

NEW HAMPSHIRE BAR ASSOCIATION
Ethics Committee Opinion 2008-2009/4

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, including 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 electronic materials subject to discovery or subpoena under applicable rules of court or 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 electronic documents subject to discovery or subpoena under applicable rules of court or 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.*, ME 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 red-lined 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").

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.

548562_1