Metadata: I sent you what?

Ethics Opinions Governing the Search for and Disclosure of Metadata

A Comparative Analysis

By Benjamin Gichner, Esq.

January 2013

Table of Contents

I. Meta “what”? - Introduction and Scope

A junior associate collaborates with his supervising attorney in drafting a motion in limine to exclude the opposing party’s expert from testifying at trial. During the collaboration, both the junior and senior attorney make comments to each other within the word processor (i.e. track changes in Microsoft Word) about various edits and revisions that should be made. After filing the document, the junior attorney e-mails it to opposing counsel in its native format (i.e. Word format or .docx).

On its face, the electronic file appears identical to a printed copy of the same document. However, underneath the skin of the document existed metadata that potentially included sensitive, confidential information, attorney work product, litigation or negotiation theories, and/or other data that would otherwise not exist in a printed copy of the motion. Hence, the junior attorney may have just opened the door to a litany of ethical violations, potential sanctions, and other issues that could jeopardize not only the client’s confidentiality, but also the junior attorney’s job.

A document is no longer a “document” in the traditional sense. Today, an electronic document usually contains hidden metadata. Metadata is

widely defined as “data about data.”[1] More specifically, metadata has been defined as data that describes the characteristics of digital documents, spreadsheets, presentations, or other electronically stored information.[2] Several types of metadata exist, and most types are created by software programs, such as Microsoft Word. For example, upon creating a Word document, the junior attorney above caused the software application to automatically create metadata that describes when the document was created, the number of pages, and the document creator (typically the name of the user who registered that copy of the software). While some metadata is hidden from a user, other types are accessible without much effort from the computer user.

Metadata can be erased from electronically stored information. The process of eliminating metadata from such information is often called “scrubbing.” Users can purchase existing software programs that scrub metadata from documents, spreadsheets, etc. for the user. Alternatively, people can create their own applications that effectively erase metadata. For example, a user with a Macintosh computer may use Automator, a free, Mac-exclusive software utility, to create an application that visibly sits on

the computer desktop as an icon and erases metadata on any file that a user drags and drops over the icon.[3]

The importance of metadata in the legal arena and its potential consequences for attorneys cannot be over-emphasized. The scope of this article focuses on ethical issues arising from both the search for and the disclosure of metadata in the legal context outside of formal discovery. However, issues arising from the transmission of electronic documents in formal discovery or pursuant to a subpoena are beyond the scope of this article. This article analyzes and compares states' ethics opinions governing both the search for and the disclosure of metadata outside of formal discovery. Also, it explains the impact of recent amendments to the ABA Model Rules of Professional Conduct that involve metadata. It addresses and discusses issues for attorneys who appear in multiple jurisdictions. Finally, it explores the future of metadata and its impact on the evolving concept of "competence" in the modern technological era.

Many jurisdictions have begun addressing electronically stored information and metadata in opinions issued from their respective ethics committees. Unsurprisingly, jurisdictions tend to deviate in their rules governing the search for and disclosure of metadata. Both jurisdictional

differences and the ethical rules related to diligence, confidentiality, and competence, necessitate attorneys' awareness and understanding of the continually arising ethical issues that revolve around metadata.

II. Disclosure of Metadata: What is the Sender's Duty?

Because certain types of metadata can encompass confidential or otherwise protected information relating to a client, the disclosure of such metadata can potentially cause an attorney to violate ethical rules governing both confidentiality and competence. The American Bar Association (ABA) and many states have addressed the question of what duty a "sending" attorney has with respect to the disclosure of metadata sent to a third party (including opposing counsel) outside of the formal discovery context.

In 2006, the ABA's Standing Committee on Ethics and Professional Responsibility discussed a sending attorney's duty to safeguard client confidentiality, but it declined to establish a rule specific to the disclosure of metadata in documents sent to a third party.[4] Instead, the Committee discussed ways attorneys can effectively eliminate such metadata, such as "by scrubbing metadata from documents or by sending a different version

of the document without the embedded information."[5] The Committee noted, however, that scrubbing metadata may constitute a violation of Model Rule of Professional Conduct 3.4(a).[6] For instance, such a violation may exist when both parties know that a document's underlying metadata contains evidentiary value. The removal of metadata, then, may be prohibited in certain situations. By declining to define the scope of a sending attorney's duty governing the disclosure of metadata, the ABA Committee presumably intended that the ethical rules governing client confidentiality would apply also to documents embedded with metadata and electronically stored information sent to a third party.

However, recognizing the importance of the evolution of technology in the legal arena, the ABA House of Delegates has recently passed a committee resolution which amends Model Rule of Professional Conduct (MRPC) 1.6 and its comments.[7] MRPC 1.6 now includes subsection (c), which requires "reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."[8] The official comments offer suggestions for determining what constitutes reasonable efforts.[9]

Similarly, in 2008 the State of Maine's Professional Ethics Commission held that 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."[10] The Maine Committee emphasized that this duty requires attorneys to reasonably apply a basic understanding of the existence of metadata embedded in electronic documents.[11] Further, attorneys must understand how to take practical measures to remove sensitive metadata when appropriate to prevent the disclosure of protected or confidential information.[12] Several other jurisdictions share the view that attorneys should generally keep abreast of the advances of technology in this context.[13]

Therefore, Maine preceded the ABA in establishing an ethical "duty" of the sending attorney to exercise reasonable care when transmitting electronic information to third parties. However, both Committees recognized the importance of metadata and the potential consequences that may arise upon its disclosure to third parties. Other jurisdictions have agreed that a sending attorney has a duty of 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.[14] However, not all jurisdictions define the scope of the "reasonable care" duty, leaving open the question of the amount of effort required to safeguard against disclosure of such sensitive information. For instance, the D.C. Professional Ethics Committee has stated that the sending attorney's duty simply falls under Rule 1.6 to safeguard confidentiality by employing "reasonably available technical means to remove such metadata before sending the document."[15]

Another northeastern jurisdiction, New Hampshire, recognizes the significance of electronic document transmission in modern law practice.[16] In Opinion 2008-2009/4, the New Hampshire Bar Association's Ethics Committee held 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."[17] The Committee, however, believed that what constitutes "reasonable care" will depend on several factors, including the subject matter of the document in question, the number of drafts, the existence of any comments within the document, and other relevant factors to be decided on a case-by-case basis.[18]

Thus, the Committee steered clear of imposing a per se rule governing the disclosure of metadata in electronic documents.[19] But a

careful analysis of this opinion reveals this committee's concern with the risks associated with electronic-document transmission. Although the Committee recognized the fast-paced nature of the technological era, it nonetheless warned that the failure to understand the risks inherent in sending electronic documents with embedded metadata can result in ethical violations.[20] Other jurisdictions have shared this view of a constantly-evolving duty of reasonable care amidst ever-changing advances in technology.[21]

III. Mining for Metadata: When is it "fine to mine?"

In the introductory example, the opposing counsel (the "receiving attorney") receives the e-mail from the junior associate and opens the motion in limine on his computer. He then uses a special forensic software application on his computer to search the document for underlying metadata.[22] The program reveals the document's metadata that is questionably protected by the attorney client privilege and/or work product doctrine. The receiving attorney may have just opened the door to several ethical violations and/or sanctions, depending upon the ethical rules in his jurisdiction.

The duty of the receiving attorney is, as the State of Vermont puts it, "a matter that has been subject to substantially more disagreement" among jurisdictions.[23] This debate has even caused one state's ethics committee members to publish a majority opinion that acknowledges the importance of the disagreeing members' minority views on this subject.[24] To understand the question of whether a receiving attorney may search for and review metadata embedded in such documents, one should familiarize himself with ABA Model Rule of Professional Conduct Rule 4.4(b), which states: "A lawyer who receives a document or electronically stored information relating to the representation of the lawyer's client and knows or reasonably should know that the document or electronically stored information was inadvertently sent shall promptly notify the sender."[25] The differing interpretations of this rule have created a debate over the scope of a receiving attorney's duty when he receives electronically stored information from opposing counsel outside of formal discovery.

In Formal Opinion 06-442, discussed *supra*, the ABA's Standing Committee on Ethics and Professional Responsibility mentioned the recent addition of Model Rule 4.4(b), identifying the sole requirement of providing notice to the sender of the receipt of inadvertently sent information.[26] This

requirement, the committee noted, carries with it the intention not to set other specific restrictions on receiving lawyers' conduct found in other Rules.[27] The committee expressed its disagreement with other jurisdictions that have found it "ethically impermissible" to mine for metadata.[28]

Moving West, however, some states take a different position. In 2008, Colorado's Professional Ethics committee decided that a receiving lawyer normally may review metadata in documents received from opposing counsel and third parties.[29] But, the committee held that if the receiving attorney is notified *before* reviewing the document that it contains confidential information embedded in metadata that was inadvertently sent, then the receiving attorney may not ethically view the metadata.[30] In such a circumstance, reviewing metadata would constitute a violation of Colorado's Rule of Professional Conduct 4.4(c).[31] To avoid this violation, the receiving attorney must adhere to the sending attorney's instructions regarding the document.[32] Although other jurisdictions agree that an attorney may not review metadata under these circumstances, some of them do not require the receiving attorney to comply with any subsequent instructions from the sender.[33]

Other jurisdictions have tackled this issue by focusing less on the concept of "mining" and more on the method by which it is done. In 2011, Oregon's Professional Ethics Committee ruled that a receiving attorney may ethically review metadata in documents sent by opposing counsel or third parties.[34] However, if the receiving attorney knows or reasonably should know that metadata was inadvertently included in the document, he is required to notify the sender.[35] The committee then focused on the receiving attorney's method of searching metadata and concluded that a receiving attorney may not use special software to hinder the sending attorney's reasonable efforts to scrub metadata before disclosure.[36] Such behavior, according to the committee, "can be analogous to surreptitiously entering the other lawyer's office to obtain client information."[37]

What this committee failed to address, however, is what it meant by "special software." Arguably, the Committee avoided this discussion due to lack of knowledge on the subject and breadth of modern types of forensic software on the market today. Inferably, the Committee would have no issue with a receiving attorney searching for metadata in other ways, such as right-clicking a file to view a document's properties. Right-clicking a file to see its properties, however, usually reveals only generic information,

limited to the document's date of creation, its author, and its file size. These types of data generally do not contain client confidences or attorney work product.

Yet other jurisdictions, like the State of Vermont, have adopted exactly the opposite viewpoint.[38] In 2009, the State of Vermont's Professional Ethics Committee agreed with other jurisdictions that allow a receiving attorney to ethically search for metadata in documents and other electronic information.[39] In fact, the committee stated that a receiving attorney may ethically use "any available tools to expose the file's content, including metadata."[40] This committee seemed more concerned with the receiving attorney's duty of competence and diligence in analyzing electronic files sent by opposing counsel and third parties.

In this opinion, the committee refused to accept the proposition that it had authority to limit a receiving attorney's use of data-processing tools to recover metadata.[41] Instead, it emphasized that the existence of metadata is "unavoidable" in this technological age.[42] Evidently, because the state ethical rules would not prohibit such behavior of a receiving attorney, then neither would the committee.

In 2012, the State of Washington's Ethics Committee issued an informal advisory opinion that effectively drew the line between ethical and unethical mining for metadata.[43] The committee ruled that a receiving attorney has a duty to promptly notify the sender if an electronic file includes "readily accessible metadata" (i.e., metadata accessible via standard word processing features).[44] On the other hand, if either (1) the sender attempted to scrub metadata before disclosure, or (2) the metadata was not readily accessible, then the receiving attorney may not ethically use special forensic software to recover underlying metadata.[45] Under such circumstances, the Committee believed that the use of special software to search for metadata would run afoul of public policy and constitute conduct that is prejudicial to the administration of justice.[46]

But, what is "readily accessible metadata?" These terms presumably mean data that can be accessed using standard word processing features, but the committee left the terms undefined. This omission raises the question of which metadata is "readily" accessible to a receiving attorney. A clear example of readily accessible metadata is data that can be accessed by using "track changes" in Microsoft Word. Beyond this example, though, the definition of "readily accessible" cannot be determined from this

committee's opinion. Presumably, readily accessible data could include any underlying data accessible without the need for special forensic software.

Of course, not all jurisdictions share the view that mining for metadata is ethical. North Carolina issued a 2009 formal opinion condemning the search for confidential information embedded in metadata received from another party or his lawyer.[47] The committee viewed metadata-mining as an interference with opposing counsel's attorney-client relationship. Several other jurisdictions prohibit the search for metadata by a receiving attorney.[48] These jurisdictions offer similar reasons for the prohibition of metadata mining, including the problem with recycling document templates.

IV. The Dangers of Using Templates

Many attorneys use templates for certain documents commonly filed with the court. A template can be any file that is used as a starting point for creating another file, and it usually has pre-formatted information, like a party caption. Although the use of templates is dangerous, it is convenient in contemporary law practice. For example, it is convenient to open a "Motion to Dismiss" from Client A's file and substitute the caption and client's name with that of a new client's information. The inherent danger in engaging in this practice comes from failing to scrub the underlying

metadata in these templates. In a 2007 formal opinion prohibiting the review of metadata by a receiving attorney, the Alabama Professional Ethics Committee warned against this practice of routinely recycling templates.[49] The committee explained that the electronic transmission of templates can lead to violations of client confidentiality.[50] The committee reasoned that a receiving attorney could review the document and "discover the original client's name and information."[51] In the example above, Client A's confidential information could be compromised due to a sending attorney's lack of diligence in scrubbing metadata from templates before sending them to a third party.

One jurisdiction prohibits the review of metadata if a receiving attorney has "actual knowledge" that the sender inadvertently sent metadata along with the document.[52] According to the D.C. Professional Ethics Committee, if a receiving attorney has actual *prior* knowledge that a document's metadata was unintentionally included in disclosure, he must refrain from reviewing the metadata's content.[53] What constitutes "actual knowledge" is fact-specific, but where a receiving attorney notices upon viewing the metadata that it was "clearly" sent unintentionally, actual knowledge is presumed.[54] Thus, the committee left *some* discretion with

the receiving attorney. It may not always be clear if a sending attorney intentionally included metadata or not. Here, at least part of this question is deferred to the receiving party's judgment.

At least one jurisdiction has deferred the *entire* question to the professional judgment of the receiving attorney.[55] Pennsylvania'a Committee on Legal Ethics and Professional Responsibility views unintentionally-embedded metadata as an inadvertent disclosure; thus, Rule 4.4(b) mandates that the receiving attorney accessing metadata "evaluate whether the extra-textual information was intended to be deleted or scrubbed from the document prior to transmittal."[56] If the receiving attorney concludes that the metadata was intentionally included with the document, he need not notify the sender. In fact, Pa. Rule of Professional Conduct 1.1 may *require* him to use such information, provided it is used without adverse consequence, and is beneficial to his client's case.[57]

V. Impact of ABA's New Amendments to MRPC 4.4(b)

The 2012 ABA Committee Resolution, discussed *supra*, also amended Model Rule of Professional Conduct Rule 4.4(b) to include the phrase "electronically stored information."[58] In addition, the comments to

this rule now explicitly define "electronically stored information" as encompassing embedded data (commonly referred to as "metadata").[59] Additionally, the comments to MRPC 4.4 now establish an obligation for the receiving attorney to notify the sender "if the receiving lawyer knows or reasonably should know that the metadata was inadvertently sent to the receiving lawyer."[60]

However, these recent amendments do not change the ABA's initial position that the receiving attorney may ethically review metadata embedded in documents sent by opposing counsel or third parties.[61] Instead, the Committee's position remains that in certain circumstances, reviewing metadata is ethical. In those circumstances, however, MRPC 4.4(b)'s notification requirement is now triggered if the receiving attorney knows or reasonably should know that the sending attorney "did not intend to include" such embedded metadata.[62]

VI. Appearing in Multiple Jurisdictions

Consider the problem that arises when a Vermont attorney e-mails documents with embedded metadata to opposing counsel located a few miles away, in New Hampshire. As discussed *supra*, the State of Vermont

allows a receiving attorney to review metadata sent by opposing counsel outside of formal discovery.[63] A young New Hampshire associate may assume that his state allows for metadata-review as well. These neighboring states have many similarities, but the rule governing the search for metadata is not one of them. Vermont and New Hampshire disagree on a receiving attorney's ethical conduct in reviewing metadata in electronic documents.[64] Therefore, although the Vermont attorney may ethically review a document's underlying metadata sent by the NH attorney, the NH attorney would violate his state's version of Model Rule 4.4(b) by engaging in the same conduct.[65] The near proximity of opposing jurisdictions like Vermont and New Hampshire can conceal the danger of making such an assumption in this context.

Due to a lack of jurisdictional uniformity with respect to metadata rules, attorneys who appear and practice in multiple jurisdictions need to familiarize themselves with the ethical rules in each jurisdiction in which they appear. At least one ethics committee has expressed its concern over the consequences of appearing in multiple jurisdictions.

In its Formal Opinion 12-01, the Wisconsin Professional Ethics Committee sent a subtle warning for attorneys not to assume that reviewing

metadata is always ethical simply because it is ethical in the jurisdiction in which he or she normally practices.[66] Reasoning that certain tribunals' local rules forbid the review of metadata absent consultation with the sending attorney, the committee warned that such conduct could violate its own version of Model Rule 3.4(c), which prohibits the knowing violation of a tribunal's rules.[67] Thus, an attorney who practices in multiple jurisdictions needs to familiarize himself with not only both jurisdictions' ethical rules relating to metadata, but also with the local rules of all tribunals in which he appears.

Pennsylvania's Committee on Legal Ethics & Professional Responsibility recently hinted at this issue and discussed the implication of its version of Model Rule 1.1.[68] As the committee emphasized, "A lawyer's duty to competently represent that client under Pennsylvania 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…".[69] The committee apparently recognized this issue as one of the receiving attorney's competence. It declared that in such a situation, "competent representation may require that the attorney refrain from disclosing or using this information."[70] As

more jurisdictions recognize this issue, the concept of "competent" representation will continue to evolve and likely expand. Attorneys will need to know each jurisdiction's respective rules for disclosing and reviewing metadata to competently represent clients in those respective jurisdictions. With the constant evolution of modern technology, this ethical duty of "competent" representation in multiple jurisdictions will continue to expand.

Therefore, it is imperative that attorneys who represent clients in multiple jurisdictions familiarize themselves with those jurisdictions' respective ethical rules governing the search and disclosure of metadata. As the above example illustrates, law firms merely a few miles from each other may be governed by rules mandating polar opposite actions by a receiving attorney in this context. The failure to understand each jurisdiction's rules governing metadata disclosure and review can open the door to ethical violations and sanctions.

VII. Technology's Impact on "Future Metadata"

As modern technology evolves, so will the concept of metadata, the types of metadata that new programs will create, and the new formats of electronically stored information that will inevitably permeate the legal

arena. Today, many attorneys use similar computer applications to produce electronic documents. For instance, most electronic documents sent by attorneys originate from either Microsoft Word, Apple Pages, Corel WordPerfect, or Adobe Acrobat. Each one of these applications produces electronic documents in a different format: ".doc/docx," ".pages." ".wpd," and ".pdf" respectively. Additionally, each program automatically creates certain metadata for its documents. Finally, each program allows various revisionary tools such as "commenting" and "track changes." Collaboration among attorneys is commonplace in modern law practice; thus, by working together with electronic documents, most attorneys create metadata every day, even if they are unaware.

But as technology continues to evolve, the number of formats for electronic documents and electronically stored information will continue to grow. Consequently, new forensic software applications will come out to scrub metadata from new programs and applications. As a result, more methods for retrieving "scrubbed" metadata from these programs (and future programs) will arise as new forensic software is created for these purposes.

Therefore, like most technological products, software programs designed to produce documents and scrub metadata will come and go at an increasingly-faster pace. Attorneys must understand their jurisdictions' rules for producing and searching metadata outside of formal discovery and keep abreast of these advances in technology every year. The breadth of the types of metadata (and consequently, the definition of metadata) will continue to expand. Without knowledge and understanding of the rules governing this fast-paced evolution of metadata, attorneys may fall below the standard for what constitutes a competent attorney.

VIII. "Competent" Attorneys Must Understand Metadata

Every ethics opinion discussed herein mentioned either Model Rule of Professional Conduct (MRPC) 1.1 or it's state-equivalent. The scope of an attorney's duty of competence has been constantly re-defined or broadened in these opinions.[71] Clearly, the conceptual notion of "competence" is changing due to the lack of uniformity among professional responsibility committees around the nation.

In a 2010 opinion issued by the Minnesota Lawyers Professional Responsibility Board, the Board defined an attorney's duty of

competence.[72] The Board stated that "competence" requires, *inter alia*, that attorneys understand that actions *can* be taken to prevent the disclosure of metadata.[73] Presumably, the more competent a sending attorney in removing metadata before transmission, the less likely an ethical violation will arise because of the transmission of metadata.

MRPC 1.1 will continue to permeate future decisions governing the search for and disclosure of metadata. The concept of attorney "competence" will likely continue to expand as technology advances each year. Consequently, attorneys in all states will benefit from Continuing Legal Education (CLE) programs that address ethical rules implicated by the use, search, and disclosure of metadata outside of formal discovery.

IX. Conclusion

Metadata has become a recent concern in modern American law practice. Most states, and the American Bar Association, agree that an attorney who sends electronic documents outside of formal discovery has a duty of reasonable care to ensure that client confidences embedded in metadata are not disclosed to third parties. Only a few states have declined to establish such a duty for a "sending attorney."

However, the heart of the metadata debate lies in the "receiving attorney's" duty when he receives electronic documents outside formal discovery. Few states, such as New York, have prohibited a receiving attorney from reviewing metadata sent by opposing counsel. But the majority of jurisdictions agree that their respective rules of professional conduct do not prohibit such review unless the receiving attorney either knows or reasonably should know that the transmission of the document(s) includes inadvertently sent metadata that contains confidential or otherwise protected information.

In the summer of 2012, the American Bar Association revised its Model Rules of Professional Conduct to address issues related to metadata and electronic transmission of documents among attorneys and third parties. Many state ethics committees (including the American Bar Association) have realized the importance of metadata and the consequences that arise from its inadvertent transmission outside the context of formal discovery. In response, ethics opinions are using this concern over metadata as a way to constantly re-define the duty of "competence" for attorneys.

Due to a lack of jurisdictional uniformity in rules governing the review of metadata, attorneys who appear in multiple jurisdictions must understand the local rules regarding metadata in all jurisdictions in which they appear. Otherwise, they are setting themselves up for possible ethical violations and sanctions.

As technology advances at an increasingly fast pace, the concept of metadata continues to expand. Subsequently, the concept of "competence" broadens each year. Metadata will be a relevant topic for Continuing Legal Education seminars in the near future. Understanding the risks inherent in electronic transmission is necessary in today's society. For attorneys, realizing the importance of metadata in electronic document transmission, and its different consequences among the fifty states, is an absolute necessity. As the Vermont/New Hampshire example shows, the difference between engaging in ethical conduct and risking ethical violations and sanctions can be just a few miles away.

Sources

[1] The Sedona ESI Glossary: E-Discovery & Digital Information Management, p. 34 (Third Edition, Sept. 2010) at http://www.thesedonaconference.org/publications (last accessed October 18, 2012).

[2] *See*, *supra* Endnote 1.

[3] The author has successfully attempted this method of scrubbing metadata.

[4] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 06-442 (2006).

[5] *Id*.

[6] *Id*. at Footnote 14 (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.")).

[7] *See* ABA Comm. on Ethics 20/20, Resolution 105A (2012).

[8] Model Rules of Prof'l Conduct R. 1.6(c) (amended 2012).

[9] Model Rules of Prof'l Conduct R. 1.6 cmt. 16 (...factors include "the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients.").

[10] Me. Prof'l Ethics Comm., Op. 196 (2008).

[11] *Id*.

[12] *Id*.

[13] *See*, *e.g.*, N.H. Ethics Comm., Op. 2008-2009/4 (2008-09).

[14] *See*, *e.g.*, Ala. Office of Gen. Counsel Ethics Op. 2007-02 (2007); Colo. Bar Ass'n. Ethics Comm., Formal Op. 119 (2008); D.C. Bar Ass'n. Formal Ethics Op. 341 (2007) ("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.").

[15] D.C. Bar Ass'n. Formal Ethics Op. 341 (2007).

[16] *See*, *e.g.*, N.H. Ethics Comm., Op. 2008-2009/4 (2008-09) ("Exchange of electronic documents is an essential part of modern law practice.").

[17] *Id*.

[18] *Id*.

[19] *Id*.

[20] *Id*.

[21] *See*, *e.g.*, Or. State Prof'l Responsibility Bd. Formal Op. 2011-187 (2011) ("What constitutes reasonable care will change as technology evolves.").

[22] An example of forensic software designed to scrub metadata is "Doc Scrubber." Information on the product can be found here.

[23] Vt. Bar Ass'n. Advisory Ethics Op. 2009-1 (2009).

[24] *See*, *e.g.*, Wis. Prof'l Ethics Comm., Formal Op. EF 12-01 (2012) ("Having considered...the views expressed by the minority of the Committee, the majority of the Committee does not believe that the Rules prohibit Wisconsin lawyers from searching for metadata in documents received from opposing counsel or third parties.").

[25] Model Rules of Prof'l Conduct R. 4.4(b) (amended 2012).

[26] *See*, *supra*, Endnote 5.

[27] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 06-442 (2006).

[28] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 06-442 (2006) (citing N.Y. Comm. on Prof'l Ethics, Op. 749 (2001) (A lawyer may not make use of computer software applications to surreptitiously "get behind" visible documents or to trace e-mail.").

[29] Colo. Bar Ass'n. Ethics Comm., Formal Op. 119 (2008).

[30] *Id.*

[31] Colo. Rules of Prof'l Conduct R. 4.4(c) (2012) ("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.")

[32] *Id.*

[33] *See*, *infra*, Or. State Prof'l Responsibility Bd. Formal Op. 2011-187 (2011) ("Oregon RPC 4.4(b) requires only notice to the sender; it does not require the receiving lawyer to return the document unread or to comply with a request by the sender to return the document.")

[34] Or. State Prof'l Responsibility Bd. Formal Op. 2011-187 (2011).

[35] *Id.*

[36] *Id.*

[37] *Id.*

[38] *See*, *e.g.*, Vt. Prof'l Responsibility Comm., Advisory Ethics Op. 2009-1 (2009). ("Such a rule would limit the ability of a lawyer diligently and thoroughly to analyze material received from opposing counsel.").

[39] *Id.*

[40] *Id.*

[41] *Id.*

[42] *Id.*

[43] *See*, *e.g.*, Wash. Exec. Ethics Bd., Informal Op. 2216 (2012).

[44] *Id.*

[45] *Id.*

[46] *Id.*

[47] N.C. Prof'l Ethics Comm., Op. 2009-1 (2009).

[48] *See*, *e.g.*, Ala. Prof'l Ethics Comm., Op. 2007-02 (2007); Fla. Prof'l Ethics Comm., Op. 06-2 (2006).

[49] *See*, *e.g.*, Ala. Prof'l Ethics Comm., Op. 2007-02 (2007).

[50] *See*, *e.g.*, Ala. Prof'l Ethics Comm., Op. 2007-02 (2007) ("Such disclosure of client identity and information could constitute a violation of Rule 1.6, Alabama Rules of Professional Conduct.).

[51] *Id.*

[52] D.C. Bar Ass'n. Formal Ethics Op. 341 (2007).

[53] *Id.*

[54] *Id.*

[55] *See* Pa. Comm. on Legal Ethics & Prof'l Responsibility, Formal Op. 2009-100 (2009).

[56] *Id.*

[57] *Id.*

[58] *See* ABA Comm. on Ethics 20/20, Resolution 105A (2012).

[59] Model Rules of Prof'l Conduct R. 4.4(b) cmt. 2.

[60] *See generally*, Model Rules of Prof'l Conduct R. 4.4(b) (amended 2012).

[61] *See*, *e.g.*, ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 06-442 (2006).

[62] *See* ABA Comm. on Ethics 20/20, Resolution 105A (2012).

[63] *See*, *supra* Endnote 40.

[64] *See* N.H. Ethics Comm., Op. 2008-2009/4 (2008-09) (concluding that Rule 4.4(b) imposes an obligation on the receiving lawyer to refrain from reviewing the metadata). But cf Vt. Prof'l Responsibility Comm., Advisory Ethics Op. 2009-1 (2009). ("Such a rule would limit the ability of a lawyer diligently and thoroughly to analyze material received from opposing counsel.").

[65] *See*, *supra*, Endnote 63.

[66] *See*, *e.g.*, Wis. Prof'l Ethics Comm., Formal Op. EF 12-01 (2012).

[67] *Id.*

[68] *See*, Pa. Comm. on Legal Ethics & Prof'l Responsibility, Formal Op. 2009-100 (2009) (discussing Pa. Rules of Prof'l Conduct R. 1.1).

[69] *Id.*

[70] *Id.*

[71] *See*, *e.g.*, Minn. Lawyers Prof'l Responsibility Bd. Op. 22 (2010) ("A lawyer is ethically required to act competently to avoid improper disclosure of confidential and privileged information in metadata in electronic documents.").

[72] *Id.*

[73] *See* Minn. Lawyers Prof'l Responsibility Bd. Op. 22 (2010) ("Competence requires that lawyers who use electronic documents understand that metadata is created in the generation of electronic documents, that transmission of electronic documents will include transmission of metadata, that recipients of the documents can access metadata, and that actions can be taken to prevent or minimize the transmission of metadata.").