119 DISCLOSURE, REVIEW, AND USE OF METADATA

Adopted May 17, 2008.

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.[1]

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 rea-

sonably 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.[2] 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.[3] 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.[4] *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.[5] *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.[6] *See* CBA Formal Ethics Op. 108, "Inadvertent Disclosure of Privileged or Confidential Documents" (2000).

NOTES

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 Information that appeared to have been inadvertently produced.

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.