

N.C. State Bar
2009 Formal Ethics Opinion 1
January 15, 2010

Review and Use of Metadata

Opinion rules that a lawyer must use reasonable care to prevent the disclosure of confidential client information hidden in metadata when transmitting an electronic communication and a lawyer who receives an electronic communication from another party or another party's lawyer must refrain from searching for and using confidential information found in the metadata embedded in the document.

Background

In the representation of clients in all types of legal matters, lawyers routinely send emails and electronic documents, spreadsheets, and PowerPoint presentations to a lawyer for another party (or directly to the party if not represented by counsel). The email and the electronic documents contain metadata¹ or embedded information about the document describing the document's history, tracking and management² such as the date and time that the document was created, the computer on which the document was created, the last date and time that a document was saved, "redlined" changes identifying what was changed or deleted in the document, and comments included in the document during the editing process. Pennsylvania Bar Ass'n. Comm. on Legal Ethics and Professional Responsibility, Formal Opinion 2007-500, *reconsidered* Pennsylvania Formal Op. 2009-100, notes that, although most metadata contains "seemingly harmless information," it 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." This embedded information may be readily revealed by a "right click" with a computer mouse, by clicking on a software icon, or by using software designed to discover and disclose the metadata.³ On occasion, one software application automatically displays or uses metadata that another software application hides from the user. The sender of the document may be unaware that there is metadata embedded in the document or mistakenly believe that the metadata was deleted from the document prior to transmission. The Ethics Committee is issuing this opinion sua sponte in light of the importance of the ethical issues raised by metadata.

Inquiry #1:

What is the ethical duty of a lawyer who sends an electronic communication to prevent the disclosure of a client's confidential information found in metadata?

Opinion #1:

Rule 1.6(a) of the Rules of Professional Conduct prohibits a lawyer from revealing information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized to carry out the representation, or disclosure is permitted by one of the exceptions to the duty of confidentiality set forth in paragraph (b) of the rule. As noted in comment [20] to the rule, "[w]hen transmitting a communication that includes information acquired during the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients." Therefore, a lawyer who sends an electronic communication must take reasonable precautions to prevent the disclosure of confidential information, including information in metadata, to unintended recipients.⁴

RPC 215 addressed the preservation of confidential client information when using modern forms of communication including cellular phones and email. The opinion states that the professional obligation to use reasonable care to protect and preserve confidential information extends to the use of communications technology; "[h]owever, this obligation does not require that a lawyer use only infallibly secure methods of communication." Nevertheless, "a lawyer must take steps to minimize the risks that confidential information may be disclosed in a communication."

Lawyers have several options to minimize the risk of disclosing confidential information in an electronic communication. Lawyers should exercise care in using software features that track changes, record notes, allow "fast saves," or save different versions, as these features increase the amount of metadata within a document. Metadata "scrubber" applications remove embedded information from an electronic document and may be used to remove metadata before sending an electronic document to opposing counsel. Finally, lawyers may opt to use an electronic document type that does not contain as much metadata, such as the portable document format (PDF), or may opt to use a hard copy or fax. Both commercial and freeware software solutions exist to help lawyers avoid inadvertently disclosing confidential information in an electronic communication.

What is reasonable depends upon the circumstances including, for example, the sensitivity of the confidential information that may be disclosed, the potential adverse consequences from disclosure, any special instructions or expectations of a client, and the steps that the lawyer takes to prevent the disclosure of metadata. Of course, when electronic communications are produced in response to a subpoena or a formal discovery request in civil litigation, the responding lawyer may not remove or restrict access to the metadata in the communications if doing so would violate any disclosure duties under law, the Rules of Civil Procedure, or court order.

Inquiry #2:

May a lawyer who receives an electronic communication from another party or the party's lawyer search for and use confidential information embedded in the metadata of the communication without the consent of the other party or lawyer?

Opinion #2:

No, a lawyer may not search for confidential information embedded in metadata of an electronic communication from another party or a lawyer for another party. By actively searching for such information, a lawyer interferes with the client-lawyer relationship of another lawyer and undermines the confidentiality that is the bedrock of the relationship. Rule 1.6. Additionally, if a lawyer unintentionally views confidential information within metadata, the lawyer must notify the sender and may not subsequently use the information revealed without the consent of the other lawyer or party.

The New York State Bar was the first to adopt the position that a lawyer should not search metadata for confidential information. The state bars of Alabama, Arizona, Florida, and Maine have followed this position.⁵ New York Ethics Opinion 749 holds 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 [the New York] Disciplinary Rules.

Agreeing with the position of the New York State Bar, the Alabama State Bar Disciplinary Commission in Opinion 2007-02 finds that, "[t]he 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." Although the ABA Standing Committee on Ethics and Professional Responsibility, in Formal Opinion 06-442 (2006),⁶ takes the position that the Model Rules of Professional Conduct do not prohibit a lawyer from reviewing and using metadata, this position was subsequently rejected by the State Bar of Arizona among others. Arizona Opinion 07-03 observes that under the ABA opinion, which puts "the sending lawyer...at the mercy of the recipient lawyer..., the sending lawyer might conclude that the only ethically safe course of action is to forego the use of electronic document transmission entirely...[this is not] realistic or necessary."

The North Carolina State Bar Ethics Committee agrees that a lawyer may not ethically search for confidential information embedded within an electronic communication from another party or the lawyer for another party. To do so would undermine the protection afforded to confidential information by Rule 1.6 and would interfere with the client-lawyer relationship of another lawyer in violation of Rule 8.4(d), which prohibits conduct that is "prejudicial to the administration of justice."

The Ethics Committee recognizes that it is possible for a lawyer to unintentionally find confidential information upon viewing the contents of an electronic communication. If this occurs, the lawyer must notify the sender and may not subsequently use the information revealed without the consent of the other lawyer or party.

Rule 4.4(b) requires a lawyer who receives a writing relating to the representation of a client that the lawyer knows, or reasonably should know, was inadvertently sent, to promptly notify the sender. Receiving confidential information embedded in the metadata of an electronic communication is analogous to receiving, for example, a faxed pleading that inadvertently includes a page of notes from opposing counsel. Although the receiving lawyer did not seek out the confidential information, the receiving lawyer in either situation has a duty to "promptly notify the sender" under Rule 4.4(b) if the receiving lawyer "knows or reasonably should know that the writing was inadvertently sent." Although the technology involved is different, the Ethics Committee believes that a lawyer who can recognize confidential information inadvertently included in a fax can also recognize confidential information inadvertently included in an electronic document.

Further, a lawyer who intentionally or unintentionally discovers confidential information embedded within the metadata of an electronic communication may not use the information revealed without the consent of the other lawyer or party.

Although the receipt of confidential information embedded in metadata is analogous to the receipt of a page of handwritten notes in a faxed pleading for purposes of notifying the sender under Rule 4.4(b), metadata differs from the readily apparent information contained in a paper communication. Confidential information may inadvertently be included in the metadata of an electronic document despite reasonable efforts by a sender to stay abreast of rapid technological changes and to prevent the transmission of confidential information. The exchange of electronic documents, however, is vital to the functioning of the legal profession in the twenty-first century. Although Rule 4.4(b) does not require a lawyer to return an inadvertently sent paper document or specifically prohibit the use of information contained in such a document, Rule 8.4(d) prohibits conduct that is "prejudicial to the administration of justice." As comment [4] to Rule 8.4 observes, "[t]he phrase 'conduct prejudicial to the administration of justice' in paragraph (d) should be read broadly to proscribe a wide variety of conduct, including conduct that occurs outside the scope of judicial proceedings." Allowing the use of confidential information that is found embedded within metadata would inhibit the efficient functioning of the modern justice system and also undermine the protections for client confidences in the Rules of Professional Conduct and the attorney-client privilege. Therefore, the use of found metadata is "prejudicial to the administration of justice" in violation of Rule 8.4(d) and is prohibited.

In summary, a lawyer may not search for and use confidential information embedded in the metadata of an electronic communication sent to him or her by another lawyer or party unless the lawyer is authorized to do so by law, rule, court order or procedure, or the consent of the other lawyer or party. If a lawyer unintentionally views metadata, the lawyer must notify the sender and may not subsequently use the information revealed without the consent of the other lawyer or party.

Endnotes

1. Metadata is explained in Pennsylvania Bar Ass'n. Comm. on Legal Ethics and Professional Responsibility, Formal Op. 2007-500 (2007), *reconsidered* Pennsylvania Formal Op. 2009-100 (2009), as follows: "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."
2. Arizona State Bar Comm. on the Rules of Professional Conduct, Op. 07-03 (2007).
3. Pennsylvania Formal Op. 2007-500 (2007), *reconsidered* Pennsylvania Formal Op. 2009-100 (2009).
4. This is consensus position among the jurisdictions that have considered the issue as well as the ABA Standing Committee on Ethics and Professional Responsibility. Alabama State Bar Disciplinary Comm'n, Op. 2007-02 (2007); Arizona State Bar Comm. on the Rules of Professional Conduct, Op. 07-03 (2007); Colorado Bar Ass'n. Ethics Comm., Op. 119 (2008); District of Columbia Legal Ethics Comm., Op. 341 (2007); Florida Professional Ethics Comm., Ethics Op. 06-2 (2006); Maine Bd. of Bar Overseers Professional Ethics Comm'n., Op. 196 (2008); Maryland State Bar Ass'n. Comm. on Ethics, Op. 2007-09 (2006); New York State Ethics Op. 782 (2004); Pennsylvania Formal Op. 2009-100 (2009); ABA Standing Comm. on Ethics and Professional Responsibility, Formal Op. 06-442 (Aug. 5, 2006).
5. Alabama Ethics Op. 2007-02 (2007); Arizona Op. 07-03 (2007); Florida Ethics Op. 06-2 (2006); Maine Op. 196 (Oct. 21, 2008); and New York Ethics Op. 749 (2001). District of Columbia Legal Ethics Comm. Op. 341 (2007) holds that a lawyer may not view metadata if the lawyer has actual knowledge that it was provided inadvertently.
6. ABA Formal Op. 06-442 (2006) concludes that the Model Rules of Professional Conduct permit a lawyer to review and use metadata contained in email and other electronic documents. The Colorado Bar Association, Maryland State Bar Association, and Pennsylvania Bar Association agree with the position expressed in the ABA opinion. Colorado Op. 119 (2008); Maryland Op. 2007-09 (2006); Pennsylvania Op. 2009-100 (2009).