyer will seek to act competently (under Rule 1.1) to protect the Confidential Information of the Sending Lawyer’s client (under Rule 1.6). Accordingly, it is reasonable to assume that the Sending Lawyer would not intentionally transmit to opposing counsel or another third party any Confidential Information included in metadata in an electronic document or file. Thus, a Receiving Lawyer reasonably should believe that any Confidential Information contained in metadata received from the Sending Lawyer was transmitted inadvertently.

Because the Receiving Lawyer reasonably should believe that Confidential Information in metadata was transmitted inadvertently, Rule 4.4(b) is directly applicable. Rule 4.4 provides:

**Rule 4.4. Respect for Rights of Third Persons**

(a) In representing a client, a lawyer shall not use means that have no substantial purpose other than to embarrass, delay, or burden a third person, or use methods of obtaining evidence that violate the legal rights of such a person.

(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.

(c) 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.

Under Rule 4.4(b), once a Receiving Lawyer knows or reasonably should know that an electronic document or file contains metadata that appear to contain Confidential Information, the Receiving Lawyer should assume that the Confidential Information was transmitted inadvertently and must promptly notify the Sending Lawyer. See also CBA Formal Ethics Op. 108, “Inadvertent Disclosure of Privileged or Confidential Documents” (2000).

Rule 4.4(b) does not state what the Receiving Lawyer should do after giving notice to the Sending Lawyer. May the Receiving Lawyer continue to review the electronic document or file that appears to include metadata containing Confidential Information?

The District of Columbia bar ethics committee concluded that a Receiving Lawyer must stop reviewing an electronic document or file when the Receiving Lawyer has actual knowledge that the Sending Lawyer did not intend to disclose Confidential Information in the metadata contained in an electronic document or file. DC Ethics Op. 341 (2007). The District of Columbia committee relied on its version of Rule 8.4(c), which provides that “It is professional misconduct for a lawyer to … engage in conduct involving dishonesty, fraud, deceit or misrepresentation.” The California Supreme Court likewise concluded that a Receiving Lawyer must stop reviewing materials when it is “reasonably apparent” that there was no intent to disclose Confidential Information. Rico v. Mitsubishi Motors Corp., 42 Cal. 4th 807 (Cal. 2007).
The Committee disagrees with these decisions. The Committee believes that Rule 4.4(b) and (c) are the more specific rules, and that these rules trump the more general requirements of Rule 8.4(c). Therefore, where the Receiving Lawyer has no prior notice from the sender, the Receiving Lawyer’s only duty upon viewing confidential metadata is to notify the Sending Lawyer. See RPC 4.4(b). There is no rule that prohibits the Receiving Lawyer from continuing to review the electronic document or file and its associated metadata in that circumstance. However, where the Receiving Lawyer has prior notice from the sender of the inadvertent transmission of confidential metadata, Rule 4.4(c) does prohibit the Receiving Lawyer from reviewing the electronic document or file.

As the Committee noted in Opinion 108, other considerations than the Receiving Lawyer’s obligations under the Rules may come into play, including professionalism and applicable substantive and procedural law. Once the Receiving Lawyer has notified the Sending Lawyer, the lawyers may, as a matter of professionalism, discuss whether waiver of privilege or confidentiality has occurred. In some instances, the lawyers may be able to agree on how to handle the matter. See RPC 4.4, comment [3]. 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 document or file, based on the substantive law of waiver. See CBA Formal Ethics Op. 108, “Inadvertent Disclosure of Privileged or Confidential Documents” (2000).

Footnotes

1. This Opinion is not intended to be a technical primer on metadata or methods to control metadata. Such a task would be beyond the expertise of the Committee, and any primer would inevitably become obsolete almost immediately.

2. The Pennsylvania Bar Association Committee on Legal Ethics declined to take a position. Instead, it summarized the rationales reached by others. It then concluded that there is no rule that would be applicable in all circumstances, and that the determination of how to address inadvertently disclosed metadata should be left to the individual Receiving Lawyer based on his or her analysis of the facts. Pennsylvania Bar Ass’n Comm. on Legal Ethics and Prof. Resp. Formal Op. 2007-500

3. The Committee rejects the notion that a lawyer is unethical if the lawyer configures word processing software in this manner. Indeed, it may be that a lawyer should configure word processing software in this manner so that the lawyer routinely sees redlining or embedded comments in the lawyer’s own documents, thus reducing the chance that the lawyer would inadvertently send such data to opposing counsel or a third party.

4. If the Receiving Lawyer receives notice before reviewing an electronic document that the electronic document contains Confidential Information in metadata, then Rule 4.4(c) applies. The Receiving Lawyer shall not review that electronic document and shall abide by the sender’s instructions as to its disposition.

5. The California Supreme Court upheld the disqualification of a lawyer who continued to review materials after the lawyer had concluded that the materials contained Confidential
6. This opinion does not address the legal issue of waiver. In some circumstances, a court may determine that the transmission of some Confidential Information waives any protections against disclosure of that Confidential Information or related Confidential Information. A Receiving Lawyer who believes that such a waiver may have occurred may ask a court to determine the issue. That is beyond the scope of this opinion.

NOTES
Maine Ethics Opinion 196

THE PROFESSIONAL ETHICS COMMISSION OF THE BOARD OF OVERSEERS OF THE BAR

APRIL 16, 2009

Question

Bar Counsel has asked for the Commission’s opinion concerning the application of the Bar Rules to 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 (“confidential information”). The issue gives rise to two questions: first, whether it is ethical for an attorney receiving electronic documents (the “receiving attorney”) to make efforts to uncover embedded metadata that contains confidential information not intended to be communicated by the attorney transmitting the document (the “sending attorney”); and second, whether the sending attorney has an ethical duty to take reasonable measures to remove metadata containing confidential information before document transmission. Applying the principles of Bar Rules 3.2(f)(3) and (4), \[3.6(h)(1)\] and (2), \[3.6(a)\], the Law Court’s reasoning in Corey v. Norman, Hanson & DeTroy, this Commission’s Opinions 172 (2000), 194 (2007) and 195 (2008), as well as opinions from other states following the lead of New York, we draw the following conclusions:

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.

Discussion

Lawyers today routinely make use of electronic document transmission, including in communications to opposing counsel. Such documents often contain metadata, which is peripheral information electronically embedded within the document but often not seen by and sometimes not even known to those who produce or read it. Much metadata is mundane and legally inconsequential, lodged within the document by the software and identifying the date and time that the document was produced and the version of the software utilized. Some of this data may be accessed with as little effort as resting the cursor upon, or right clicking, the document icon. However, purposeful efforts to ‘mine’ metadata in a document may allow a receiving attorney to glean information that was clearly never intended to be communicated by the sending attorney. The revelation of such metadata could result in the disclosure of client confidences, litigation and negotiation strategy, legal theories, attorney work product and other legally privileged and confidential information. Due to the rapid advance and general opaqueness of some computer technology, it may not be reasonably possible for an attorney to know all the
types of metadata that might be embedded in a document or the extent to which such data may be subject to being probed by someone using extraordinary but technologically available methods.

A number of other jurisdictions have considered these questions. While there are inconsistent approaches taken regarding the ethical duties of receiving attorneys in probing documents for metadata containing confidential information, there is greater harmony among the jurisdictions with respect to the duties of sending attorneys to take reasonable measures to minimize the prospect that such data will be inadvertently transmitted. In this Opinion, the Commission adopts a balanced view, articulating reasonable ethical duties on both the receiving and sending attorneys.

Duties of Receiving Attorneys in Probing Documents for Metadata Containing Confidential Information

In the first major bar ethics opinion on the subject, relying principally upon a lawyer’s ethical duty to refrain from dishonest, fraudulent, or deceitful conduct, New York determined that “Lawyers may not ethically use available technology to surreptitiously examine and trace email and other electronic documents.” NY Bar Ethics Op. 749 (2001). Citing a 1992 ABA opinion, New York concluded that “the strong policy in favor of confidentiality outweighs what might be seen as the competing principles of zealous representation…. “No such balance need be struck here because it is a deliberate act by the receiving lawyer, not carelessness on the part of the sending lawyer, that would lead to the disclosure of client confidences and secrets.”

Three years later, in an opinion discussed below focused on the duties of sending attorneys, New York renewed its ethical admonition to receiving attorneys: “Lawyer-recipients also have an obligation not to exploit an inadvertent or unauthorized transmission of client confidences or secrets.” NY Bar Ethics Op. 782 (2004).

Generally following New York’s lead, Florida concluded that “A lawyer receiving an electronic document should not try to obtain information from metadata that the lawyer knows or should know is not intended for the receiving lawyer. A lawyer who inadvertently receives information via metadata in an electronic document should notify the sender of the information’s receipt.” “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.” FL Bar Ethics Op. 06-02 (2006).

Emphasizing “the strong public policy in favor of preserving confidentiality as the foundation of the lawyer-client relationship,” Alabama followed the New York analysis in finding that “the receiving lawyer also has an ethical obligation to refrain from mining an electronic document.” “The disclosure of metadata contained in an electronic submission to an opposing party could lead to the disclosure of client confidences and secrets, litigation strategy, editorial comments, legal issues raised by the client, and other confidential information.” AL Bar Ethics Op. 2007-02 (2007).

In contrast to the New York rule, some jurisdictions have adopted a view that more or less liberates receiving attorneys from ethical considerations in probing metadata in electronic documents, thereby placing upon the sending attorney the entire burden of cleansing the
document of any possible, embedded client confidences or other privileged information. This view is based upon the fact that no bar rule specifically addresses the issue, together with the difficulty in prescribing permissible conduct in the context of rapidly changing technology.

Thus, recognizing that “metadata is ubiquitous in electronic documents” and that its model rules “do not contain any specific prohibition against a lawyer’s reviewing and using embedded information in electronic documents,” the ABA opinion placed the sole ethical obligation on the sending attorney: “A lawyer who is concerned about the possibility of sending, producing, or providing to opposing counsel a document that contains or might contain metadata, or who wishes to take some action to reduce or remove the potentially harmful consequences of its dissemination, may be able to limit the likelihood of its transmission by ‘scrubbing’ metadata from documents or by sending a different version of the document without the embedded information.” ABA Ethics Op. 06-442 (2006).

Following the ABA view, Maryland concluded that “there is no ethical violation if the recipient attorney… reviews or makes use of metadata without first ascertaining whether the sender intended to [send it].” MD Bar Ethics Op. 2007-09 (2007). Likewise, Colorado rejected New York’s and adopted a variation of the ABA’s view, emphasizing the responsibilities of the sending lawyer “to guard against the disclosure of metadata containing Confidential Information” and “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 steps that can be taken to remove metadata if necessary.” Generally absolving the receiving attorney of ethical responsibilities in probing metadata embedded in the document (“[T]here is nothing inherently deceitful or surreptitious about searching for metadata”), Colorado reasoned that the lawyer “who receives electronic documents or files generally may search for and review metadata.” However, Colorado went on to create a complex and perhaps impractical set of requirements for the parties to such communications: “If a Receiving Lawyer knows or reasonably should know that the metadata contain … Confidential Information, the Receiving Lawyer should assume that the Confidential Information was transmitted inadvertently unless the Receiving Lawyer knows that confidentiality has been waived. The Receiving Lawyer must promptly notify the Sending Lawyer,” in which case “the lawyers may, as a matter of professionalism, discuss whether a waiver of privilege or confidentiality has occurred.” If, however, before examining the metadata, “the Receiving Lawyer receives notice from the sender that Confidential Information was inadvertently included, the Receiving Lawyer must not examine the metadata and must abide by the sender’s instructions regarding the disposition of the metadata.” CO Bar Ethics Op. 119 (2008).

Two other jurisdictions have adopted variations on the New York and ABA views. Acknowledging that there is no specific rule determining the ethical obligations of attorneys in this particular context, Pennsylvania arrived at what seems a default. “[E]ach attorney must… ‘resolve [the issue] through the exercise of sensitive and moral judgment guided by the basic principles of the Rules’ and determine for himself or herself whether to utilize the metadata contained in documents and other electronic files based upon the lawyer’s judgment and the particular factual situation.” “The utilization of metadata by attorneys receiving electronic documents from an adverse party is an emerging problem. Although 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, those tools still may not remove all metadata.” PA Bar Ethics Op. 2007-
500 (2007). The District of Columbia has articulated yet another approach: “A receiving lawyer is prohibited from reviewing metadata sent by an adversary only where he has actual knowledge that the metadata was inadvertently sent.” (emphasis added). “[W]e believe that 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 the metadata…. Where there is such actual prior knowledge…, the receiving lawyer’s ethical 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.” DC Bar Ethics Op. 341 (2007).

Having considered all of the approaches extant, this Commission believes that the better view is that generally expressed by New York and the jurisdictions that have followed it. While the Commission recognizes, as is the case in those jurisdictions, that no Bar Rule specifically addresses this particular situation, and the Commission is appropriately cautious in its specific application of the general proscription in Bar Rule 3.2(f)(3) and (4) on attorneys engaging in conduct involving dishonesty or prejudicial to the administration of justice, an attorney who purposefully seeks to unearth confidential information embedded in metadata attached to a document provided by counsel for another party, when the attorney knows or should know that the information involved was not intended to be disclosed, has acted outside of these broad ethical requirements. While the Commission has considered the contrary view held by the ABA and the states that have followed it, the Commission believes that Bar Rule 3.2(f)(3) and (4) would have little (and we believe quite inadequate) meaning if it were not applied in this situation. Not only is the attorney’s conduct dishonest in purposefully seeking by this method to uncover confidential information of another party, that conduct strikes at the foundational principles that protect attorney-client confidences, and in doing so it clearly prejudices the administration of justice.

The Law Court’s decision in Corey, while not directly addressing the Bar Rules, and the Commission’s adoption of Corey in Opinion 172 (reversing Opinion 146), offer additional support for this conclusion. There, the issue was whether an attorney might retain and make use of confidential information that had been inadvertently disclosed to him by opposing counsel, the Law Court determining that he could not, based upon the shared responsibility to protect the attorney-client privilege. In Opinion 172, this Commission determined that it would be a violation of the Bar Rules, in direct contravention of the holding in Corey and therefore prejudicial to the administration of justice, for an attorney to retain and make use of such information. If anything, the issue before us now is more straightforward. Unlike in Corey, here the receiving attorney is making purposeful efforts to probe for information he or she knows or should know to be confidential and not to have been knowingly communicated by opposing counsel. That such conduct is dishonest and designed to prejudice the administration of justice seems beyond dispute.

In sum, following the general analysis of New York and the other states that have adopted its view, and based upon Bar Rule 3.2(f)(3) and (4) and Corey, we find that an attorney may not ethically take steps to uncover metadata, embedded in an electronic document sent by counsel for another party, in an effort to detect information that is legally confidential and is or should be reasonably known not to have been intentionally communicated.

Ethical Duties of Sending Attorneys in Taking Measures to Avoid Transmission of Metadata Containing Confidential Information
While the jurisdictions opining to date have arrived at inconsistent views in dealing with the ethical duties of document-receiving attorneys, there has been relative unanimity in dealing with those of sending attorneys. Therefore, we have no difficulty in following the consensus approach on the subject.

New York determined that sending attorneys have a duty to take reasonable measures to guard against improper disclosure of confidential information contained in metadata in documents transmitted to other parties. This conclusion was based on the rule “that a lawyer shall not ‘knowingly’ reveal a confidence or secret of a client.” “When a lawyer sends a document by email, as with any other type of communication, a lawyer must exercise reasonable care to ensure that he or she does not inadvertently disclose his or her client’s confidential information.” NY Bar Ethics Op. 782 (2004).

Following New York’s lead, Florida concluded that “A lawyer who is sending an electronic document should take care to ensure the confidentiality of all information contained in the document, including metadata.” “It is the sending lawyer’s obligation to take reasonable steps to safeguard the confidentiality of all communications sent by electronic means… and to protect from other lawyers and third parties all confidential information, including information contained in metadata.” “The foregoing 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.” FL Bar Ethics Op. 06-02 (2006).

Alabama, Maryland, Colorado and Pennsylvania have all followed suit. AL Bar Ethics Op. 2007-02 (2007); MD Bar Ethics Op. 2007-09 (2007); CO Bar Ethics Op. 119 (2008); PA Bar Ethics Op. 2007-500 (2007). However, those jurisdictions following the ABA analysis (described above), in finding few or no ethical duties of the receiving attorney to refrain from probing document metadata, have placed a correspondingly heavier burden on the sending attorney to take measures to avoid the transmission of metadata containing confidential information. “The ultimate responsibility for control of metadata rests with the Sending Lawyer,” who “may not limit the duty to exercise reasonable care in preventing the transmission of metadata that contain Confidential Information by remaining ignorant of technology relating to metadata or failing to obtain competent computer support.” CO Bar Ethics Op. 119 (2008). Going further, the Colorado opinion suggests that attorneys should access resources exceeding those normally expected of lawyers by retaining computer experts who understand the reach of metadata and methods to avoid transmission of confidential information embedded therein.

While we stop short of embracing the full force of Colorado’s advice, we agree with the other jurisdictions that attorneys are ethically required to take reasonable measures to avoid the communication of confidential information, regardless of the mode of transmission. This duty logically extends to metadata that the attorney should reasonably know may lie within an electronic document. If an attorney is in doubt, many documents can be readily converted to generic files (such as PDF) which retain little of the metadata contained in word processing documents, and of course resort can be made to paper copies where issues of metadata confidentiality are significant. Although we do not believe that an attorney’s ethical duties dictate, in routine work, the retention of a computer expert for these purposes, we also do not believe it reasonable for an attorney today to 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.
This Opinion is consistent with others the Commission has recently issued dealing with confidentiality of information in the computer era. In Opinion 195 (2008), the Commission concluded that, as a general matter and subject to appropriate safeguards, an attorney may utilize unencrypted e-mail without violating the attorney's ethical obligation to maintain client confidentiality. The issue invoked the prohibition on knowing disclosure of confidential client information under Bar Rule 3.6(h)(1) as well as the general standard requiring lawyers to "employ reasonable care and skill and apply the lawyer's best judgment in the performance of professional services" under Bar Rule 3.6(a). While we found that it is reasonable for attorneys transacting routine business through unencrypted email, some circumstances might require a more secure method of communication.

Likewise, in Opinion 194 (2007), the Commission concluded that, with appropriate safeguards, an attorney may utilize transcription and computer server backup services remote from both the lawyer's physical office and the lawyer's direct control or supervision, without violating the attorney's ethical obligation to maintain client confidentiality. The Opinion cautioned, however, that the lawyer utilizing such services has a duty to take practical measures to assure that the services are reasonably secure and appropriate for the intended purpose. As here, the issue is not amenable to an unqualified answer but requires the application of a standard of reasonableness, weighing all the factors of which the lawyer should be aware.

On the issue before us, we conclude that, in applying Bar Rules 3.6(h)(1) and (2) in combination with 3.6(a), the sending attorney has an ethical duty to use reasonable care when transmitting an electronic document to prevent the disclosure of metadata containing confidential information. Undertaking this duty requires the attorney to reasonably apply 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.

1Rule 3.2(f) sets forth an attorney’s ethical obligations in broad terms: “A lawyer shall not:… (3) engage in conduct involving dishonesty, fraud, deceit, or misrepresentation; (4) engage in conduct that is prejudicial to the administration of justice.”

2Rule 3.6(h)(1) sets forth an attorney’s ethical obligations to maintain client confidentiality:

Except as permitted by these rules, or when authorized in order to carry out the representation, or as required by law or by order of the court, a lawyer shall not, without informed consent, knowingly, disclose or use information (except information generally known) that:

i. Is protected by the attorney-client privilege in any jurisdiction relevant to the representation;

ii. Is information gained in the course of representation of a client or former client for which that client or former client has requested confidential treatment;

iii. Is information gained in the course of representation of the client or former client and the disclosure of which would be detrimental to a material interest of the client or former client; or
iv. Is information received from a prospective client, the disclosure of which would be detrimental to a material interest of that prospective client, when the information is provided under circumstances in which the prospective client has a reasonable expectation that the information will not be disclosed.

Rule 3.6(h)(2) addresses an attorney’s ethical obligation to ensure that others working on the attorney’s behalf in the course of representation who are privy to confidential client information likewise maintain the client's confidences: "A lawyer shall exercise reasonable care to prevent lawyers and non-lawyers employed or retained by or associated with the lawyer from improperly disclosing or using information protected by paragraph (1) of this subdivision."

3 Rule 3.6(a) sets forth a general standard requiring lawyers to "employ reasonable care and skill and apply the lawyer's best judgment in the performance of professional services.”

4 199 ME 196

5 This Opinion is not intended to deal with the extent to which relevant information may be sought in litigation through proper discovery under the guidance of a court.

6 Although the type of metadata embedded in an electronic document varies with the software being used, and its full scope is unknown except to those with advanced computer expertise, examples include recording of the document’s source, authors, editors and those offering comments, as well as changes and comments made in the course of document preparation. Some metadata may reveal client confidences and attorney work product and advice, among other confidential information.

7 While metadata may be “ubiquitous” (to use the words of the ABA), we think that, with rapid technological advances, it may be overly simple to assume that an attorney may reasonably be able to know its full extent in all the software applications used, or that easily applied steps will cleanse the document of all embedded information not intended to be revealed. While reasonable steps can and should be taken to minimize the amount of metadata contained in an electronic document to be transmitted to another party, and of course the document can be transmitted in paper copy if security is paramount, there is no absolute assurance that electronic transmission of documents can be undertaken in a manner that is totally immune from unwanted probing for confidential information.

8 “In Corey, the Law Court, jurisdictionally unconstrained, has now pronounced that, as a matter of common law, the obligation to preserve the lawyer-client privilege is indeed an affirmative obligation shared by adversaries, and that the privilege cannot be inadvertently relinquished.” Opinion 172.

9 See footnote 5.

10 As stated in Opinion 194, “[T]he primary responsibility for file integrity, maintenance, disposition, and confidentiality rests with the attorney employed by the client. See Maine Professional Ethics Commission Opinion # 74 (10/1/86)…. Rule 3.6(h)(2) implies that lawyers have a responsibility to train, monitor, and discipline their non-lawyer staff in such a manner as to guard effectively against breaches of confidentiality. Failure to take reasonable steps to provide adequate training, to monitor performance, and to apply discipline for the purpose of
enforcing adherence to ethical standards is grounds for concluding that the lawyer has violated Rule 3.6(h)(2). See Maine Professional Ethics Commission Opinion #134 (9/21/93).”

“With the pervasive and changing use of evolving technology in communication and other aspects of legal practice, particular safeguards which might constitute reasonable efforts in a specific context today may be outdated in a different context tomorrow. Therefore, rather than attempting to delineate acceptable and unacceptable practices, this opinion will outline guidance for the lawyer to consider in determining when professional obligations are satisfied.” Opinion 194.

NOTES
NEW HAMPSHIRE BAR ASSOCIATION
Ethics Committee Opinion 2008-2009/4
April 16, 2009

Disclosure, Review and Use of Metadata in Electronic Materials

Rule References:
Rule 1.1
Rule 1.6(a)
Rule 4.4(b)
Rule 5.1
Rule 5.3

Subjects:
* Attorney-Client Relationship
* Client Communications
* Confidentiality
* Inadvertent Disclosure
* Conduct Towards Opponent

Annotation

Electronic materials sent and received by lawyers in modern law practices contain hidden information called “metadata,” which may contain confidential information relating to representation of a client. Both sending and receiving lawyers share ethical obligations to prevent disclosure of such confidential information.

Lawyers sending electronic materials to opposing counsel are ethically required to take reasonable care to avoid improper disclosure of confidential information contained in metadata, which might include appropriate training and education on reasonable measures that can be taken to reduce the likelihood of improper disclosure of confidential information through transmission of metadata. There can be no per se rule on what constitutes reasonable care in transmission of metadata, as the facts and circumstances of each case will dictate the reasonableness of protective measures taken by sending lawyers.

Receiving lawyers 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. Receiving lawyers necessarily know that any confidential information contained in the electronic material is inadvertently sent, triggering the obligation under Rule 4.4(b) not to examine the material. To the extent that metadata is mistakenly reviewed, receiving lawyers should abide by the directives in Rule 4.4(b).

This opinion does not address issues relating to the discovery of electronic materials in adjudicative proceedings, which are handled under applicable rules of court and law.

Introduction

In modern legal practice, lawyers routinely send and receive e-mails and other materials in electronic form from opposing counsel and other parties. Electronic documents are sent and received during the course of negotiations, due diligence reviews, litigation, investigations and other dealings. E-mails and other electronic documents
inevitably contain “embedded” information commonly referred to as “metadata.” Metadata is “information about information” not ordinarily visible on the computer screen that describes the history, tracking or management of an electronic document.

Some metadata is automatically lodged within the document by software, such as the date and time the document was produced, and can be accessed simply by right-clicking on it with a computer mouse. Other types of metadata are produced by word processing programs that allow users to “redline” changes to a document or to embed comments, which may or may not pop up as the cursor is moved over them. If metadata is “mined” by use of readily available computer programs, it can show, among other things, the changes made to a document during its drafting, as well as comments made by various reviewers of the document. Metadata may, therefore, reveal client confidences, litigation and negotiation strategy, legal theories, attorney work product and other legally privileged and confidential information that was never intended to be communicated by the sender. This raises ethical issues for both the sending and receiving lawyers.

The Ethics Committee believes it appropriate to provide guidance to New Hampshire lawyers on ethical obligations regarding transmission, receipt and use of metadata under the New Hampshire’s Rules of Professional Conduct. This opinion addresses both the ethical obligations of the sending lawyer to prevent the disclosure of metadata containing confidential information when transmitting electronic materials and the ethical obligations of the recipient lawyer with respect to searching for, reviewing and using metadata found in electronic materials. The Committee’s view is that both sending and receiving lawyers share ethical obligations to preserve confidential information relating to representation of clients and that it is impermissible for New Hampshire lawyers to seek to review or use metadata received from opposing counsel.

In assessing the ethical obligations of both the sending and receiving attorneys with respect to metadata, the Committee does not address issues relating to the discovery of electronic materials in adjudicative proceedings, which are handled under applicable rules of court and law. Discovery of electronic materials raises separate issues and rules that go beyond the scope of this opinion.

Discussion

Ethical Obligations of Lawyers Sending Electronic Materials

Exchange of electronic documents is an essential part of modern law practice. At the same time that advances in technology permit users to access metadata that may relate to another lawyer’s representation of a client, the ethical obligation imposed upon lawyers to avoid such disclosures remains unchanged. Protection of client confidences is one of the most significant obligations imposed upon lawyers and forms the core of the attorney-client relationship. Rule 1.6(a) 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).” As stated in this Committee’s comment to Rule 1.6, “[t]he disclosure of client confidences is an extreme and irrevocable act.” The
confidentiality rule applies not only to matters communicated in confidence by the client, but also to all information related to the representation, whatever its source. See 2004 ABA Model Rule Comment [3].

There is general consensus among jurisdictions reviewing the ethical obligations of lawyers who send electronic materials to opposing counsel that they are ethically required to take reasonable care to avoid improper disclosure of confidential information contained in metadata. See, e.g., ABA Formal Op. 06-442 (2006); FL Bar Ethics Op. 06-02 (2006) (a lawyer who is sending an electronic document should take care to ensure the confidentiality of all information contained in the document, including metadata); NY Bar Ethics Op. 782 (2004) (a lawyer must exercise reasonable care to ensure that he or she does not inadvertently disclose his or her client’s confidential information”). The Ethics Committee agrees that a sending lawyer who transmits electronic documents or files has a duty to use reasonable care to guard against disclosure of metadata that might contain confidential information. However, the Committee also believes that what constitutes reasonable care will depend upon the facts and circumstances, including the subject matter of the document, whether there have been multiple drafts of the document with multiple commenting parties, whether the client has commented on the document and other relevant factors. Thus, there can be no per se rule on transmission of metadata.

Lawyers should consider the duty to provide competent representation under Rule 1.1, as well as the general requirement under Rules 5.1 and 5.3 that lawyers make reasonable efforts to ensure that their firms, including lawyers and non-lawyers, conform to the Rules. In general, 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, if necessary. Lawyers should stay abreast of technological advances and potential risks of transmission through appropriate training and education. In the Committee’s view, lawyers should acquire, at the very least, a basic understanding of the existence of metadata embedded in electronic documents, the features of the software they have used to generate the document and any practical measures that may be taken to limit the likelihood of transmitting metadata or to purge the documents of sensitive information. This view is generally shared by other jurisdictions that have reviewed this subject. See, e.g., MI Bar Ethics Op. 196 (2008).

The Committee recognizes that, as 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. See,
e.g., ABA Formal Op. 06-442 (2006). Simply substituting a scanned version of sensitive documents may be adequate in most circumstances.

Ethical Obligations of Lawyers Receiving Electronic Materials

In reviewing the ethical obligations of a lawyer who receives metadata from opposing counsel, the Committee considered the variety of circumstances under which metadata might be received and reviewed. For example, in the context of negotiating a contract, a sending lawyer might intend the receiving lawyer to search and review redlined comments in a draft document or to review underlying formulas used to create a spreadsheet. Conversely, a sending lawyer may send a draft contract that includes a client’s comment on “bottom line price” that the lawyer either was unaware existed in metadata contained within a document or that the lawyer had unsuccessfully attempted to eliminate. In the latter set of circumstances, the sending lawyer may have exercised reasonable care in avoiding disclosure of client confidences through transmission of metadata but was either unsuccessful or unaware of the receiving lawyer’s purposeful efforts to uncover confidential information that may provide an advantage during negotiations. There is also the possibility that receiving lawyer may use sophisticated software to reveal or recover information not revealed by most programs.

New Hampshire’s Rule 4.4(b), Respect for Rights of Third Persons, was amended in 2008 to provide guidance to lawyers who receive confidential information from opposing counsel or third persons, as follows:

* * *

(b) 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.

* * *

New Hampshire’s Rule 4.4 varies from the American Bar Association’s (ABA’s) Model Rule in several respects: by substituting “materials” for “document” to make clear that electronic information is covered; by replacing “reasonably should know” with “knows” to create an objective standard; and by adding a new second sentence to specify the obligations of the receiving attorney with regard to inadvertently sent materials. See 2008 New Hampshire Comment to Rule 4.4. These differences are significant in light of the ABA’s conclusion, shared by a number of jurisdictions, that there is no express ethical prohibition against a receiving lawyer reviewing or using opposing counsel’s metadata. See ABA Formal Op. 06-442 ("unless other law requires otherwise, a lawyer who receives an inadvertently sent document ordinarily may, but is not required to, return it unread, as a matter of professional judgment"). The ABA and several other jurisdictions have tended to avoid the issue of whether disclosure of confidential information is presumably inadvertent, preferring instead to apply a literal reading of the rule prohibitions. The Committee rejects this approach, for the reasons set forth below.
While most jurisdictions agree that sending attorneys must take reasonable precautions to prevent inadvertent disclosure of confidential information in the form of metadata, there is a split on whether it is permissible for attorneys to review or use metadata received from their opponents. For example, in concluding that the Model Rules of Professional Conduct generally do not prohibit review or use of metadata, the ABA concluded that “the Rules do not contain any specific prohibition against a lawyer’s reviewing and using the embedded information in electronic documents.” ABA Formal Op. 06-442 (2006). Maryland has followed the ABA on this point, concluding that “there is no ethical violation if the recipient attorney reviews or makes use of the metadata without first ascertaining whether the sender intended to [send it].” MD Bar Ethics Op. 2007-09 (2007).

The District of Columbia has articulated a view that the receiving lawyer is prohibited from reviewing metadata sent by an adversary only where there is actual knowledge of inadvertence: “[W]e believe that 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 the metadata ….” DC Bar Ethics Op. 341 (2007). Colorado adopted a variation of the ABA view, concluding that receiving lawyers may ethically search for and review metadata, but adding that the receiving lawyer should know that any confidential information transmitted with the metadata was transmitted inadvertently unless confidentiality was waived. CO Bar Ethics Op. 119 (2008). Pennsylvania has not adopted a conclusive view, deciding instead that each attorney must exercise moral judgment under the principles of the Rules under particular factual situations. PA Bar Ethics Op. 2007-500 (2007).

The Committee believes 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” as that term is used in Rule 4.4(b). In addition, because no lawyer would intentionally send confidential information in violation of Rule 1.6, the receiving lawyer necessarily “knows” that the information has been inadvertently sent. The objective standard dictates a conclusion that receipt of confidential information in the form of metadata is the result of inadvertence, just as receipt of attorney notes stapled to draft documents would necessarily be the result of inadvertence. As a result, Rule 4.4(b) imposes an obligation on the receiving lawyer to refrain from reviewing the metadata.

The Committee does not ascribe to the view that the lack of an express prohibition in the Rules defines the extent of a receiving lawyer’s obligations. The Committee believes that purposefully seeking to unearth confidential information embedded in metadata attached to a document provided by opposing counsel implicates the broad principles underlying the Rules, including the strong public policy in favor of maintaining client confidentiality. In the Committee’s view, there is a shared responsibility on both sides to protect the attorney-client privilege through imposition of a receiving lawyer’s obligation to refrain from reviewing confidential information that can be nothing other than “inadvertently sent.” See Rule 4.4(b) (2008).
Because metadata is simply another form of information that can include client confidences, the Committee sees little difference between a receiving lawyer uncovering an opponent’s metadata and that same lawyer peeking at opposing counsel’s notes during a deposition or purposely eavesdropping on a conversation between counsel and client. There is a general expectation of honesty, integrity, mutual courtesy and professionalism in the New Hampshire bar. Lawyers should be able to reasonably assume that confidential information will not be sought out by their opponents and used against their clients, regardless of the ease in uncovering the information.

The Committee also rejects the ABA’s notion that sending lawyers can avoid harm to their clients by negotiating confidentiality agreements in advance if there is any concern about misuse of metadata. See ABA Formal Op. 06-442 (2006). While such agreements may be effective tools in the context of litigation and discovery and are expressly sanctioned under court rules, they are not as effective in transactional settings. There is often no way to effectively retract confidential information, once learned, especially if it involves the subject matter of negotiations. Therefore, 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. To the extent that metadata is unintentionally reviewed, receiving lawyers should abide by the directives set forth in Rule 4.4(b).

The Committee’s interpretation of the New Hampshire Rules is consistent with those jurisdictions that have rejected the ABA conclusion that metadata can be ethically accessed. These jurisdictions include New York, Florida, Alabama and Maine. In 2001, the New York State Bar Association Committee on Professional Ethics concluded that a lawyer may not search for or review metadata in electronic documents, relying principally on a lawyer’s ethical obligation to refrain from dishonest, fraudulent or deceitful conduct, as well as conduct prejudicial to the administration of justice. NY Bar Ethics Op. 749 (2001). New York also concluded that “the use of computer technology in the manner described above constitutes an impermissible intrusion on the attorney-client relationship in violation of the Code.” Id. Interestingly, New York viewed mining of metadata to be a “deliberate act by the receiving lawyer, not carelessness on the part of the sending lawyer, which would lead to the disclosure of client confidences and secrets.” Id.

Since New York’s opinion was issued, Florida, Alabama and Maine have followed the same or similar reasoning in concluding that receiving lawyers cannot review or use metadata. See FL Ethics Op. 06-2 (2006) (It is the recipient lawyer’s concomitant obligation . . . 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”, AL Bar Ethics Op. 2007-02 (2007) (“the receiving lawyer also has an ethical obligation to refrain from mining an electronic document”), ME Bar Ethics Op. 196 (2008) (“an attorney may not ethically take steps to uncover metadata embedded in an electronic document sent by counsel for another party, in an effort to detect information that is legally confidential and is or should be reasonably known not to have been intentionally communicated”).

7
Conclusion

New Hampshire lawyers who either send or receive electronic materials share an ethical obligation to preserve confidential information relating to representation of clients. Sending lawyers must take reasonable care to avoid improper disclosure of confidential information that may be hidden within metadata accompanying electronic materials sent to opposing counsel. It is impermissible for receiving lawyers to search for, review or use confidential information in the form of metadata that is associated with transmission of electronic materials from opposing counsel. This does not preclude opposing counsel from reaching mutual agreement on review of metadata.
L.E.O. 2009-01
WHAT IS METADATA AND WHY SHOULD LAWYERS BE CAUTIOUS?

Introduction

The Lawyer Disciplinary Board sees the need to raise awareness of metadata in electronic documents and emphasizes the need for attorneys to protect this kind of information.

All computer files have metadata (literally, the “data behind the data”) associated or within them that provide information about the files. Whenever a document is created, opened, or saved in a program on a computer, the document stores information, such as the author’s identity, the number of revisions made and comments and redlining. This metadata adds functionality to the editing, viewing, filing and retrieving capabilities of computer programs. In essence, metadata reveals information about electronic documents beyond the printable text and is used for a variety of legitimate purposes.

If legal professionals provide electronic versions of documents to other parties, metadata that is embedded in the document may be provided inadvertently. The information that is embedded is often of little or no interest, but in some instances it may reveal significant information. When this information is passed on to inappropriate parties, it can create adverse consequences for a legal professional or a client. In order to avoid these consequences, it is important to be familiar with the types of metadata contained in computer documents and to take steps to protect or remove it whenever necessary. Failure to do so
could be viewed as a violation of the Rules of Professional Conduct. Additionally, searching for or viewing metadata in documents received from others after an attorney has taken steps to protect such could also be viewed as a violation of the Rules of Professional Conduct.

**Discussion**

The ABA has noted that the Rules of Professional Conduct do not contain any specific prohibition against a lawyer’s reviewing and using embedded information in electronic documents, whether received from opposing counsel, an adverse party, or an agent of an adverse party. See ABA Formal Op. 06-442. However, metadata use may implicate other Rules of Professional Conduct.

Lawyers sending electronic documents have an obligation under Rule 1.1, which provides that a lawyer shall provide competent representation to a client, together with Rule 1.6, which obligates a lawyer not to reveal confidential information relating to the representation of a client, to take reasonable steps to maintain the confidentiality of documents in their possession. This includes taking care to avoid providing electronic documents that inadvertently contain accessible information that is either confidential or privileged, and to employ reasonable means to remove such metadata before sending the document. Accordingly, lawyers must either acquire sufficient understanding of the software that they use or ensure that their office employs safeguards to minimize the risk of inadvertent disclosures. See N.Y. State Bar Ass’n Committee Op. 782; D.C. Bar Op. 341.
It is the duty of the lawyer sending electronic documents to protect sensitive metadata, and protecting metadata is not difficult. Sending documents in hard copy, creating an image of the document and sending only the image (scanning and creating a .pdf file, for example), or printing and faxing a document will prevent the transmission of embedded information. Software programs that remove metadata are also available. Lawyers must always exercise reasonable care not to disclose confidential information and ensure that the lawyer’s firm and staff have the appropriate technology and systems in place to control the transmission of metadata.

Where a lawyer knows that privileged information was inadvertently sent, it could be a violation of Rule 8.4(c) for the receiving lawyer to review and use it without consulting with the sender. Therefore, if a lawyer has received electronic documents and has actual knowledge that metadata was inadvertently sent, the receiving lawyer should not review the metadata before consulting with the sending lawyer to determine whether the metadata includes work-product or confidences. See N.Y. State Bar Ass’n Committee Op. 749 (concluding that lawyers have an obligation under Rule 8.4(c) not to exploit an inadvertent or unauthorized transmission of client confidences).

In a discovery or subpoena context, however, a lawyer must be careful in situations where electronic documents constitute tangible evidence. Rule 3.4(a) prohibits altering, destroying or concealing material having potential evidentiary value. Therefore, in certain instances involving discovery responses or subpoena compliance, removal of metadata may
be prohibited and must be produced when requested and not objected to. However, any metadata that is privileged can still be protected and exempt from discovery, upon proper assertion of a privilege.

In many situations, it may not be clear whether the disclosure was inadvertent. In order to avoid misunderstandings, it is always safer to notify the sender before searching electronic documents for metadata. If attorneys cannot agree on how to handle the matter, either lawyer may seek a ruling from a court or other tribunal on the issue.

**Conclusion**

The Board finds that there is a burden on an attorney to take reasonable steps to protect metadata in transmitted documents, and there is a burden on a lawyer receiving inadvertently provided metadata to consult with the sender and abide by the sender’s instructions before reviewing such metadata.

**APPROVED** by the Lawyer Disciplinary Board on the 5th day of June, 2009, and **ENTERED** this 11th day of June, 2009.

![Signature]

David A. Jividen, Chairperson
Lawyer Disciplinary Board
Vermont Ethics Opinion 2009-1
September, 2009

ETHICS OPINION 2009-1

"Metadata" refers to electronically stored information about electronic documents. Metadata often is included in files that are stored electronically. It may be apparent on the face of an electronic document, or may be hidden. Some metadata may be innocuous and unimportant, revealing basic information about dates an electronic file was created and edited. On the other hand, however, sensitive and confidential information, including comments reflecting attorney-client communications and tracked changes revealing work product, may also be contained in metadata embedded in electronic documents. When documents are transmitted and received electronically, tools may be available that enable the recipient to search for hidden metadata.

In this opinion, the Vermont Bar Association Professional Responsibility Section concludes that the Vermont Rules of Professional Conduct ("VRPC") do not compel a specific answer to the question whether a lawyer can search for metadata within an electronic document prepared by and received from opposing counsel. The Section further concludes that a lawyer who receives an electronic document from opposing counsel that contains inadvertently disclosed, privileged and confidential metadata must notify the sending lawyer, with the question whether the receiving lawyer can use this information being decided by a court of competent jurisdiction. With respect to discovery practice in the litigation context, the Section concludes that, with limited exceptions relating to privileged matters, lawyers are obligated to disclose all responsive information including metadata to opposing counsel, and nothing prohibits the recipient from searching for electronic information about the history of the document or file.

Questions Presented:

The Vermont Bar Association Board of Managers has posed a series of questions to the Professional Responsibility Section about metadata.

The Board first inquires as follows about situations where a lawyer receives an electronic file from opposing counsel: (a) Can the receiving lawyer use tools in the program that created the file to mine\(^1\) for metadata?; (b) Can the receiving lawyer use more specialized tools to mine for metadata?; (c) Can the receiving lawyer engage the “track changes” function to review the history of edits made to the document; (d) Is the receiving lawyer’s responsibility different if the sending lawyer has inadvertently left the “track changes” function engaged, so that the entire history of changes to the document are exposed without any action being taken by the receiving lawyer.

The Board also inquires about disclosure of and searching for metadata during discovery in the litigation context, including whether (a) in the absence of a court order addressing discovery issues relating to metadata, lawyers or parties can mine for metadata in documents received from the opposing party during discovery; and (b) whether it is permissible for a party to remove metadata from documents before disclosing them during discovery.

\(^1\) The Section notes that the term “mine” appears to be a pejorative characterization of the use of electronic tools to analyze electronic documents. Throughout this Opinion, the phrase “search” is used in place of the phrase “mine,” because it characterizes the search for embedded metadata in a more neutral manner.
Analysis

The questions presented by the VBA Board of Governors pose a number of inquiries. First, does a lawyer who sends electronic documents to opposing counsel have a duty to exercise reasonable care to avoid disclosing confidential metadata? Second, can a lawyer who receives electronic documents from opposing counsel search those documents for metadata? Third, what steps should be taken by a lawyer who becomes aware that electronic documents received from opposing counsel contain metadata? These questions have been the subject of a growing body of ethics opinions issued by the American Bar Association and various State Bar Associations. This opinion now summarizes the conclusions of these opinions and expresses its view on each.

Potentially Applicable Provisions of the Vermont Rules of Professional Conduct

As discussed in detail below, no provisions of the VRPC speak directly to the questions presented in this Opinion, although recently adopted VRPC 4.4(b), which becomes effective September 1, 2009, does address the obligation of a lawyer who receives inadvertently disclosed documents. The following provisions of the Rules, reprinted below in the form in effect in Vermont as of September 1, 2009, have formed the legal bases for Ethics Opinions issued by other Bar Associations reaching contradictory conclusions about the questions presented.

VRPC 1.1 Competence:

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

VRPC 1.3 Diligence:

A lawyer shall act with reasonable diligence . . . in representing a client.

VRPC 1.6(a) Confidentiality of Information:

A lawyer shall not reveal information relating to representation of a client unless the client gives informed consent . . . .

VRPC 3.4 Fairness to Opposing Party and Counsel

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;
(b) falsify evidence, counsel or assist a witness to testify falsely, or offer an inducement to a witness that is prohibited by law;
(c) knowingly disobey an obligation under the rules of a tribunal except for an open refusal based on an assertion that no valid obligation exists;
(d) in pretrial procedure, make a frivolous discovery request or fail to make reasonably
diligent effort to comply with a legally proper discovery request by an opposing party;
.... or
(f) request a person other than a client to refrain from voluntarily giving relevant
information to another party unless:
(1) the person is a relative or an employee or other agent of a client; and
(2) the lawyer reasonably believes that the person’s interests will not be adversely
affected by refraining from giving such information.

VRPC 4.4 Respect for Rights of Third Persons:

(a) In representing a client, a lawyer shall not use means that have no substantial purpose
other than to embarrass, delay, or burden a third person, or use methods of obtaining
evidence that violate the legal rights of such a person.
(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.

VRPC 8.4 Misconduct:

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) engage in a “serious crime,” defined as illegal conduct involving any felony or
involving any lesser crime a necessary element of which is interference with the
administration of justice, false swearing, intentional misrepresentation, fraud, deceit,
bribery, extortion, misappropriation, theft, or an attempt or a conspiracy or solicitation of
another to commit a “serious crime”;
(c) engage in conduct involving dishonesty, fraud, deceit or misrepresentation;
(d) engage in conduct that is prejudicial to the administration of justice ....

Duty of Sending Lawyer

The Bar Associations that have examined the duty of the sending lawyer with respect to
metadata have been virtually unanimous in concluding that lawyers who send documents in
electronic form to opposing counsel have a duty to exercise reasonable care to ensure that
metadata containing confidential information protected by the attorney client privilege and the
work product doctrine is not disclosed during the transmission process. See Alabama Ethics Op.
2008-2009-4; New York City Lawyers Ass’n Ethics Op. No. 738 (2008); New York State Ethics
Op. 782 (2004). A number of other ethics opinions note that a sending lawyer has tools available
to prevent against the risk of disclosing client confidences when electronic documents are
transmitted to opposing counsel, but do not affirmatively address the scope of the sending
lawyer’s duty to take these steps. See Pennsylvania Formal Ethics Op. 2007-500; ABA Formal
Ethics Op. 06-442.
This Opinion agrees that, based upon the language of the VRPC, a lawyer has a duty to exercise reasonable care to ensure that confidential information protected by the attorney-client privilege and the work product doctrine is not disclosed. This duty extends to all forms of information handled by an attorney, including documents transmitted to opposing counsel electronically that may contain metadata embedded in the electronic file. This duty has its roots in VRPC 1.1, which requires lawyers to provide competent representation; VRPC 1.3, which requires lawyers to exercise diligence; and VRPC 1.6, which requires lawyers to protect confidential client information.

The Professional Responsibility Section notes that various tools are available to comply with this duty to exercise reasonable care, including programs to “scrub” metadata from electronic documents before they are dispatched, converting electronic documents to a read-only, PDF format before transmission, or insisting on transmission of sensitive documents only on paper. The steps that should be taken by the sending lawyer in specific instances depend on the circumstances, and are beyond the scope of this opinion.

**Duty of Receiving Lawyer**

The duty of the receiving lawyer is a matter that has been the subject of substantially more disagreement.

In the following ethics opinions, various State Bar Ethics Committees have concluded that applicable rules of professional conduct prohibit a receiving lawyer from searching for metadata in documents that are received electronically. See Alabama Ethics Op. RO 2007-02; Arizona Ethics Op. 07-03; Florida Ethics Op. 06-2; New Hampshire Ethics Op. 2008-2009/4; New York City Lawyers Ass’n Ethics Op. No. 738 (2008); New York State Ethics Op. 782 (2004). The foundations for the conclusions reached in these Opinions are located in the rules of professional conduct protecting confidential information, prohibiting lawyers from engaging in conduct that is dishonest, deceitful, or prejudicial to the administration of justice; and requiring respect for the rights of others. Through various chains of inference, and based on Professional Conduct Rules drafted differently from the Rules in Vermont, these opinions conclude that a lawyer who searches for metadata is unjustifiably attempting to intrude on the confidential relationship between the opposing lawyer and client, which is conduct that is dishonest or deceitful, and prejudicial to administration of justice.

On the other hand, a series of other ethics opinions reach the opposite conclusion, finding that the Rules of Professional Conduct do not contain any prohibition, whether express or implied, on searching electronic documents for embedded metadata, and that characterization of such searching as “deceitful,” “dishonest,” and “prejudicial” is not supported by the Rules. See Colorado Ethics Op. 119 (2008); DC Ethics Op. 341 (2007); Pennsylvania Formal Ethics Op. 2007-500; ABA Formal Ethics Op. 06-442.

Reviewing the language of the Vermont Rules of Professional Conduct quoted above, the Vermont Bar Association Professional Responsibility Section finds nothing to compel the conclusion that a lawyer who receives an electronic file from opposing counsel would be ethically prohibited from reviewing that file using any available tools to expose the file's
content, including metadata. A rule prohibiting a search for metadata in the context of electronically transmitted documents would, in essence, represent a limit on the ability of a lawyer diligently and thoroughly to analyze material received from opposing counsel. None of the Rules in effect in Vermont either state or imply that lawyers must refrain from thoroughly reviewing documents and information received from opposing counsel, regardless of the medium is which the document is transmitted. The Rule where such an obligation would most likely be found -- VRPC 3.4 Fairness to Opposing Party and Counsel -- is wholly silent on this issue. Neither do VRPC 4.4 Respect for Rights of Third Persons, or VRPC 8.4 Misconduct, directly address this issue. On the other hand, there is a clear basis for an inference that thorough review of documents received from opposing counsel, including a search for and review of metadata included in electronically transmitted documents, is required by VRPC 1.1 Competence, and VRPC 1.3 Diligence.

The existence of metadata is an unavoidable aspect of rapidly changing technologies and information data processing tools. It is not within the scope of this Section's authority to insert an obligation into the Vermont Rules of Professional Conduct that would prohibit a lawyer from thoroughly reviewing documents provided by opposing counsel, using whatever tools are available to the lawyer to conduct this review.

**Duty Imposed Upon Lawyer Who Learns Of Receipt Of Inadvertently Disclosed Privileged Information**

Answering the question whether a lawyer can search for metadata does not, however, end the analysis. The more critical inquiry arguably is whether inadvertently disclosed confidential information, including metadata, can be used by the lawyer who receives it.

Whether inadvertent disclosure of privileged information constitutes a waiver of the document's privileged status is a question of substantive law. Different approaches have been taken by courts throughout the United States when addressing this issue, but research has not revealed any case law in Vermont addressing the impact of inadvertent disclosure of privileged documents.

Given that the attorney-client privilege is intended to protect the client, many courts have chosen to protect the privilege when inadvertent disclosure occurs, focusing on whether the client intended the disclosure to occur and whether counsel had authority to disclose. See e.g., Mendenhall v. Barber-Greene Co., 531 F. Supp. 951, 954-55 (N.D.III. 1982); Berg Elecs., Inc. v. Moylex Inc., 875 F. Supp. 261, 263 (D. Del. 1995); Corey v. Norman, Hanson & DeTroy, 742 A.2d 933, 941 (Me. 1999). However, alternate approaches that are less protective of the attorney client privilege also have been adopted. One such approach provides that inadvertent disclosure destroys the privilege if the lawyer and client did not take adequate steps to protect confidentiality. See e.g., Gray v. Bicknell, 86 F.3d 1472, 1483-84 (8th Cir. 1996). Effective September 19, 2008, the Federal Rules of Evidence were amended to add a variation of this position. Current Federal Rule of Evidence Rule 502(b) provides that, in Federal Court proceedings, inadvertent disclosure does not result in waiver of the attorney client privilege or

---

2 Given this conclusion, this Opinion does not separately analyze the four different mechanisms for locating metadata that are listed in the questions presented by the VBA Board of Governors.
work product protection if reasonable steps to prevent disclosure were taken by the holder of the privilege or protection, and reasonable steps were promptly taken by the holder of the privilege or protection to respond to the inadvertent disclosure. Adoption of Rule 502 arguably overruled the holdings of previous Federal Court decisions, including International Digital Sys. Corp. v. Digital Equip. Corp., 120 F.R.D. 445, 449-50 (D. Mass. 1988), and Federal Dep. Ins. Corp. v. Singh, 140 F.R.D. 252, 253 (D. Me. 1992), which took the blanket position that inadvertent disclosure waives the privilege, because confidentiality had been lost.

It is beyond the scope of this Ethics Opinion to address what analysis the Vermont Supreme Court should adopt on the question of inadvertent disclosure. However, the steps that lawyers should take upon learning that inadvertently disclosed privileged information has come into their possession is a matter that has been the subject of substantial discussion in the Ethics Opinions and is at the core of the inquiry posed by the VBA Board of Governors. Accordingly, this Opinion now turns to this issue.

In 1992, the American Bar Association Committee on Ethics and Professional Responsibility issued Formal Opinion 92-368. This Opinion advised that a lawyer who receives materials which appear on their face to be privileged and clearly appear not to be intended for the receiving lawyer must not look at those materials, must contact the sending lawyer, and must follow the sending lawyer’s instructions relating to those materials. Substantial debate followed issuance of this Opinion, and the ABA Ethics Committee ultimately added Model Rule of Professional Conduct 4.4(b), which 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.

Pursuant to amendments to the Vermont Rules of Professional Conduct promulgated on June 17, 2009, Rule 4.4(b) becomes effective in Vermont on September 1, 2009.

As explained in its Comments, the purpose behind Rule 4.4(b) is to ensure that lawyers who inadvertently disclose privileged and confidential documents to opposing counsel can take protective measure in an effort to limit or eliminate damage to their client’s interests. The Comment continues by recognizing, however, that questions including whether additional remedies may be available to the sending lawyer, and whether inadvertent disclosure leads to waiver of the privilege, depend on substantive law and are beyond the scope of the Rules.3

With the adoption of Rule 4.4(b), Vermont lawyers are subject to the obligation to notify opposing counsel if they receive documents that they know or reasonably should know were inadvertently disclosed. Whether inadvertent disclosure results in waiver of the attorney-client privilege or the work product protection, and whether the receiving lawyer can review and use the inadvertently disclosed information, remain issues of substantive law.

---

3 As a result of the amendment of Model Rule 4.4(b), including its clear requirements for the steps that must be taken when confidential documents are inadvertently disclosed, ABA Formal Opinion 05-437 withdrew Formal Opinion 92-368.
Litigation Context

The inquiry posed by the VBA Board of Governors relating to the litigation context poses somewhat different considerations. While it is beyond the scope of this Opinion to address the discovery rights and obligations of parties in the litigation context, the Section makes the following observations.

The provisions of the VRPC that are cited above, including the requirements of acting competently, diligently, and in a manner that protects client confidences and respects the rights of third parties, apply to all of an attorney's legal related activities, including in the litigation context. Basic rules of diligence, competence, and prudence caution a lawyer who is preparing to disclose documents during discovery thoroughly to review those documents in order, among other things, to ensure that communications protected by the attorney client privilege and the work product doctrine are not being disclosed. This rule applies with equal force to electronic discovery, where basic rules of competence now require lawyers to be aware that discoverable information may be included in electronic documents, and that privileged and confidential information may be embedded in electronic files, including in hidden metadata.

Standard practice and procedural rules in litigation matters allow lawyers to withhold documents containing privileged and confidential communications when serving discovery responses, and those rules apply with equal force to production of electronic documents. Where such materials are being withheld from discovery disclosures, applicable rules may require preparation and service of a privilege log, which also should list any privileged and confidential electronic documents that are being withheld from production. See, e.g., Fed. R. Civ. P. 26(b)(3)(A) (requiring party that withholds otherwise discoverable information based on privilege or work product claim to make the claim expressly and describe the documents being withheld from production).

Except to this extent, the Professional Responsibility Section is aware of no authority or support for the proposition that a lawyer can redact, remove, or withhold metadata from electronic client documents that are being disclosed during discovery. Neither is the Committee aware of any restriction on the ability of the receiving lawyer or party fully to analyze electronic documents received during discovery, including use of any available tools to search for metadata embedded within those electronic files.4

4 It should be noted, however, that recent amendments to the Federal Rules of Civil Procedure codify a procedure for use in Federal Court when inadvertent disclosures occur. Pursuant to Fed. R. Civ. P. 26(b)(3)(B), when a party inadvertently discloses materials that it believes are privileged or work product and provides notice to opposing counsel, the recipient has the duty, among other things, promptly to return, destroy, or sequester the information, and not to use or disclose the information until the privilege or work product claim has been resolved. These recent amendments to Rule 26 provide clear direction to lawyers confronted with inadvertent disclosure issues, and the Professional Responsibility Section believes it could be useful for the Vermont Supreme Court to consider the possibility of making similar amendments to the Vermont Rules of Civil Procedure.