

AMERICAN BAR ASSOCIATION

STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion 06-442

August 5, 2006

Review and Use of Metadata

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."¹ This opinion² 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 party³ or an agent of an adverse party. The Committee

1. 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.

2. 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.

3. 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.

AMERICAN BAR ASSOCIATION STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY, 321 N. Clark Street, Chicago, Illinois 60610-4714 Telephone (312)988-5300 CHAIR: William B. Dunn, Detroit, MI □ Elizabeth Alston, Mandeville, LA □ T. Maxfield Bahner, Chattanooga, TN □ Amie L. Clifford, Columbia, SC □ Timothy J. Dacey, III, Boston, MA □ James A. Kawachika, Honolulu, HI □ Steven C. Krane, New York, NY □ John P. Ratnaswamy, Chicago, IL □ Irma Russell, Memphis, TN □ Thomas Spahn, McLean, VA □ CENTER FOR PROFESSIONAL RESPONSIBILITY: George A. Kuhlman, Ethics Counsel; Eileen B. Libby, Associate Ethics Counsel

© 2006 by the American Bar Association. All rights reserved.

concludes that the Rules generally permit a lawyer to do so.⁴

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.⁵ 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.

4. 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_Opinions/Opinion_782.htm (last visited Sep. 15, 2006) (under New York’s Code of Professional Responsibility, New York’s version of predecessor ABA Model Code of Professional Responsibility, lawyers must exercise reasonable care to prevent inappropriate disclosure of client confidences and secrets contained in metadata).

5. 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.

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.⁶ 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,⁷ 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.”⁸ 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.⁹

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

7. 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.

8. 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.

9. 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

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.¹⁰ 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.¹¹ 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.¹²

The Committee observes that counsel sending or producing electronic doc-

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.

10. 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 "intentional[ly] 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/53EDED5599019138525719A006DCE1B/\\$FILE/062%20pao.pdf?OpenElement#search=%22Florida%20%2B%20opinion%20%2B%20metadata%22](http://www.floridabar.org/TFB/TFBResources.nsf/Attachments/53EDED5599019138525719A006DCE1B/$FILE/062%20pao.pdf?OpenElement#search=%22Florida%20%2B%20opinion%20%2B%20metadata%22) (last visited Sept. 15, 2006).

11. 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/e2k-rule44rem.html> (last visited Sept. 15, 2006), regarding this amendment.

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

uments 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.¹³ 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,¹⁴ 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.¹⁵ 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.

13. 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[.]”)

14. 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.

15. 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.