

The Ethics of Mining for Metadata Outside of Formal Discovery

Elizabeth W. King*

TABLE OF CONTENTS

I.	INTRODUCTION.....	803
II.	METADATA: THE SOURCE OF THE ETHICAL DILEMMA.....	805
	A. <i>What is Metadata?</i>	805
	B. <i>Inadvertent Disclosure of Confidential Metadata</i>	807
III.	THE FEDERAL RULES OF CIVIL PROCEDURE AND METADATA..	810
	A. <i>Rules Governing Metadata in Formal Discovery</i>	810
	B. <i>The Rules Do Not Resolve the Ethical Dilemma</i>	813
IV.	ETHICS RULES IMPLICATED IN THE SENDING AND RECEIVING OF METADATA.....	815
V.	SEARCHING FOR METADATA OUTSIDE OF FORMAL DISCOVERY	816
	A. <i>Duties of the Sending Attorney: A Near-Unified Approach</i>	817
	B. <i>Duties of the Receiving Attorney: Competing Approaches</i>	819
	1. Attorney May Not Ethically Search for Metadata—New York, Florida, Arizona, Alabama, Maine	819
	2. Attorney May Ethically Search for Metadata—American Bar Association, Maryland, and Colorado ...	820
	3. A Middle Ground—The District of Columbia.....	824
	4. Let the Lawyers Decide—Pennsylvania	825
VI.	SEARCHING FOR METADATA IN ELECTRONIC DOCUMENTS RECEIVED OUTSIDE OF FORMAL DISCOVERY IS UNETHICAL	828
	A. <i>Requiring Sending Attorneys to Refrain from Creating Metadata and Sending Documents Electronically is Impractical and Unnecessary</i>	829

* Visiting Professor of Law, Hofstra Law School. I am grateful to Luke Dalton for valuable contributions and to Campbell University Norman Adrian Wiggins School of Law and Hofstra Law School for their support.

B.	<i>The Shortcomings of a Rule Forbidding Receiving Attorneys from Searching for Metadata are Adequately Addressed</i>	830
C.	<i>The Duty of Confidentiality Trumps the Duty of Diligence Because the Risk of Searching Outweighs the Benefits</i>	833
D.	<i>Searching and Reviewing Confidential Metadata is Dishonest and Prejudicial to the Administration of Justice</i>	835
VII.	PROFESSIONALISM REQUIRES ATTORNEYS TO REFRAIN FROM SEARCHING	838
VIII.	CONCLUSION.....	839

I. INTRODUCTION

One of the most familiar ethical issues in the practice of law is the conflict between advocating on behalf of a client and maintaining standards of professional ethics.¹ As technology in the practice of law increases, lawyers are facing a greater number of ethical challenges. This paper explores the particular ethical dilemma that is created when, outside of formal discovery, an attorney inadvertently, unknowingly, or unintentionally sends metadata hidden behind an electronic document to another attorney. This paper attempts to answer the question of whether the attorney who receives the electronic document, outside of formal discovery, should be ethically permitted to use computer software or some other means to search for the inadvertently disclosed metadata.

There is an ethical tension between allowing the receiving party to intentionally search for metadata and forbidding the receiving attorney from searching for metadata. Proponents of a rule permitting receiving attorneys to search for metadata argue that attorneys should be permitted to search to fulfill an ethical obligation to diligently represent their clients.² The metadata may contain information helpful to the representation of the client,³ and forbidding an attorney from searching for the metadata would hinder the attorney's ability to represent the client. The sending attorney, it is argued, should bear all responsibility for the inadvertent disclosure of metadata.⁴ This argument is strongest in the context of formal discovery and weakest outside of formal discovery and in transactional contexts.

On the other hand, proponents of a rule forbidding receiving attorneys from searching for metadata view the searching as an intentional intrusion on the attorney-client relationship of the sending attorney and the client. Despite reasonable precautions the sending attorney takes in advance of sending an electronic document, the receiving lawyer may learn information that the sending party did not intend for the receiving party to learn, including information protected by

1. WILLIAM M. SULLIVAN ET AL., EDUCATING LAWYERS: PREPARATION FOR THE PROFESSION OF LAW 129-30 (2007).

2. See generally Jessica M. Walker, *What's a Little Metadata Mining Between Colleagues?*, DAILY BUSINESS REVIEW, April 21, 2006, available at <http://www.stg.srs.com/eds/archive/What's%20a%20Little%20Metadata%20Mining%20Between%20Colleagues.pdf> (discussing attorneys' reasons for searching for metadata in electronic documents and noting that lawyers say they could be giving their client the short shrift by not looking at the metadata).

3. See *Williams v. Sprint/United Mgmt.*, 230 F.R.D. 640, 651-52 (D. Kan. 2005); ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 06-442, at 2 (2006).

4. See ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 06-442, at 2 (2006).

the attorney-client privilege or work product doctrine.⁵ The receiving attorney, it is argued, searches with the sole purpose of trying to find protected information, and searching with this purpose is viewed as an intentional intrusion into the attorney-client relationship.⁶ This argument bears the most weight outside of formal discovery and in transactional practices, and weakens during formal discovery.

This paper begins in Part II by exploring the source of the ethical dilemma, metadata. In Part III, the paper examines the Federal Rules of Civil Procedure, questions whether the Rules provide enough protection to the sending attorney, and explains why the Rules do not resolve the ethical question of whether, outside of formal discovery, a receiving attorney may search for metadata in electronic documents. After a discussion of the ethics rules implicated in the sending and receiving of metadata in Part IV, Part V of the paper compares the various approaches the ethics committees take to resolve the issue of whether an attorney may ethically search for metadata in electronic documents transmitted outside of formal discovery. Finally, Part VI of the paper evaluates the strengths and shortcomings of the varying approaches and concludes that, outside of formal discovery, a lawyer who receives electronic documents should not be ethically permitted to search for inadvertently disclosed metadata.

The paper advances two primary justifications for this conclusion. First, searching for inadvertently disclosed metadata is unethical because it violates the duty of confidentiality and the duty to refrain from engaging in conduct that is dishonest and prejudicial to the administration of justice. In response to the argument that the receiving attorney should be permitted to search for metadata to comply with an ethical obligation of diligent representation, the paper argues that when the risk of destroying the confidential nature of information outweighs any benefit to be achieved from searching, the duty of confidentiality should trump the duty of diligence. Moreover, the duty of diligence is not a license to engage in “offensive tactics” and to press for every advantage for a client at the cost of respect and professionalism.⁷ Second, a rule forbidding searching for metadata outside of formal discovery promotes professionalism and civility, and the interests of overall justice and professionalism should outweigh the slight, if any,

5. See N.Y. State Bar Ass’n Comm. on Prof’l Ethics, Op. 749, at 2 (2001); Ala. Office of Gen. Counsel, Op. RO-2007-02, at 3 (2007); State Bar of Ariz. Comm. on the Rules of Prof’l Conduct, Op. 07-03, at 2 (2007).

6. See N.Y. State Bar Ass’n Comm. on Prof’l Ethics, Op. 749, at 2 (2001); Ala. Office of Gen. Counsel, Op. RO-2007-02, at 3 (2007); State Bar of Ariz. Comm. on the Rules of Prof’l Conduct, Op. 07-03, at 2 (2007).

7. MODEL RULES OF PROF’L CONDUCT R. 1.3, cmt. 3 (2008).

advancement of substantive justice in a particular case gained by searching.

II. METADATA: THE SOURCE OF THE ETHICAL DILEMMA

A. *What is Metadata?*

The most common definition for metadata is “data about data.”⁸ However, this definition alone is not very helpful to an understanding of what metadata is and how it can be the source of an ethical dilemma. It is better to view metadata as “hidden data.” In other words, metadata is data that is not visible on the face of an electronic document when it is either viewed or printed but is instead hidden underneath the document.⁹ Generally, metadata includes information about authors of documents, embedded comments, tracked changes, and other technical information about the electronic document.¹⁰ Metadata is embedded in electronic documents and is always transmitted along with the electronic document itself when sent electronically, unless it is purposefully removed before the document is sent.¹¹ In order to view metadata, the person viewing the electronic document will ordinarily need to go looking for it.¹²

There are two principal ways metadata is created. First, metadata is created automatically by software programs, such as Microsoft Word and Microsoft Excel.¹³ Second, attorneys working on documents can, and often do, create metadata.¹⁴ Automatically-created metadata includes the name of the author of the document, the date on which the document was created and last edited, where the document was stored, and numerous other pieces of technical information.¹⁵ Metadata can also reveal all names of individuals who have made revisions to a document and the

8. DENNIS KENNEDY, *FRCP AND METADATA: AVOIDING THE LURKING E-DISCOVERY DISASTER* 7 (2007), <http://www.workshare.com/downloads/whitepapers/frcp-metadata.aspx>.

9. *Id.*

10. *Id.* at 7-8 (discussing types of metadata generally and the difference between automatically generated metadata and user-created metadata).

11. David Hricik, *I Can Tell When You're Telling Lies: Ethics and Embedded Confidential Information*, 30 J. LEGAL PROF. 79, 81 (2005-2006).

12. There may, however, be a situation where metadata is visible on the face of an electronic document without the receiving attorney making any effort to reveal the metadata. For example, if an attorney uses the “track changes” function to maintain a record of changes and deletions in a document and forgets to turn off “track changes” before sending the document, the receiving attorney will be able to see the changes and deletions made to the document when the attorney opens it.

13. For a discussion of the different types of metadata that are created by various word processing systems, see generally Hricik, *supra* note 11, at 79.

14. KENNEDY, *supra* note 8, at 7.

15. *Id.* at 7-8.

dates of the revisions.¹⁶ In law firms, where multiple versions of documents are created during the drafting process, it may be possible to find out the names of all persons who have accessed the document, viewed the document, made revisions, printed the document, and the dates of each access to the document.¹⁷

User-created metadata includes metadata that is created when functions included in Microsoft Word, or an equivalent word processing system, are used, such as track changes and comments.¹⁸ For example, an attorney can use the “track changes” function in Microsoft Word, either for personal use or for collaboration with other attorneys, when drafting a document. The track changes function allows a user to track or identify every change—additions, deletions, re-organizations—made to an electronic document.¹⁹ By using the track changes function, the user is creating metadata. If the attorney accepts all changes the attorney or another attorney makes to a document and turns off the track changes function, the changes made to the document are no longer visible. However, the metadata is still embedded in the document. The attorney who subsequently receives the document may be able to view the sending attorney’s changes, as well as the names of people who made the changes—the metadata—by turning the track changes function on again or using some other technological means to reveal the metadata.²⁰ Accordingly, if a receiving lawyer searches for metadata in an electronic document received from opposing counsel, the attorney may be able to reveal all revisions made to documents at different stages of the drafting process, which may reveal information protected by the attorney-client privilege or work product doctrine.²¹

Another example of user-created metadata is the use of comments. When attorneys are drafting and revising documents in a collaborative environment, attorneys frequently insert comments into the document. A comment is a note inserted into an electronic document about a particular part, paragraph, or sentence of the document. Word processing programs allow an attorney to either embed a comment into the document, which requires someone reading the document to hold the cursor over a certain spot to view the comment, or the attorney can insert comments into the document so that the comments appear on the margin of the document

16. N.Y. State Bar Ass’n Comm. on Prof’l Ethics, Op. 749 (2001).

17. Hricik, *supra* note 11, at 83.

18. KENNEDY, *supra* note 8, at 8.

19. *See id.* at 3.

20. Eileen B. Libby, *What Lurks Within: Hidden Metadata in Electronic Documents Can Win or Lose Your Case*, April 2007, http://www.abanet.org/cpr/about/Hidden_Metadata.html.

21. N.Y. State Bar Ass’n Comm. on Prof’l Ethics, Op. 749 (2001).

and are readily viewable by other attorneys.²² Similar to the track changes function, an attorney who receives a document and searches for metadata may be able to view comments inserted into the document by the sending attorney even though the sending attorney thought the comments were removed.²³

B. Inadvertent Disclosure of Confidential Metadata

For the most part, metadata is harmless and does not provide any helpful or hurtful information to anyone looking at the data, or reveal any confidential information.²⁴ This is particularly true with automatically-created metadata. Moreover, there are many instances where attorneys intentionally share electronic documents containing metadata with opposing counsel or other attorneys outside the law firm. For example, attorneys communicating back and forth over contract terms often use the track changes function so that each attorney working on the document can easily view, and either accept or reject, the proposed changes. Using the track changes function can save each attorney time because each is able to readily view the changes proposed instead of searching a potentially lengthy document for obscure changes. In this example, both attorneys are aware that metadata is being created and shared.

However, metadata is not always useless; to the contrary, it can be very helpful, especially during formal discovery in litigation. For example, metadata revealing the date and time a document was created may help determine “who said what when” or “who knew what when,” which can be critical to establishing a claim or defense.²⁵ In *Williams v.*

22. ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 06-442, at 1 (2006).

23. The use of templates is another example of user-created metadata. David Hricik & Robert R. Jueneman, *The Transmission and Receipt of Invisible Confidential Information*, 15 No. 1 PROF. LAW. 18, 4 (2004). A template is a document that is created for a particular purpose for a client and is saved in order to be used for future clients having similar needs. For example, a basic lease or simple will that has been saved as a template can be changed to meet the needs of many different clients. Lawyers also use templates as a starting point for drafting complaints, motions, discovery requests, and other documents. When templates are created and used for different clients, every change made and saved on the template is stored in the document's metadata. Therefore, for example, the metadata in a lease for a client drafted from a template may include information about a previous client for which the template was also used.

24. See The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production, at 5 (Jan. 2004) [hereinafter *Sedona Principles*] (noting that ordinarily “metadata will have no material evidentiary value”).

25. ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 06-442, at 2 (2006) (discussing the review and use of metadata); see also *Sedona Principles*, *supra* note 24, at 5 (“[I]t is easy to conceive of situations where metadata is necessary to

Sprint/United Management Company,²⁶ terminated employees sought Microsoft Excel spreadsheets in their original format, including all metadata, so they could view the formulae used in the spreadsheets.²⁷ The district court ultimately required the defendant to produce the spreadsheets in their original format, with all metadata intact, because of the importance of the metadata in supporting the plaintiffs' discrimination claims.²⁸

Not only can metadata be useful, it can also lead to the disclosure of information that the sending attorney did not intend to share.²⁹ The receiving attorney can use software to search for and reveal the metadata. The metadata may reveal information protected by the attorney-client privilege or work product doctrine, which may give a party an advantage in negotiations, contract drafting, and in other settings. For example, metadata hidden in a demand letter may reveal what a client was originally willing to accept as payment to settle a matter short of litigation, knowledge of which may give the receiving attorney an advantage in the negotiations. By searching for metadata, an attorney may be able to view comments embedded in the document, which may reveal insights from the client about particular contract terms. The searching attorney may be able to view revisions and comments made by attorneys, revealing mental thoughts and conclusions about a particular legal strategy, the viability of a claim or defense, a settlement range, or contract terms.³⁰

Unfortunately, there are many instances where the inadvertent disclosure of metadata has led to the release of confidential information.³¹ Recently in May 2008, lawyers representing the plaintiffs and defendants in a class action sex discrimination case against General Electric discovered that several documents filed with the court electronically could be downloaded and pasted into a Word Document. Even though the plaintiffs' lawyers redacted confidential information from the documents, the metadata was still embedded in the documents.

authenticate a document, or establish facts material to a dispute, such as when a file was accessed in a suit involving theft of trade secrets.”).

26. 230 F.R.D. 640 (D. Kan. 2005).

27. *Id.* at 643.

28. *Id.* at 651-52.

29. Metadata can be inadvertently transmitted in three situations. First, the sending attorney may be unaware of the existence of metadata in general or that the word processing system created metadata. Second, a lawyer may turn off the track changes function or delete comments but not realize that the metadata is still embedded in the document. Third, a lawyer can take precise steps and precautions to remove or “scrub” the document of its metadata, but may nevertheless be unsuccessful in removing all of the document's metadata.

30. N.Y. State Bar Ass'n Comm. on Prof'l Ethics, Op. 749 (2001).

31. See KENNEDY, *supra* note 8, at 3; Libby, *supra* note 20.

When the documents were copied and pasted into Microsoft Word, the previously deleted confidential information appeared.³² Another example of inadvertent disclosure is when a partner at former Florida Bar President Henry Coxe III's law firm electronically sent a brief to a lawyer at another firm who was working on a similar case.³³ The lawyer at the other firm was able to view all the changes that had been made to the brief, including communications between the partner and his client, which led to the disclosure of work product and confidential information.³⁴

Another important issue implicated with the inadvertent disclosure of metadata is whether the disclosure leads to the waiver of the attorney-client privilege or protection under the work product doctrine. The issue of waiver is outside the scope of the ethical dilemma this paper attempts to resolve. There are, however, differing approaches to resolving the issue of whether inadvertent disclosure of electronic information waives any protection,³⁵ and the enactment of new Federal Rule of Evidence 502 governing inadvertent disclosure and waiver will only increase the level of discussion about this important issue.³⁶

32. *Preserving Your Client's Confidential Information: Another Electronic Nightmare*, (McGuire Woods LLP, Richmond, VA), Jun. 5, 2008, <http://www.mcguirewoods.com/news-resources/item.asp?item=3337#page=1>.

33. Walker, *supra* note 2, at 1.

34. *Id.* Other notable examples of inadvertent disclosure of metadata include: in 2003, the SCO Group revealed legal strategy when it filed a complaint with tracked changes and comments; in 2004, the Pentagon de-classified a document because metadata was disclosed; in 2005, the Democratic National Committee revealed the name of the author of a memo about Judge Samuel Alito, the Chronicle of Higher Education revealed the names of anonymous peer-reviewers, and in a products liability suit, metadata revealed that Merck removed negative information from a drug study, which led to the filing of 7,000 personal injury lawsuits; and in 2006, the United Nations revealed the name of a person allegedly involved in a Lebanese assassination plan that had been deleted from a document. KENNEDY, *supra* note 8, at 3; Libby, *supra* note 20.

35. Generally, courts take three different approaches to analyze waiver in the context of inadvertent disclosure of electronic information. The majority approach uses a balancing test and considers up to five factors to determine whether waiver has occurred: (1) the reasonableness of the precautions taken to prevent inadvertent disclosure; (2) the number of inadvertent disclosures; (3) the extent of the disclosures; (4) any delay in measures taken to rectify the disclosure; and (5) overriding interests in justice. *See, e.g., Victor Stanley, Inc. v. Creative Pipe, Inc.*, 250 F.R.D. 251 (D.Md. 2008). The "strict" approach, followed only by the D.C. Circuit, holds that "the privilege is lost 'even if the disclosure is inadvertent.'" *In re Sealed Case*, 877 F.2d 976, 980 (C.A.D.C. 1989) (citation omitted). Finally, under the "lenient" or "subjective intent" approach, the court examines "the subjective intent of the holder of the privilege and the relevant surrounding circumstances for any manifestation of the holder's consent to disclose the information." *State Comp. Ins. Fund v. WPS, Inc.*, 70 Cal.App.4th 644, 652-53 (2 Dist. 1999); *see also Mendenhall v. Barber-Greene Co.*, 531 F.Supp. 951 (N.D.Ill.1982).

36. On September 19, 2008, President Bush signed into law S. 2450, a bill to amend the Federal Rules of Evidence to add new Rule 502. Federal Rule of Evidence 502 addresses the issue of inadvertent disclosure of privileged or protected information and

As attorneys are increasingly using and relying upon technology to communicate with their clients, collaborate with other attorneys, file documents electronically, and engage in electronic discovery, the risk that information protected by the attorney-client privilege or work product doctrine may be inadvertently revealed increases. The creation of metadata may be responsible for the increased risk of inadvertent disclosures. Attorneys who transmit documents electronically may, even after taking reasonable precautions, inadvertently or unknowingly transmit metadata containing privileged or protected information. When this happens, the receiving attorney may be able to view the privileged or protected metadata. Because of the risk of destruction of the attorney-client privilege and work-product protection, it is critical to resolve whether receiving attorneys should be ethically permitted to search for metadata.

III. THE FEDERAL RULES OF CIVIL PROCEDURE AND METADATA

A. *Rules Governing Metadata in Formal Discovery*

While this paper primarily addresses whether it is ethically permissible for a receiving attorney to search for metadata in electronic documents in a context other than formal discovery, it is necessary to briefly examine metadata in the context of formal discovery to determine whether the Federal Rules of Civil Procedure help resolve this ethical dilemma.

Before the revised Federal Rules of Civil Procedure went into effect in December 2006,³⁷ there was a presumption that the producing party had no obligation to either preserve or produce metadata unless the producing party knew that the metadata contained relevant information which was material to resolving the dispute in litigation.³⁸ Additionally,

the issue of waiver. Proposed Rule 502 provides protection from waiver of the attorney-client privilege and work product protection if the disclosure was inadvertent, the holder of the privilege or protection took reasonable steps to prevent the disclosure, and the holder promptly took reasonable steps to rectify the error. *See* FED. R. EVID. 502. The rule does not define “inadvertent” or “reasonable steps.” However, a letter written from the Advisory Committee on Evidence Rules to Senators Leahy and Specter defines inadvertent as “the result of an innocent mistake.” Letter from Lee H. Rosenthal, Chair Comm. on Rules of Practice and Procedure, to Hon. Patrick J. Leahy, Chairman Comm. on the Judiciary, U.S. Senate, and Hon. Arlen Specter, Member Comm. on the Judiciary, U.S. Senate (Sept. 26, 2007), *available at* http://www.uscourts.gov/rules/Hill_Letter_re_EV_502.pdf.

37. *See* FED. R. CIV. P. (2006).

38. Sedona Principles, *supra* note 24, at Principle 12, cmt. 12a (concluding that metadata should only be produced in an exceptional situation). *But see* Williams v. Sprint/United Mgmt. Co., 230 F.R.D. 640, 652 (D. Kan. 2005) (agreeing with Sedona

it was sufficient for parties to produce electronic documents as image files, such as .pdf or .tiff (tagged image file format),³⁹ so that the requesting party would only see data ordinarily visible from a printed piece of paper, not the hidden metadata.⁴⁰ Consequently, the risk of inadvertent disclosure of metadata containing privileged or protected information was nearly nonexistent.

The revised Federal Rules of Civil Procedure,⁴¹ however, changed these presumptions. The revised rules acknowledge that metadata can be relevant and discoverable during formal discovery.⁴² Rule 34(a) creates a new category of discoverable material, electronically stored information, which leaves no doubt that electronic documents, including hidden metadata, can be discoverable.⁴³ Rules 16(b) and 26(f) encourage parties to discuss the need for production of metadata during discovery early in the litigation.⁴⁴

Additionally, new Rule 34(b) allows the requesting party to specify the format in which the responding party should produce the electronic information.⁴⁵ Accordingly, the requesting party may ask the producing party to produce the electronic documents in their native format, i.e. the same format in which the document was originally created, which will contain all metadata. For example, a party that maintains its word processing documents in Microsoft Word and its spreadsheets in Microsoft Excel format will be required to produce those documents in

Principles that “emerging standards of electronic discovery appear to articulate a general presumption against the production of metadata,” but also holding that “when a party is ordered to produce electronic documents as they are maintained in the ordinary course of business, the producing party should produce the electronic documents with their metadata in tact”).

39. Sedona Principles, *supra* note 24, at Principle 12, cmt. 12a; *id.* at Principle 12, cmt. 12c.

40. KENNEDY, *supra* note 8, at 6 (explaining that production in native format allows the person viewing the information to “see formulas used in cells and other information not available from a paper printout or TIFF or PDF versions of the same spreadsheet”).

41. See FED. R. CIV. P. (2006).

42. KENNEDY, *supra* note 8, at 1.

43. FED. R. CIV. P. 34(a)(1)(A) (allowing a party to serve on another party a request to produce “electronically stored Information . . . stored in any medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form”).

44. See FED. R. CIV. P. 16(b) (listing the discovery of electronically stored information as a matter that may be addressed in the scheduling order); see also *id.* 26(f)(2) (requiring parties to discuss the need for preservation of electronically stored information and any issues with the format of production of electronically stored information in the initial meet and confer conference); Jo Maitland, *Judges Speak Candidly on New E-Discovery Rules*, STORAGE, Jan. 31, 2007, http://searchstorage.techtarget.com/news/article/0,289142,sid5_gci1241499,00.html.

45. FED. R. CIV. P. 34(b)(1)(C) (allowing the requesting party to “specify the form or forms in which electronically stored information is to be produced”).

their original formats, .doc and .xls, instead of producing the documents in .pdf or .tiff. By requesting electronic documents in their native formats, the requesting party is essentially asking for the original document, in its original format, with all metadata intact. Upon review of the electronic document, the requesting party will be able to view information hidden in the Microsoft Word documents and in cells in the Microsoft Excel documents, as well as other information not otherwise viewable if the responding party had produced the document in a printed or image format.⁴⁶

Under the revised Federal Rules, a party's duty to preserve relevant information now requires the party to take reasonable measures to preserve metadata associated with electronic documents.⁴⁷ Accordingly, scrubbing documents of their metadata during litigation may result in the destruction of relevant, discoverable metadata, and may subject the attorney and client to sanctions from the court and may subject the attorney to disciplinary action from the State Bar.⁴⁸

The revised Rules do not specifically address whether the requesting party may or may not search for the metadata. However, because the rules clarify that electronically stored information, including metadata, is discoverable, the presumption is that the receiving party should be able to comb through the metadata to find information to support claims or defenses.⁴⁹ Moreover, ethics committees that have addressed the issue of whether a receiving attorney can mine for metadata in electronic documents acknowledge that any prohibition in mining for metadata would not apply during electronic discovery because of the potential relevance of the metadata.⁵⁰

46. See KENNEDY, *supra* note 8, at 7.

47. See FED. R. CIV. P. 16(b), 26(f), 34(a)-(b); Libby, *supra* note 20.

48. See MODEL RULES OF PROF'L CONDUCT R. 3.4 (2008) (prohibiting attorneys from "unlawfully obstruct[ing] another party's access to evidence or unlawfully alter[ing], destroy[ing] or conceal[ing] a document or other material having potential evidentiary value").

49. D.C. Bar Ass'n, Ethics Op. 341, at 3 (2007) (noting that the receiving attorney has the duty to competently and diligently review, use, and preserve the evidence to represent her client's interests, and that the receiving attorney may consult with a computer expert to fully reveal and review metadata).

50. See Ala. Off. of Gen. Couns., Op. RO-2007-02 (2007) (discussing the disclosure and mining of metadata); ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 06-442, at 5 n. 13 (2006) (noting that by scrubbing, an attorney may violate Model Rules of Prof'l Conduct R. 3.4 (2008), which forbids lawyers from unlawfully destroying documents having evidentiary value); D.C. Bar Ass'n, Ethics Op. 341 (2007) (discussing the same).

B. The Rules Do Not Resolve the Ethical Dilemma

Although the revised Federal Rules of Civil Procedure do not specifically address whether a receiving attorney may search for metadata in electronic documents or whether the inadvertent disclosure of metadata results in a waiver of a privilege or protection,⁵¹ Rule 26(b)(5)(B) sets up a “claw-back” mechanism for a producing party to assert a claim of privilege or protection after the party has produced documents in discovery.⁵² Specifically, the producing party must notify the requesting party and assert a claim that the information produced is subject to a privilege or to protection under the work product doctrine.⁵³ Once the producing party makes the claim, a duty on the requesting party is triggered.⁵⁴ The requesting party must return, destroy or sequester the information, and may not use the information, until the court resolves the claim.⁵⁵ Accordingly, if a sending attorney realizes that privileged or protected metadata was inadvertently produced during discovery, the attorney must notify the receiving attorney and make the claim in order to trigger the duties imposed on the receiving attorney. If the sending attorney does not notify, the receiving attorney’s duties under the Federal Rules are not triggered.

A critical issue is whether Rule 26(b)(5)(B) provides sufficient protection to the sending party. Rule 26(b)(5)(B) only triggers a duty on an attorney who receives privileged or protected metadata if the sending attorney notifies the receiving attorney and makes a claim of privilege or protection.⁵⁶ The rule by itself is problematic because in the absence of notice by the sending attorney, the receiving attorney has free reign not only to search for, but also to use, privileged or protected metadata that was inadvertently disclosed. The rule places all of the responsibility on the sending attorney, regardless of how much care the sending attorney takes to protect the information from disclosure. The rule also provides no encouragement to the receiving attorney to notify the sending attorney upon discovering that the sending attorney unintentionally produced privileged or protected metadata. Finally, the rule, standing alone, does not protect the sending party who never realizes that privileged or protected metadata was inadvertently produced.

51. FED. R. CIV. P. 26(b)(5)(B) (specifically noting that the rule does not address the substantive issue of waiver).

52. *Id.*

53. *Id.*

54. *Id.*

55. *Id.*

56. *Id.*

Even though a duty is not triggered on the receiving attorney under Rule 26(b)(5)(B) until the sending attorney gives notice, depending on the jurisdiction, the receiving attorney may have an ethical duty to notify the sending attorney even in the absence of any notice by the sending attorney. ABA Model Rule of Professional Conduct 4.4(b) states that “[a] lawyer who receives a document . . . and knows or reasonably should know that that the document was inadvertently sent shall promptly notify the sender.”⁵⁷ Model Rule 4.4(b) appears to fill in the gap left by Rule 26(b)(5)(B) by requiring the receiving attorney to notify the sending attorney, even in the absence of any notification by the sending party. Not all jurisdictions, however, have a rule identical to Model Rule 4.4(b). For example, in Maryland, the receiving party has no duty to notify the sending party at any time after learning that privileged or protected metadata was inadvertently produced.⁵⁸ Under Rule 26(b)(5)(B) as it is currently written, and in jurisdictions with no ethics rule similar to Model Rule 4.4(b), if a sending party never realizes that privileged or protected information was inadvertently disclosed, the receiving attorney has free reign to search and use the information and is not required to notify the sending attorney. It is questionable whether Rule 26(b)(5)(B) provides sufficient protection for the sending attorney.

While the revised Federal Rules of Civil Procedure give some guidance to attorneys about how to handle metadata in formal discovery, the rules give no guidance to attorneys handling litigation but not engaged in formal discovery, or to attorneys engaging in transactional practices.⁵⁹ If litigation has commenced, but the parties are not engaging in formal discovery or formal discovery has ended, it is unclear whether the receiving attorney is permitted to search through the electronic documents to find metadata. If an attorney electronically sends opposing counsel a draft settlement agreement, can the receiving attorney intentionally activate the track changes function or use other means to discover revisions to the agreement in the hopes of revealing information, such as an initial settlement figure, that may help in the settlement negotiations? In a transactional context, if an attorney sends opposing counsel a draft contract, can the receiving attorney intentionally search for metadata in the document to reveal revisions the sending party

57. MODEL RULES OF PROF'L CONDUCT R. 4.4(b) (2008).

58. Md. St. Bar Ass'n Comm. on Ethics, Docket No. 2007-09 (2007).

59. Federal Rule of Civil Procedure 26 governs discovery in general, and Rule 26(b)(5)(B) applies specifically to a claim asserted during the production of documents in formal discovery. *See* FED. R. CIV. P. 26 (titled “Duty to Disclose; General Provisions Regarding Discovery”); *see also id.* 26(b) (titled “Discovery Scope and Limits”); *id.* 26(b)(5) (titled “Claiming Privilege or Protecting Trial Preparation Material”); *id.* 26(b)(5) (titled “Information Produced” and limiting the scope of the duties imposed to instances where information is produced in discovery).

made to the contract in the hopes of improving her posture in negotiation? These are the ethical questions left unresolved by the Federal Rules that this paper attempts to resolve.

IV. ETHICS RULES IMPLICATED IN THE SENDING AND RECEIVING OF METADATA

The principle rules implicated for the attorney sending electronic documents are the duties of confidentiality, competence, and communication. Unless an exception applies, lawyers have a duty not to reveal information related to the client's representation.⁶⁰ Lawyers also have a duty to provide competent representation to a client, which "requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."⁶¹ The duties of confidentiality and competence together require attorneys to be educated about the sending of metadata, to take reasonable precautions to preserve the confidentiality of information contained in metadata, and "to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure."⁶² Finally, a lawyer has the duty to communicate with the client about the means to accomplish the client's objectives, and to explain matters to the client to help the client make informed decisions about the representation.⁶³ In the context of sending metadata, the duty of communication may require the sending attorney to communicate with the client about metadata in general, and more specifically, the use and cost of software to scrub metadata.

There are also numerous ethics rules that are implicated in the receiving of electronic documents and metadata. First, a lawyer's duty of diligence is implicated. Lawyers must "act with reasonable diligence and promptness in representing a client."⁶⁴ The attorney must be committed and dedicated to the client's interests and must represent those interests with zeal.⁶⁵ Additionally, in jurisdictions that permit the searching of metadata, a receiving lawyer's duty of communication may require attorneys to communicate with the client about the need to purchase and use software that will enable the attorney to effectively search for metadata. A lawyer also has a duty to respect the rights of third persons.⁶⁶ Model Rule of Professional Conduct 4.4(b) imposes a duty on a lawyer who receives a document and knows or should know

60. MODEL RULES OF PROF'L CONDUCT R. 1.6 (2008).

61. *See id.* R. 1.1.

62. *See id.* R. 1.6 cmt. 16 (2008).

63. *See id.* R. 1.4(a)(2); *id.* R. 1.4(b).

64. *See id.* R. 1.3.

65. *See id.* R. 1.3 cmt. 1.

66. *See id.* R. 4.4.

that it was inadvertently sent to notify the sending attorney.⁶⁷ Finally, if a lawyer engages in conduct involving dishonesty or deceit, or engages in conduct prejudicial to the administration of justice, the lawyer is engaging in professional misconduct and may be subject to discipline.⁶⁸

When analyzing the ethical rules to resolve the ethical dilemma presented, questions to consider include: Does a lawyer who inadvertently discloses metadata containing confidential information violate the duty of confidentiality? Does a lawyer's duty of diligence require the receiving attorney to search for the metadata, and if the lawyer does not search for it, is the lawyer violating a duty by not diligently advancing the client's interests? Does a lawyer who intentionally searches metadata received violate a duty of confidentiality? Does the concern for confidentiality outweigh a lawyer's ethical obligation to represent her client with diligence or vice versa? Is it dishonest or deceitful misconduct for a lawyer to search for metadata? Is searching for metadata considered conduct that is prejudicial to the administration of justice?

V. SEARCHING FOR METADATA OUTSIDE OF FORMAL DISCOVERY

The ethics committees from various jurisdictions agree that the sending attorney has a duty to take reasonable steps to preserve confidential information contained in metadata.⁶⁹ The committees, however, reach different conclusions about whether a receiving party is ethically permitted to search for metadata outside of formal discovery. Most jurisdictions outright ban the practice of looking for metadata,⁷⁰ some allow the active searching of metadata,⁷¹ one jurisdiction allows an

67. *Id.* R. 4.4(b). As discussed *infra*, however, not all jurisdictions have an ethical rule similar to Model Rules of Prof'l Conduct R. 4.4(b).

68. *Id.* R. 8.4(c), (d).

69. See N.Y. State Bar Ass'n Comm. on Prof'l Ethics, Op. 782 (2004); Prof'l Ethics of the Fla. Bar, Op. 06-2 (2006); Ala. Office of Gen. Couns., Op. RO-2007-02 (2007); State Bar of Ariz. Comm. on the Rules of Prof'l Conduct, Op. 07-03 (2007); N.Y. County Law. Ass'n Comm. on Prof'l Ethics, Op. 738 (2008); ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 06-442 (2006); Md. State Bar Ass'n Comm. on Ethics, Docket No. 2007-09 (2007); D.C. Bar Ass'n, Ethics Op. 341 (2007); Me. Prof'l Ethics Comm. of the Bd. of Overseers of the Bar, Op. 196, at 4 (2008).

70. See N.Y. State Bar Ass'n Comm. on Prof'l Ethics, Op. 749 (2001); N.Y. State Bar Ass'n Comm. on Prof'l Ethics, Op. 782 (2004); Prof'l Ethics of the Fla. Bar, Op. 06-2 (2006); Ala. Office of Gen. Couns., Op. RO-2007-02 (2007); State Bar of Ariz. Comm. on the Rules of Prof'l Conduct, Op. 07-03 (2007); N.Y. County Law. Ass'n Comm. on Prof'l Ethics, Op. 738 (2008); Me. Prof'l Ethics Comm. of the Bd. of Overseers of the Bar, Op. 196, at 3 (2008).

71. See ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 05-437 (2005); ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 06-442 (2006); Md. St. Bar Ass'n Comm. on Ethics, Docket No. 2007-09 (2007); Colo. Bar Ass'n Ethics Comm., Op. 119 (2008).

attorney to search for metadata unless the attorney has actual knowledge that the metadata was inadvertently produced,⁷² and finally, one state, Pennsylvania, leaves the decision of whether to search or not up to the attorney.⁷³

A. *Duties of the Sending Attorney: A Near-Unified Approach*

Under all circumstances, the sending attorney has a fundamental duty to preserve client confidentiality, and must always take reasonable precautions to avoid disclosing confidential information contained in metadata.⁷⁴ The sending attorney's responsibility to take reasonable precautions to avoid disclosure of confidential information in metadata arises primarily from the ethical duties of confidentiality and competence.⁷⁵

The ethics committees agree that the sending attorney must take reasonable precautions to prevent disclosure of confidential information in metadata, but the committees interpret "reasonable" differently.⁷⁶ A few committees conclude that reasonable steps necessary to prevent disclosure simply depends on the circumstances.⁷⁷ Relevant considerations include the subject matter of the document,⁷⁸ the

72. See D.C. Bar Ass'n, Ethics Op. 341 (2007).

73. See Pa. Bar Ass'n Comm. on Legal Ethics and Prof'l Responsibility, Formal Op. 2007-500 (2007).

74. See N.Y. State Bar Ass'n Comm. on Prof'l Ethics, Op. 782 (2004); Prof'l Ethics of the Fla. Bar, Op. 06-2 (2006); Ala. Office of Gen. Couns., Op. RO-2007-02 (2007); State Bar of Ariz. Comm. on the Rules of Prof'l Conduct, Op. 07-03 (2007); N.Y. County Law. Ass'n Comm. on Prof'l Ethics, Op. 738 (2008); ABA Comm. On Ethics and Prof'l Responsibility, Formal Op. 06-442 (2006); Md. State Bar Ass'n Comm. on Ethics, Docket No. 2007-09 (2007); D.C. Bar Ass'n, Ethics Op. 341 (2007); Me. Prof'l Ethics Comm. of the Bd. Of Overseers of the Bar, Op. 196, at 4 (2008).

75. Ala. Office of Gen. Couns., Op. RO-2007-02, at 3 (2007); Prof'l Ethics of the Fla. Bar, Op. 06-2, at 2 (2006); State Bar of Ariz. Comm. on the Rules of Prof'l Conduct, Op. 07-03, at 2 (2007); Md. State Bar Ass'n Comm. on Ethics, Docket No. 2007-09, at 3 (2007); Colo. Bar Ass'n Ethics Comm., Op. 119, at 2 (2008) ("The duty to provide competent representation requires [a 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.").

76. The ethics committees have noted that the inadvertent disclosure of confidential information in metadata may violate the duty of confidentiality, but none have actually found a violation. See Md. State Bar Ass'n Comm. on Ethics, Docket No. 2007-09, at 3 (2007) (noting that not every inadvertent disclosure of privileged or work product material violates the duties of competence and confidentiality).

77. N.Y. State Bar Ass'n Comm. on Prof'l Ethics, Op. 782, at 2 (2004); Ala. Office of Gen. Couns., Op. RO-2007-02, at 3 (2007); State Bar of Ariz. Comm. on the Rules of Prof'l Conduct, Op. 07-03, at 2 (2007); Colo. Bar Ass'n Ethics Comm., Op. 119, at 2 (2008).

78. N.Y. State Bar Ass'n Comm. on Prof'l Ethics, Op. 782, at 2 (2004); Ala. Office of Gen. Couns., Op. RO-2007-02, at 3 (2007).

sensitivity of the information being transmitted,⁷⁹ whether the document is a template,⁸⁰ whether there have been multiple drafts of a document,⁸¹ whether the client has commented in the document,⁸² the identity of the recipients,⁸³ steps taken by attorney to prevent disclosure,⁸⁴ the nature and scope of metadata revealed,⁸⁵ the potential consequences of inadvertent disclosure,⁸⁶ and whether the client has given any special instructions regarding the metadata or transmission of the electronic document.⁸⁷

There is disagreement among the ethics committees as to whether a sending attorney is required to scrub documents of their metadata in order to preserve the confidentiality of information in electronic documents. Only a few jurisdictions require the sending attorney to scrub metadata before sending the document to opposing counsel,⁸⁸ while others have refused to impose an absolute duty to scrub.⁸⁹

Some jurisdictions recommend that attorneys refrain from creating metadata in the first place.⁹⁰ For example, Arizona instructs a lawyer who is asked to make a comment in a draft circulating in the office and who knows that the document will be sent to opposing counsel to think twice about inserting a comment in the draft.⁹¹ Arizona also recommends lawyers drafting pleadings, contracts, and other documents to use a “clean” form and not a document that was used for another client.⁹² The American Bar Association and Colorado Bar Association Ethics Committee recommend that lawyers refrain from using the track

79. State Bar of Ariz. Comm. on the Rules of Prof'l Conduct, Op. 07-03, at 2 (2007).

80. N.Y. State Bar Ass'n Comm. on Prof'l Ethics, Op. 782, at 2 (2004).

81. *Id.*

82. *Id.*

83. *Id.*; Ala. Office of Gen. Couns., Op. RO-2007-02, at 3 (2007).

84. Ala. Office of Gen. Couns., Op. RO-2007-02, at 3 (2007).

85. *Id.*

86. State Bar of Ariz. Comm. on the Rules of Prof'l Conduct, Op. 07-03, at 2 (2007).

87. *Id.*

88. *See* N.Y. County Law. Ass'n Comm. on Prof'l Ethics, Op. 738, at 1 (2008); ABA Comm. On Ethics and Prof'l Responsibility, Formal Op. 06-442, at 1 (2006); D.C. Bar Ass'n, Ethics Op. 341, at 1 (2007); Colo. Bar Ass'n Ethics Comm., Op. 119, at 2 (2008) (holding that the sending lawyer has an ethical duty to reduce the likelihood that metadata containing confidential information would be disclosed in an electronic document, which may require scrubbing files of their metadata).

89. *See* N.Y. State Bar Ass'n Comm. on Prof'l Ethics, Op. 782, at 3 n.3 (2004) (noting there is no absolute duty to scrub unless the attorney either knows that the metadata contains confidential information or knows that the receiving attorney is technologically savvy or is aggressive in mining for metadata).

90. *See* State Bar of Ariz. Comm. on the Rules of Prof'l Conduct, Op. 07-03, at 2 (2007); ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 06-442, at 2 (2006); Colo. Bar Ass'n Ethics Comm., Op. 119, at 2 (2008).

91. State Bar of Ariz. Comm. on the Rules of Prof'l Conduct, Op. 07-03, at 2 (2007).

92. *Id.*

changes function in word processing documents and from embedding comments in documents,⁹³ and advise attorneys to send documents by fax, hand delivery, or in an image format.⁹⁴

While there is no doubt that a sending attorney should take all reasonable steps to protect sensitive information, the ultimate question is whether an attorney receiving an electronic document should be ethically permitted to intentionally search for metadata, knowing that the metadata may contain inadvertently disclosed, privileged information.

B. Duties of the Receiving Attorney: Competing Approaches

1. Attorney May Not Ethically Search for Metadata—New York, Florida, Arizona, Alabama, Maine

The principle argument advanced in support of a rule forbidding a receiving attorney from searching for metadata in electronic documents is that the searching constitutes an impermissible intrusion into the attorney-client relationship between the sending attorney and her client.⁹⁵

The Ethics Committees concluding that a receiving attorney may not search reason that the attorney-client relationship is the most important obligation of an attorney, on which the proper function of the legal system relies.⁹⁶ Moreover, the protection of the fiduciary relationship between attorney and client is a “fundamental tenet of the legal profession.”⁹⁷ The duty of confidentiality, therefore, not only forms

93. ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 06-442, at 2 (2006); Colo. Bar Ass'n Ethics Comm., Op. 119, at 2 (2008).

94. ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 06-442, at 2 (2006); Colo. Bar Ass'n Ethics Comm., Op. 119, at 2 (2008).

95. See N.Y. State Bar Ass'n Comm. on Prof'l Ethics, Op. 749, at 2 (2001); Ala. Office of Gen. Counsel., Op. RO-2007-02, at 3 (2007); State Bar of Ariz. Comm. on the Rules of Prof'l Conduct, Op. 07-03, at 2 (2007).

96. N.Y. State Bar Ass'n Comm. on Prof'l Ethics, Op. 749, at 2 (2001). The New York State Bar Association's Committee on Professional Ethics was the first ethics committee to decide that the receiving attorney is not ethically permitted to search for metadata. The question New York addressed was whether an attorney may ethically “use available technology to surreptitiously examine and trace e-mail and other electronic documents.” *Id.* at 2 (noting that modern technology allows lawyers to “get behind” the visible document and “bug” an email sent to opposing counsel in order to learn the identity of anyone who subsequently receives the email and the comments they make). New York analogized the searching of metadata in electronic documents to other impermissible, but less technologically involved, intrusions into the attorney-client relationship, including soliciting the unauthorized disclosure of communications and exploiting the will of others to undermine client confidentiality. *Id.* at 2-3.

97. Ala. Office of Gen. Counsel, Op. RO-2007-02, at 3-4 (2007); see also State Bar of Ariz. Comm. on the Rules of Prof'l Conduct, Op. 07-03, at 2 (2007) (holding that it is impermissible for the receiving attorney to search for metadata because of the

the basis for the sending attorney's duty to protect against disclosing confidential information in metadata, but also forms the basis for the receiving attorney's duty to refrain from searching.⁹⁸

Ethics Committees also cite their versions of Model Rules of Professional Conduct 8.4(c) and (d) which forbid attorneys from engaging in dishonest or deceitful conduct, or conduct prejudicial to the administration of justice.⁹⁹ When an attorney searches for metadata, the attorney is intentionally attempting to learn information protected by the attorney-client privilege and work product doctrine in order to gain an unfair advantage over the sending attorney.¹⁰⁰ By actively searching for confidential information in metadata, the receiving attorney "crosses the line" from upholding a duty of diligent representation to engaging in conduct that is dishonest, deceitful, and prejudicial to the administration of justice.¹⁰¹

2. Attorney May Ethically Search for Metadata—American Bar Association, Maryland, and Colorado

The American Bar Association, Maryland, and Colorado take the position that a receiving party may ethically search for and review metadata contained in electronic documents.¹⁰²

On the general issue of the inadvertent transmission of information, the ABA initially took a position that required more of receiving attorneys than its position requires today. In 1992, the ABA held that a lawyer who receives a document that appears to contain confidential

fundamental principle of maintaining the sanctity of the attorney-client relationship); Me. Prof'l Ethics Comm. of the Bd. of Overseers of the Bar, Op. 196, at 3 (2008).

98. See Me. Prof'l Ethics Comm. of the Bd. of Overseers of the Bar, Op. 196, at 3 (2008) (noting that attorneys share responsibility for protecting the attorney-client privilege).

99. N.Y. State Bar Ass'n Comm. on Prof'l Ethics, Op. 749, at 3 (2001); see also MODEL RULES OF PROF'L CONDUCT R. 8.4(c)(2008); MODEL RULES OF PROF'L CONDUCT R. 8.4(d) (2008); Me. Prof'l Ethics Comm. of the Bd. of Overseers of the Bar, Op. 196, at 3 (2008).

100. Ala. Office of Gen. Counsel, Op. RO-2007-02, at 4 (2007); N.Y. County Law Ass'n Comm. on Prof'l Ethics, Op. 738, at 3 (2008).

101. N.Y. State Bar Ass'n Comm. on Prof'l Ethics, Op. 749, at 3 (2001); N.Y. County Law Ass'n Comm. on Prof'l Ethics, Op. 738, at 3 (2008); Me. Prof'l Ethics Comm. of the Bd. of Overseers of the Bar, Op. 196, at 3 (2008) (attorney "who purposefully seeks to unearth confidential information embedded in metadata attached to a document . . . when the attorney knows or should know that the informed involved was not intended to be disclosed, has acted outside" the ethical duties to refrain from conduct that is dishonest and prejudicial to the administration of justice).

102. ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 05-437 (2005); ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 06-442 (2006); Md. State Bar Ass'n Comm. on Ethics, Docket No. 2007-09 (2007); Colo. Bar Ass'n Ethics Comm., Op. 119 (2008).

information—under circumstances where the document was not intended for the receiving lawyer—has a duty to refrain from examining the document, to notify the sending attorney, and to abide by the sending attorney’s instructions.¹⁰³ Subsequently, in February 2002, the ABA amended Rule 4.4 to add section (b), which states that “[a] lawyer who receives a document relating to the representation of the lawyer’s client and knows or reasonably should know that the document was inadvertently sent shall promptly notify the sender.”¹⁰⁴ After the addition of Rule 4.4(b), the ABA withdrew its original position and in October 2005, held that a “lawyer who receives a document from opposing parties or their lawyers and knows or reasonably should know that the document was inadvertently sent should promptly notify the sender in order to permit the sender to take protective measures.”¹⁰⁵

According to the ABA, Rule 4.4(b) narrowed the scope of the receiving attorney’s duties from requiring the receiving attorney to refrain from examining the document, notify the sender, and abide by the sender’s instructions to only requiring the receiving attorney to notify the sender.¹⁰⁶ The ABA noted that under Model Rule 4.4(b), the receiving attorney’s decision of whether to return the original document unread to the sender is a matter of professional judgment, not an ethical obligation.¹⁰⁷

In 2006, the ABA applied this narrow obligation to the context of the review and use of metadata in electronic documents, holding that the Model Rules of Professional Conduct permit a receiving lawyer “to review and use embedded information contained in e-mail and other electronic documents.”¹⁰⁸ Rejecting the idea that a receiving lawyer’s review and use of metadata was dishonest, the ABA held that a receiving attorney may ethically review and use metadata because there are no ethical rules expressly prohibiting the conduct, and the only affirmative

103. ABA Comm. on Ethics and Prof’l Responsibility, Formal Op. 05-437 (2005). (“Inadvertent Disclosure of Confidential Materials: Withdrawal of Formal Opinion 92-638” (November 10, 1992)).

104. MODEL RULES OF PROF’L CONDUCT R. 4.4(b) (2008).

105. ABA Comm. on Ethics and Prof’l Responsibility, Formal Op. 05-437, at 1 (2005).

106. *Id.*

107. *Id.* at 2 (citing cmt. 3 to R. 4.4). Comment [3] to Rule 4.4 provides:

Some lawyers may choose to return a document unread, for example, when the lawyer learns before receiving the document that it was inadvertently sent to the wrong address. Where a lawyer is not required by applicable law to do so, the decision to voluntarily return such a document is a matter of professional judgment ordinarily reserved to the lawyer.

MODEL RULES OF PROF’L CONDUCT R. 4.4 cmt. 3 (2008).

108. ABA Comm. on Ethics and Prof’l Responsibility, Formal Op. 06-442, at 1 (2006).

obligation of the receiving attorney is to notify the sending attorney.¹⁰⁹ The ABA's position allowing receiving attorneys to review and use metadata places the entire burden of protecting against disclosure of confidential information on the sending attorney, and recommends that sending attorneys scrub metadata from electronic documents, avoid creating metadata in the first place, and refrain from sending documents electronically.¹¹⁰ Despite placing the entire burden on the sending attorney, the ABA recognizes that "more thorough or extraordinary investigative measures sometimes might permit the retrieval of embedded information that the provider of electronic documents either did not know existed, or thought was deleted."¹¹¹

Maryland follows the ABA approach and allows receiving attorneys to review and to use metadata.¹¹² Unlike the Model Rules of Professional Conduct, Maryland's ethics rules were never amended to add Rule 4.4(b). Accordingly, Maryland does not even impose an obligation on the receiving attorney to notify the sending attorney upon learning that privileged or work product material was inadvertently sent. Maryland merely advises the receiving attorney to discuss with her client the pros and cons of notifying the sending attorney in particular circumstances.¹¹³

Recently, the Ethics Committee of the Colorado Bar Association joined the ABA and Maryland in holding that a receiving attorney may ethically review metadata.¹¹⁴ Colorado emphasized that "the ultimate responsibility for control of metadata rests with the Sending Lawyer,"¹¹⁵ and concluded that a receiving attorney may search for metadata in electronic documents.¹¹⁶ First, Colorado reasoned that searching for metadata is not inherently deceitful or surreptitious.¹¹⁷ Second, a rule banning receiving attorneys from reviewing metadata in electronic documents incorrectly assumes that the metadata, when searched, will reveal confidential information.¹¹⁸ Finally, it reasoned that metadata is for the most part insignificant.¹¹⁹ The Colorado Ethics Committee, like the ABA, noted that there is no rule in the Colorado Rules of

109. *Id.* at 4 (noting that the addition of Rule 4.4(b) evidenced an intent to place the sole obligation of notice on the receiving attorney).

110. *Id.* at 4-5.

111. *Id.* at 2.

112. Md. State Bar Ass'n Comm. on Ethics, Docket No. 2007-09 (2007).

113. *Id.*

114. The Colorado Ethics Committee wrote an opinion on the metadata issue because of the split among jurisdictions. Colo. Bar Ass'n Ethics Comm., Op. 119, at 2 (2008).

115. *Id.* at 3.

116. *Id.*

117. *Id.*

118. Colo. Bar Ass'n Ethics Comm., Op. 119, at 3 (2008).

119. *Id.*

Professional Conduct that prohibits receiving attorneys from searching for metadata.¹²⁰

In addition to the issue of whether a receiving attorney may search for metadata in the first place, Colorado analyzed the separate issue of what the receiving lawyer must do upon receiving metadata that appears to contain confidential information.¹²¹ Colorado first held that it is reasonable for the receiving party to assume that metadata containing confidential information was sent inadvertently by the sending attorney.¹²² Based on this assumption, and following Colorado Rule of Professional Conduct 4.4(b),¹²³ if an attorney receives metadata that appears to contain confidential information, the receiving lawyer must notify the sender.¹²⁴ Because Rule 4.4(b) only requires the receiving party to notify the sending party, the receiving party is free to continue reviewing metadata, even though it appears to contain confidential information.¹²⁵ Colorado takes the position that continuing to review the metadata under this circumstance would not amount to professional misconduct, and held that the specific Rule 4.4(b) trumps the more general misconduct Rule 8.4(c).¹²⁶

Colorado's approach, however, does differ from the ABA approach in one respect. Unlike the Model Rules of Professional Conduct, the Colorado Rules of Professional Conduct include Rule 4.4(c), which states:

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.¹²⁷

Accordingly, if the sending attorney notifies the receiving attorney that the document was inadvertently sent before the receiving attorney

120. *Id.*

121. *Id.*

122. Colo. Bar Ass'n Ethics Comm., Op. 119, at 3 (2008). If a sending attorney complies with her ethical obligations and acts competently to guard confidential information, then the sending attorney would not intentionally send metadata containing confidential information, and therefore, it is reasonable to assume that it was sent inadvertently. *Id.*

123. COLO. RULES OF PROF'L CONDUCT 4.4(b) is identical to MODEL RULES OF PROF'L CONDUCT R. 4.4(b).

124. Colo. Bar Ass'n Ethics Comm., Op. 119, at 4 (2008).

125. *Id.*

126. *Id.*

127. COLO. RULES OF PROF'L CONDUCT 4.4(c) (2008).

reviews the document, Colorado's Rule 4.4(c) requires the receiving party to refrain from reviewing the document.¹²⁸

3. A Middle Ground—The District of Columbia

The District of Columbia attempts to reach a middle ground on the issue of whether a receiving attorney may ethically search for metadata in electronic documents. Under the District of Columbia's approach, a receiving attorney may ethically search and use metadata unless she has actual knowledge that the metadata was inadvertently sent.¹²⁹ A receiving attorney will have actual knowledge that metadata was inadvertently sent under two circumstances: 1) where the attorney is told by the sending attorney before review that the metadata was inadvertently sent; or 2) where the attorney immediately notices upon review of the metadata that protected information was inadvertently sent.¹³⁰ An example of when an attorney immediately notices that protected information was inadvertently sent is where the metadata reveals a conversation between an attorney and client, such that it is readily apparent on its face that it is protected information. In this situation, the receiving attorney has actual knowledge because it is clear that the sending attorney inadvertently sent the information.¹³¹

If the receiving attorney has actual knowledge under either of the above circumstances, the District of Columbia considers it a dishonest act under Rule 8.4(c) for the lawyer to review the metadata and use it.¹³² When the receiving attorney has actual knowledge, the receiving attorney's duty of honesty requires her to refrain from reviewing the metadata, regardless of whether the sending attorney simply made a mistake, was negligent, or breached an ethical obligation.¹³³

The District of Columbia's Rule 4.4(b) differs from MRPC 4.4(b) and the Colorado Rules of Professional Conduct in that it imposes an obligation on the receiving attorney to refrain from examining the metadata in addition to notifying the sending attorney.¹³⁴ Accordingly,

128. Colo. Bar Ass'n Ethics Comm., Op. 119, at 4 (2008).

129. D.C. Bar Ass'n, Ethics Op. 341, at 1 (2007).

130. *Id.* at 2.

131. *Id.*

132. *Id.* at 1-2 (agreeing with New York and Alabama that Rule 8.4(c) is implicated when a receiving attorney wrongfully searches metadata).

133. *Id.* at 2-3.

134. D.C. RULES OF PROF'L CONDUCT 4.4(b) provides:

A lawyer who receives a writing relating to the representation of a client and knows, before examining the writing, that it has been inadvertently sent, shall not examine the writing, but shall notify the sending party and abide by the instructions of the sending party regarding the return or destruction of the writing.

while the ABA and Colorado permit receiving attorneys to continue to review metadata in the situation where the receiving attorney immediately notices upon review of the metadata that protected information was inadvertently sent, the District of Columbia, based on its version of Rule 4.4(b) and Rule 8.4(c),¹³⁵ forbids the receiving attorney from continuing to review the metadata.

However, where it is not clear that metadata contains protected information, and consequently the receiving attorney does not definitively have actual knowledge that metadata was inadvertently sent, the receiving attorney may continue to review the metadata.¹³⁶ “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.”¹³⁷ Taking it one step further, the District of Columbia concludes that, where the privileged nature of the material cannot be determined on its face, the receiving attorney’s duty of diligent representation under Rule 1.3 “may trump confidentiality concerns,” and would permit the attorney to continue reviewing the metadata.¹³⁸ The District of Columbia is the only jurisdiction to hold that the duty of diligent representation can trump confidentiality in this context.

4. Let the Lawyers Decide—Pennsylvania

Whereas all jurisdictions that have addressed this ethical dilemma have decided that an attorney either may or may not ethically search for metadata, Pennsylvania takes the unique position of leaving the decision up to the attorneys themselves.¹³⁹ In Pennsylvania, where is it clear that the metadata was not intended to be sent:

[E]ach attorney must . . . “resolve [the issue] through the exercise of sensitive and moral judgment guided by the basic principles of the Rules” and determine for himself or herself whether to utilize the metadata contained in documents and other electronic files based upon the lawyer’s judgment and the particular factual situation.¹⁴⁰

Pennsylvania first made clear that there are no Rules of Professional Conduct governing an attorney’s ethical obligations upon receipt of

D. C. RULES OF PROF’L CONDUCT 4.4(b).

135. D.C. RULES OF PROF’L CONDUCT 8.4(c) is identical to MODEL RULES OF PROF’L CONDUCT 8.4(c).

136. D.C. Bar Ass’n, Ethics Op. 341, at 2 (2007).

137. *Id.* at 2.

138. *Id.*

139. Pa. Bar Ass’n Comm. on Legal Ethics and Prof’l Responsibility, Formal Op. 2007-500 (2007).

140. *Id.* at 1 (citing the Preamble to the Pennsylvania Rules of Professional Conduct) (alteration in original).

metadata in electronic documents.¹⁴¹ It then concluded that the duty of confidentiality and Pennsylvania Rule 4.4(b)¹⁴² require receiving attorneys to notify the sending attorney of inadvertently sent metadata so the sending attorney can take protective measures.¹⁴³

However, in addressing the issue of whether the receiving attorney may ethically review metadata contained in electronic documents in the first place, Pennsylvania declined to take a position. It merely reviewed the positions taken by other jurisdictions, and concluded that “it would be difficult to establish a rule applicable in all circumstances,” although each position “offers a persuasive rationale.”¹⁴⁴ The only guidance Pennsylvania gave to its attorneys was to use judgment, common sense, and professional courtesy, and to consider the facts of the particular situation, their duty of diligence, the nature of the information received, how and from whom the information was received, and attorney-client privilege and work product rules.¹⁴⁵

In refusing to take a position on the issue, the Pennsylvania Committee failed to serve the basic purposes of an ethics committee. The primary purpose of ethics committees is to provide advice to attorneys about ethical dilemmas.¹⁴⁶ Typically, an attorney member of a state bar may request guidance or a ruling from the ethics committee of the state bar or a bar association regarding actual or contemplated conduct.¹⁴⁷ The vehicle for providing advice to attorneys is through formal opinions, which attorneys often rely upon when engaging in conduct. The fact that an attorney relies on guidance given by an ethics opinion may be a defense to an allegation that the attorney violated the state’s ethics rules.¹⁴⁸ In some jurisdictions, attorneys acting in conformity with ethics opinions receive explicit protection from

141. *Id.* at 1.

142. Pa. Rules of Prof’l Conduct 4.4(b) is identical to MODEL RULES OF PROF’L CONDUCT 4.4(b).

143. Pa. Bar Ass’n Comm. on Legal Ethics and Prof’l Responsibility, Formal Op. 2007-500, at 5 (2007).

144. *Id.* at 5-9.

145. *Id.* at 1-2.

146. See Peter A. Joy, *Making Ethics Opinions Meaningful: Toward More Effective Regulation of Lawyers’ Conduct*, 15 GEO. J. LEGAL ETHICS 313, 313(2002); Alice Neece Mine, *How the State Bar Rules on Questions of Legal Ethics*, Ethic Opinion Articles–NC State Bar Journal, available at http://www.ncbar.com/ethics/how_state_rule.asp (last accessed July 11, 2008).

147. See Joy, *supra* note 146, at 331 (“Because few court decisions interpret the remaining ethical rules, lawyers will often have questions about the application of an ethics rule to situations not found in any reported case.”); Mine, *supra* note 146.

148. See Mine, *supra* note 146.

discipline.¹⁴⁹ Attorneys may even be entitled to rely on oral advice given by ethics committees.¹⁵⁰ When ethics committees make well-reasoned decisions, “the legal profession is better served because duties are clear and unintended violations of ethics rules can be avoided.”¹⁵¹

Moreover, courts are increasingly citing ethics opinions to support their decisions.¹⁵² Accordingly, even if an ethics opinion is simply advisory and has little to no binding effect, it should nevertheless give a well-reasoned, definitive answer, so that a court in that state can use the opinion.

Instead of reaching a well-reasoned decision on the issue, Pennsylvania took a lazy approach. In the guise of giving guidance to Pennsylvania attorneys, it left Pennsylvania attorneys in the exact same position as they were in before the Committee decided to address the issue—unclear of their obligations when they receive electronic documents outside of formal discovery. The Pennsylvania Committee failed to give its attorneys a definitive answer to an issue it recognizes as an “emerging problem.”¹⁵³ By failing to give Pennsylvania attorneys a clear answer to the question, the Committee is discouraging attorney participation in the formulation and interpretation of ethics rules.¹⁵⁴ If attorneys are left in the same position after the decision as before the decision, they may think their participation in the formulation and interpretation of ethics rules is illusory, and may ultimately be discouraged from bringing questions to ethics committees.¹⁵⁵

Because Pennsylvania did not give a clear answer to its attorneys about whether or not they can search for metadata in electronic documents, Pennsylvania attorneys do not have a clear sense of what conduct Pennsylvania is trying to encourage and what conduct it is trying to discourage. By recommending the lawyer to use judgment, common sense, and professional courtesy, Pennsylvania arguably would like its attorneys to voluntarily refrain from searching for metadata. However, without making that explicit decision, attorneys in Pennsylvania, as well

149. See Joy, *supra* note 146, at 335-37 (2002). In Alabama, Kentucky, and Rhode Island, Supreme Court rules establish the bar against discipline, while in Pennsylvania and Nebraska, the bar to disciplinary action is by custom. *Id.* at 337.

150. See Mine, *supra* note 146.

151. Joy, *supra* note 146, at 340.

152. See *id.* at 341 (“Courts treat these opinions with great deference, and, in fact, attribute to them a degree of attention similar to that usually found in the treatment of judicial opinions.”).

153. Pa. Bar Ass’n Comm. on Legal Ethics and Prof’l Responsibility, Formal Op. 2007-500, at 9 (2007).

154. See Charles M. Oldfather, *Defining Judicial Inactivism: Models of Adjudication and the Duty to Decide*, 94 GEO. L.J. 121, 139-144 (2005).

155. *Id.* at 140.

as other ethics committees that will eventually confront this issue, will not be able to reference or rely upon Pennsylvania's formal opinion.

Aside from failing to reach a well-reasoned decision, it is questionable whether the decision to search for metadata is a decision best left for the lawyers. In an ideal legal profession, attorneys would always act ethically and professionally; however, this is not realistic. Unfortunately, there are attorneys who, if it were up to them, would systematically search for metadata in all incoming electronic documents, with the sole intent of exposing attorney-client or work product information to take advantage of the adversary. By leaving the question open, Pennsylvania is encouraging, perhaps unintentionally, unethical and unprofessional conduct.

VI. SEARCHING FOR METADATA IN ELECTRONIC DOCUMENTS RECEIVED OUTSIDE OF FORMAL DISCOVERY IS UNETHICAL

There are both strengths and shortcomings to each of the positions taken by the jurisdictions that have considered the ethical implications presented by the sending and receiving of metadata outside of formal discovery. Unquestionably, an attorney who sends documents electronically has a fundamental duty of confidentiality, which includes taking measures to prevent the transmission of metadata containing privileged or protected information. However, several of the "reasonable steps" mandated or suggested by some of the Ethics Committees¹⁵⁶ are impractical and unnecessary. It is recognized that there may be valid arguments in support of a rule allowing attorneys to search for metadata. However, the searching of metadata is unethical because it is an intentional intrusion into the attorney-client relationship and constitutes conduct that is dishonest and prejudicial to the administration of justice. Moreover, because the risks of allowing an attorney to search for metadata in electronic documents outside of formal discovery substantially outweigh any benefit gained from searching, the duty of confidentiality should trump the duty of diligence and searching should be prohibited. In a legal profession where it is becoming more common for attorneys to be disciplined or disqualified for engaging in unethical

156. See State Bar of Ariz. Comm. on the Rules of Prof'l Conduct, Op. 07-03, at 2 (2007) (recommending lawyers to refrain from inserting comments in documents and from using templates); ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 06-442, at 2 (2006) (recommending lawyers to refrain from using the "track changes" function and inserting comments in word processing documents; also recommending lawyers to send documents by hand delivery, by fax, or in an image format); Colo. Bar Ass'n Ethics Comm., Op. 119, at 2 (2008) (same).

conduct,¹⁵⁷ a rule forbidding receiving attorneys from searching for metadata would help to promote needed ethics and professionalism.

A. *Requiring Sending Attorneys to Refrain from Creating Metadata and Sending Documents Electronically is Impractical and Unnecessary*

As the use of technology in law practices increases, attorneys undoubtedly must stay current with technology, including training and continuing education on the transmission of electronic documents and metadata, and the associated risks.¹⁵⁸ The responsibility to stay current with technology also includes becoming familiar with scrubbing software, how to use the software, and ensuring that colleagues and administrative assistants are educated about and are actually using the software.¹⁵⁹

Ethics Committees correctly recommend and require attorneys to scrub electronic documents before sending them to opposing counsel or elsewhere.¹⁶⁰ Scrubbing should be used as a matter of course regardless of the subject matter of the document, the sensitivity of the information it contains, and the identity of the receiving party, because a uniform system of scrubbing has a higher likelihood of effectively protecting against the disclosure of confidential information.¹⁶¹

157. *See Rico v. Mitsubishi Motors Corp.*, 171 P.3d 1092 (Cal. 2007) (affirming disqualification of plaintiff's lawyer for photocopying and using defense counsel's notes of an interview with expert witness obtained inadvertently through court reporter at deposition of expert witness).

158. N.Y. State Bar Ass'n Comm. on Prof'l Ethics, Op. 782, at 2-3 (2004); Prof'l Ethics of the Fla. Bar, Op. 06-2, at 3 (2006); *see also* Colo. Bar Ass'n Ethics Comm., Op. 119, at 2 (2008) (recommending that lawyers consider hiring a computer expert to assist with controlling the transmission of metadata); Me. Prof'l Ethics Comm. of the Bd. of Overseers of the Bar, Op. 196, at 4-5 (2008) ("undertaking this duty [to prevent the disclosure of confidential metadata] requires the attorney to reasonably apply a basic understanding of the existence of metadata embedded in electronic documents, the features of software . . . to generate the document and practical measures that may be taken to purge documents of sensitive metadata. . .").

159. D.C. Bar Ass'n, Ethics Op. 341, at 1 (2007) (attorneys must either acquire sufficient understanding of the software they use or ensure that their office employs safeguards to minimize the risk of inadvertent disclosures); *see also* Colo. Bar Ass'n Ethics Comm., Op. 119, at 2 (2008) (holding that a supervising lawyer has a duty to ensure that proper systems are in place so lawyers and non-lawyers can control the transmission of metadata).

160. *See* N.Y. County Law. Ass'n Comm. on Prof'l Ethics, Op. 738, at 1 (2008); ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 06-442, at 1 (2006); D.C. Bar Ass'n, Ethics Op. 341, at 1 (2007); Colo. Bar Ass'n Ethics Comm., Op. 119, at 2 (2008); N.Y. St. Bar Ass'n Comm. on Prof'l Ethics, Op. 782, at 3 n. 3 (2004).

161. *See* J. Brian Beckham, *Production, Preservation, and Disclosure of Metadata*, 7 COLUM. SCI. & TECH. L. REV. 1, 24 (2005-2006) (concluding that attorneys should use

However, requiring attorneys to refrain from creating metadata is impractical and would result in decreased efficiency and increased cost of representation. The benefits of technology in the practice of law include increased efficiency, productivity, and ease of collaboration, which in turn result in reduced client expense.¹⁶² Requiring attorneys to avoid creating metadata in the first place would require them to take a step backward in time and would decrease productivity and increase client expense. If attorneys are required to refrain from using the track changes function or from inserting comments in drafts of electronic documents, the benefits of electronic collaboration are defeated.

Requiring attorneys to hand deliver documents, or use image formats or fax machines to transmit documents would likewise decrease efficiency. Frequently, lawyers collaborating in a law firm on a lengthy contract need to transmit drafts electronically back and forth between opposing counsel all day in order to meet a client-imposed deadline. Requiring these lawyers to change the method of transmittal may drastically impede their ability to meet deadlines. Further, hand delivering the document may be impossible given geographical limitations. Sending the document in an image format would decrease efficiency because all attorneys involved in drafting would spend much of their time trying to decipher the changes proposed by opposing counsel as opposed to responding to the changes and making additional changes. Simply stated, any rule governing the searching of metadata must take into account the benefits of technology. Avoiding the creation of metadata, and the resulting decreased productivity and increased cost, would not be necessary if receiving attorneys are prohibited from searching for metadata in electronic documents.¹⁶³

B. The Shortcomings of a Rule Forbidding Receiving Attorneys from Searching for Metadata are Adequately Addressed

One shortcoming of a rule forbidding receiving attorneys from searching for metadata in electronic documents is that it assumes, for right or for wrong, that every attorney is acting improperly and is searching or viewing metadata with the primary goal of finding

scrubbing software because the cost is low compared to the risk of disclosing confidential, privileged, or protected information).

162. See Brian D. Zall, *Metadata: Hidden Information in Microsoft Word Documents and its Ethical Implications*, 33 COLO. LAW. 53, 53 (Oct. 2004) (noting that the collaborative exchange of electronics documents among lawyers reduce attorney billable hours and cost to clients).

163. See St. Bar of Ariz. Comm. on the Rules of Prof'l Conduct, Op. 07-03, at 3 (2007) (concluding that foregoing the use of electronic transmission of documents is not realistic or necessary).

privileged or protected information.¹⁶⁴ Some lawyers argue that there are justifiable reasons for mining metadata, and therefore, mining is not improper.¹⁶⁵ Also, the receiving attorney may accidentally come across metadata containing confidential information.¹⁶⁶ For these reasons, it is improper to categorically assume that all lawyers who mine documents for metadata are unethical.

It is recognized that there are legitimate reasons for searching metadata outside of formal discovery. Some practicing attorneys claim to search metadata for simple purposes such as finding out the name of the law firm and the lawyer who drafted a document.¹⁶⁷ Other attorneys claim to search metadata in order to “root out wrongdoing” and fraud.¹⁶⁸ For example, by searching for metadata in an electronic certificate, one attorney was able to expose an individual who was falsely claiming that a part was manufactured by a certain company.¹⁶⁹ As discussed more fully below, however, these benefits of searching are small in comparison to the substantial risks associated with searching for metadata in electronic documents outside of formal discovery. Moreover, while there may be some attorneys who do not purposefully search metadata in an effort to discover confidential information, there are attorneys who search metadata with the primary goal of finding confidential information. Therefore, a rule forbidding receiving attorneys from searching for metadata is the better approach.

Another shortcoming of a rule forbidding receiving attorneys from searching is that, by itself, it does not encourage the sending attorney to be more careful when sending electronic documents. If there is a rule that bans a receiving attorney from looking for metadata, then the sending attorney arguably has no incentive to take steps to avoid the inadvertent disclosure of metadata. Fortunately, all ethics committees agree that there is a corresponding duty on the sending party to take reasonable steps to prevent an inadvertent disclosure.¹⁷⁰ A rule barring the searching of metadata must not limit the duty of the sending attorney

164. See Colo. Bar Ass’n Ethics Comm., Op. 119, at 3 (2008) (noting that attorneys are not always being deceitful when searching metadata or are not always using surreptitious means of finding metadata).

165. Walker, *supra* note 2, at 2.

166. For example, the receiving attorney may unintentionally find a comment embedded in a document simply by holding the cursor over a word and unknowingly causing an embedded comment to appear. Upon opening a document, a receiving attorney may find that the sending attorney accidentally left the “track changes” function on when transmitting the document. Any rule holding that a receiving lawyer acts unethically when searching for metadata should not encompass this situation.

167. Walker, *supra* note 2, at 2-3.

168. *Id.*

169. *Id.*

170. See Section V.A. *supra*.

to exercise reasonable care to prevent the inadvertent transmission of confidential metadata. Otherwise, the rule would encourage attorneys to remain ignorant of advances in technology and would encourage carelessness with confidential information.

Arguably, the receiving attorney should not be prevented from looking for metadata, because by exercising reasonable care, the sending attorney could have reviewed and removed the metadata before sending the document electronically.¹⁷¹ This would be a strong argument if there were a guarantee that the sending attorney could remove all metadata from an electronic document before transmission. However, there appears to be consensus that scrubbing software may not completely remove all metadata from electronic documents.¹⁷² If that is the case, then despite all reasonable efforts a sending attorney may take, confidential metadata may still slip through the cracks, and whether or not any confidential or protected information is revealed depends entirely on whether the receiving party may or may not search.

Furthermore, there may be a situation where the sending attorney simply makes a mistake or where the sending attorney did not use due care in the sending of documents and privileged information was disclosed. A rule allowing receiving attorneys to search for metadata would permit the receiving attorney to unfairly take advantage of the sending party's innocent mistake or breach of ethics.¹⁷³ It is certainly true that the sending lawyer may have violated the duties of competence and confidentiality, but it would not be fair for the receiving party to exploit the sending party's breach of duty. The receiving attorney will

171. Hricik & Jueneman, *supra* note 23, at 20.

172. *See id.* at 18 (noting that metadata cannot be removed easily from documents and that scrubbing programs are not foolproof; most scrubbing programs "do not integrate with e-mail systems to remove metadata from documents being sent out from the e-mail program, and most macro solutions still put the onus on the users to run the macro"); Jembaa Cole, *When Invisible Electronic Ink Leaves Red Faces: Tactical, Legal and Ethical Consequences of the Failure to Remove Metadata*, 1 SHIDLER J. L. COM. & TECH. 8 (2005), available at <http://www.lctjournal.washington.edu/Vol1/a008Cole.html> (scrubbing software may not remove all metadata); Microsoft, How to minimize metadata in Word 2003, July 27, 2006, <http://support.microsoft.com/kb/825576/> (last accessed Aug. 6, 2008) (there is no single method to remove all metadata from electronic documents); Mark Grossman, *Metadata*, Grossman Law Group, http://www.ecomputerlaw.com/articles/show_article.php?article=2006_metadata (last accessed Aug. 6, 2008) (warning lawyers not to assume that the scrubbing software got rid of all metadata).

173. *But see* J. Brian Beckman, *Production, Preservation, and Disclosure of Metadata*, 7 COLUM. SCI. & TECH. L. REV. 1, 28-30 (2005-2006) (concluding that a receiving attorney should not be permitted to search for documents when the sending attorney took reasonable steps to scrub the documents of metadata, but should be permitted to take advantage of the sending attorney's inadvertent mistake of neglecting to scrub documents of their metadata).

not know at the time of the searching for metadata whether the sending attorney complied with the duties of competence and confidentiality, and just made a mistake, or whether the sending attorney was in breach of those duties. Accordingly, the better approach is to forbid the receiving attorney from searching for metadata, and thereby potentially taking advantage of either an ethical breach or an innocent mistake.

C. The Duty of Confidentiality Trumps the Duty of Diligence Because the Risk of Searching Outweighs the Benefits

A rule allowing receiving attorneys to search for metadata wrongfully favors the duty of diligence over the duty of confidentiality. Arguably, the receiving attorney violates a duty of confidentiality by searching for metadata in electronic documents transmitted outside of formal discovery. Even though the duty of confidentiality protects against “the disclosure by a lawyer of information relating to the representation of a client,” the duty of confidentiality also broadly protects “the trust that is the hallmark of the client-lawyer relationship.”¹⁷⁴ All lawyers, therefore, have a duty to protect confidentiality, and this duty is owed to the bench and bar, and to the legal profession as a whole.¹⁷⁵ Accordingly, the duty of confidentiality not only forms the foundation of the sending attorney’s duty to protect against inadvertent disclosure of confidential information in metadata, but also forms the foundation of the receiving attorney’s duty to refrain from searching for the metadata.¹⁷⁶

The reason the duty of confidentiality should trump the duty of diligence, at least in the context of searching for metadata in electronic documents transmitted outside of formal discovery, is that the risk of exposing attorney-client privileged or work product information outweighs the benefits of searching for the metadata. The highest benefit from searching for metadata is achieved in the context of formal discovery. This is because in formal discovery the parties are requesting the production of documents in order to gather information to support their claims and defenses. It is undisputed that metadata can sometimes be critical to helping a party establish a claim or defense.

174. MODEL RULES OF PROF’L CONDUCT R. 1.6 cmt. 2 (2008).

175. See *Rico v. Mitsubishi Motors Corp. et al.*, 171 P.3d 1092, 203 (Cal. 2007) (noting that attorney have an obligation to respect members of the bench and bar, as well as the overall administration of justice); Me. Prof’l Ethics Comm. of the Bd. of Overseers of the Bar, Op. 196, at 3 (2008) (noting that attorneys share responsibility for protecting the attorney-client privilege).

176. See N.Y. St. Bar Ass’n Comm. on Prof’l Ethics, Op. 749, at 4 (2001) (holding that the disclosure of client confidences is a result of a deliberate act of the receiving attorney, not any inadvertence or carelessness by the sending attorney).

However, outside of formal discovery, there is very little benefit to be obtained from searching for metadata. As discussed above, the only examples of the benefits of searching for metadata outside of formal discovery are to learn the identity of the law firm or attorney who drafted a document and to root out wrongdoing or fraud. The receiving attorney gains little benefit from learning the name of the drafting law firm and attorney, and certainly, the receiving attorney can acquire this information from some other means besides searching through metadata. Additionally, although a receiving attorney may be able to expose wrongful claims or other misrepresentations by looking at the metadata, this same benefit may be achieved during formal discovery where searching for metadata is presumptively allowed. Furthermore, despite the existence of valid reasons for searching, it cannot be ignored that some attorneys will search metadata for the sole purpose of discovering privileged or protected information.¹⁷⁷

The corresponding risk, however, is greater than the benefit. If a receiving attorney is allowed to search for metadata in electronic documents, there is a risk that the receiving attorney will uncover privileged or protected information. It may be true that the chance of discovering confidential information in metadata is slight.¹⁷⁸ However, if the metadata does in fact contain confidential information, the risk of the confidential nature of the information being destroyed is great because there is no way to redress the destruction of the confidence. Even though the receiving attorney may have a duty under Rule 4.4(b) to notify the sender if she knows or reasonably should know that the document was inadvertently sent,¹⁷⁹ once the attorney sees the protected information, it is impossible for the receiving attorney to “forget” what was read. The information is out there, and some information, such as the figure a client is willing to settle for, is learned information that cannot be returned or forgotten. Even if a court later orders that the information was protected by the attorney-client privilege or work product doctrine, there is nothing a court can do to redress the inadvertent disclosure as it “would be the equivalent of closing the barn door after the animals have already run away.”¹⁸⁰ Because the risk of destruction is so great and the

177. See David Hricik, *Mining For Embedded Data: Is it Ethical to Take Intentional Advantage of Other People's Failures*, 8 N.C. J. L. & TECH. 231, 235 (2007) (noting that by searching for metadata, a lawyer is looking for information from earlier drafts and hoping that the sending lawyer “either failed to remove the information or failed in his attempt to do so”).

178. Colo. Bar Ass'n Ethics Comm., Op. 119, at 3 (2008).

179. See MODEL RULES OF PROF'L CONDUCT R. 4.4(b).

180. Deborah Cassens Weiss, *E-Discovery Disclosure Goof Waived Attorney-Client Privilege, Judge Rules*, at 1, June 4, 2008, http://www.abajournal.com/news/e_

corresponding benefit is so low, the duty of confidentiality should trump the duty of diligence, and attorneys should not be ethically permitted to search for metadata.

D. Searching and Reviewing Confidential Metadata is Dishonest and Prejudicial to the Administration of Justice

A rule allowing receiving attorneys to search for metadata, and to continue reviewing the metadata even after learning that the information is confidential, considers Rule 4.4 in a vacuum and does not adequately address the other ethical obligations of attorneys, such as the duty of honesty and the duty to refrain from engaging in conduct prejudicial to the administration of justice.¹⁸¹

The American Bar Association, Maryland, and Colorado all permit receiving attorneys to search for metadata in electronic documents, and to review and use metadata *even after learning that the information contains confidential information* and was not intended for the receiving attorney.¹⁸² All three positions rely solely on their versions of Rule 4.4 to come to this conclusion. The American Bar Association and Colorado hold that the only affirmative obligation of the receiving attorney is to notify the sending attorney if the receiving party knows or reasonably should know that the document was inadvertently sent.¹⁸³ Maryland, which does not have a Rule 4.4(b), does not even require notice of an inadvertent transmission to the sending attorney.¹⁸⁴ Colorado, at least, holds that its Rule 4.4(c) requires receiving attorneys to refrain from reviewing metadata if the sending attorney gives notification of the inadvertent disclosure.¹⁸⁵

discovery_disclosure_goof_waived_attorney_client_privilege_judge_rules/ (last accessed Aug. 6, 2008).

181. See MODEL RULES OF PROF'L CONDUCT R. 8.4(c); (d).

182. See ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 05-437, at 2 (2005) (interpreting Rule 4.4(b) to permit receiving lawyers to search and review inadvertently disclosed material); ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 06-442, at 2 (2006) (holding that Rule 4.4(b) only requires the receiving lawyer to notify the sending lawyer of the receipt of inadvertently transmitted electronic information, and imposes no other restrictions); Md. St. Bar Ass'n Comm. on Ethics, Docket No. 2007-09, at 2 (2007) (interpreting Maryland's Rule of Professional Conduct 4.4 to impose no obligation on the receiving lawyer to notify the sending lawyer of the inadvertent transmission of electronic information, thereby allowing receiving lawyers to search, review, and use confidential metadata); Colo. Bar Ass'n Ethics Comm., Op. 119, at 4 (2008) (holding that the receiving lawyer may continue to review inadvertently disclosed confidential metadata after learning of its confidential nature in the absence of notice of inadvertent disclosure from the sending lawyer).

183. See ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 06-442, at 2 (2006); Colo. Bar Ass'n Ethics Comm., Op. 119, at 4 (2008).

184. See Md. St. Bar Ass'n Comm. on Ethics, Docket No. 2007-09, at 2 (2007).

185. Colo. Bar Ass'n Ethics Comm., Op. 119, at 4 (2008).

The ABA, Maryland, and Colorado look at their Rule 4.4 in a vacuum, and do not address other important ethical considerations, such as a lawyer's duty of honesty or duty to refrain from conduct that is prejudicial to the administration of justice. For example, the ABA's position is that a lawyer's duty of honesty is not implicated because Rule 4.4(b) does not prohibit the searching and review of metadata.¹⁸⁶ Likewise, Maryland does not address concerns of misconduct; because Rule 4.4 does not prohibit searching and reviewing of metadata, the searching is ethical. A conclusion about whether searching and reviewing metadata is dishonest cannot be reached, however, without an analysis of the ethical rules governing misconduct, especially where Rule 4.4(b) neither expressly prohibits the searching nor expressly sanctions the searching.

Allowing receiving attorneys to search for metadata in electronic documents outside of formal discovery allows attorneys to engage in behavior that is dishonest and deceitful, in violation of ethics rules prohibiting misconduct.¹⁸⁷ As discussed above, although it is recognized that some attorneys have valid reasons for searching metadata, attorneys also search with the sole intention of finding privileged or protected information.¹⁸⁸ The dishonesty is a result of the steps the receiving attorney takes to intentionally intrude into the attorney-client privilege or work product protection to obtain knowledge of privileged or protected information, without the knowledge of the sending attorney.¹⁸⁹

Colorado is the only jurisdiction that attempted to address a receiving attorney's duty of honesty under Rule 8.4(c).¹⁹⁰ Colorado, in holding that a receiving attorney may continue to review metadata even after learning that it is confidential, rejected the District of Columbia's

186. See ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 06-442, at 2 (2006) (addressing the propriety of using the lawyer's duty of honesty to hold that searching metadata is ethically impermissible simply by stating that "Rule 4.4(b) identif[ies] the sole requirement of providing notice to the sender of the receipt of inadvertently sent information. . . .").

187. MODEL RULES OF PROF'L CONDUCT R. 8.4(c) (2008).

188. See Hricik, *supra* note 177, at 235 (noting that by searching for metadata, a lawyer is looking for information from earlier drafts and hoping that the sending lawyer "either failed to remove the information or failed in his attempt to do so").

189. Certainly the searching of metadata will ordinarily be unknown to the sending attorney, and further, the sending attorney may never learn of any inadvertently disclosed privileged information. This is especially true in jurisdictions, such as Maryland, that do not require receiving attorneys to give notice to the sending attorney that privileged or protected information was inadvertently transmitted. See Me. Prof'l Ethics Comm. of the Bd. of Overseers of the Bar, Op. 196, at 3 (2008) (the receiving attorney's "purposeful efforts to probe for information he or she knows or should know to be confidential and not to have been knowingly communicated by opposing counsel" is dishonest and prejudicial to the administration of justice).

190. See Colo. Bar Ass'n Ethics Comm., Op. 119, at 4 (2008).

conclusion that to continue to review the confidential information would amount to professional misconduct under Rule 8.4.¹⁹¹ In reasoning that the more specific Rule 4.4(b) trumps the more general Rule 8.4, Colorado incorrectly wrote into Rule 4.4(b) language permitting searching for metadata and continuing to review metadata after learning of its confidential information. It cannot be said that a “specific” rule trumps a more general rule when the specific rule does not even contain express language sanctioning the conduct at issue. If Colorado’s Rule 4.4(b) did contain express language permitting receiving attorneys to search and to continue to review metadata, then Colorado’s conclusion that Rule 4.4(b) trumps Rule 8.4 would have merit.¹⁹²

There is something inherently dishonest about allowing a receiving attorney to continue to review and use privileged or protected information even after learning of its confidential nature. If a jurisdiction wants to allow an attorney to search, which this paper ultimately concludes is not the best approach, at the very least a receiving attorney should be obligated to refrain from continuing to review the information once the attorney realizes that it is confidential.¹⁹³ Continuing to review this confidential information is dishonest and is prejudicial to the administration of justice because the searching attorney is intruding into the most important relationship in the legal profession—the relationship between the client and attorney. Moreover, the searching attorney is intruding into one of the most precious areas of the legal profession—the mental thoughts, impressions, and conclusions of the attorney. Finally, these intrusions irreversibly prejudice the sending attorney and client.

It is hard to imagine that this conduct would be sanctioned if the same information were transmitted by hand. Consider the situation where a plaintiff’s attorney inadvertently comes into possession of work product—defense counsel’s notes of interviews with defense experts—and plaintiff’s attorney knows that defense counsel did not intend for plaintiff’s attorney to have the document.¹⁹⁴ Should plaintiff’s attorney be ethically permitted to make a copy of the notes, give copies to co-

191. *See id.*

192. *See Hricik, supra* note 177, at 243 (noting that conduct made permissible by a specific rule would not violate a more general rule).

193. Whether or not the receiving attorney would be able to exercise restraint and refrain from continuing to review the information is another question. Certainly, the inability of attorneys to exercise restraint is not a valid reason for failing to adopt a rule that prohibits them from doing so, and it cannot justify a rule allowing attorneys to continue doing so.

194. These are the facts from *Rico v. Mitsubishi Motors Corp.*, 171 P.3d 1092, 1094-95 (Cal. 2007), where it was unclear how plaintiff’s attorney obtained a copy of the defense attorney’s notes; plaintiff’s attorney claimed that the court reporter gave him the notes, and the defense attorney claimed that plaintiff’s counsel took them from the case file.

counsel and use the notes to impeach the defense expert at a deposition?¹⁹⁵ In Maryland, the plaintiff's attorney will have no duty to notify defense counsel and would be free to make the copies and to use the work product notes to impeach the witness at the deposition.

The California Supreme Court, when confronted with these facts in *Rico v. Mitsubishi Motors Corp.*, held that plaintiff's counsel acted unethically by making copies and "surreptitiously using it to gain maximum adversarial advantage."¹⁹⁶ Rejecting plaintiff's counsel's argument that he had a duty to use the material to his client's advantage, the California Supreme Court concluded that plaintiff's attorney should have refrained from reviewing the notes any more than was necessary to determine the confidential nature of the information.¹⁹⁷ This rule, California reasoned, would prevent attorneys from taking unfair advantage of opposing counsel and causing irreparable prejudice.¹⁹⁸ The California Supreme Court also noted that attorneys have an obligation to respect members of the bar, the judiciary, and the overall administration of justice.¹⁹⁹ The result should not be any different with electronic information.

VII. PROFESSIONALISM REQUIRES ATTORNEYS TO REFRAIN FROM SEARCHING

The duty of diligence does not mandate a rule allowing receiving attorneys to search for metadata. While Rule 4.4(b) stops short of placing an affirmative duty on the receiving attorney to refrain from searching and viewing metadata, an attorney may use professional judgment to return a document to the sending party unread when she knows or reasonably should know that it was sent inadvertently.²⁰⁰ Even though Rule 1.3 requires attorneys to act diligently to represent their clients, an attorney is not obligated "to press for every advantage that might be realized for a client" or to use offensive tactics.²⁰¹ Further, the duty of diligence does not impede an attorney from being courteous and respectful or from using professional judgment with respect to the means of pursuing a matter for a client.²⁰² Accordingly, principles of confidentiality and professionalism may outweigh an attorney's duty of diligent representation in some circumstances, including the searching

195. This is what the plaintiff's counsel did in *Rico*, 171 P.3d 1092.

196. *Rico*, 171 P.3d at 1096.

197. *See id.* at 1098-99.

198. *See id.* at 1096, 1099.

199. *See id.* at 1099.

200. *See* MODEL RULES OF PROF'L CONDUCT R. 4.4 cmt. 3 (2008).

201. *See* MODEL RULES OF PROF'L CONDUCT R. 1.3 cmt. 1 (2008).

202. *See id.*

for metadata outside of formal discovery. Just because Rule 4.4(b) does not specifically forbid an attorney from searching for metadata does not mean that permitting the attorney to do so is the only option.²⁰³

The legal profession is one in which rules should be created to encourage ethical behavior and professionalism. Attorneys are officers of the court and are relied upon to make the legal system function properly. As such, there are times when attorneys should make decisions that promote justice in a broader sense, as opposed to focusing solely on the pursuit of substantive justice in an individual case.²⁰⁴ Unfortunately, regardless of how careful the sending attorney is, there is no guarantee that human error will not occur or that scrubbing software will eliminate all metadata from electronically transmitted documents.²⁰⁵ A rule allowing a receiving attorney to search for metadata encourages the receiving attorney to take advantage of an innocent mistake. The better response to a mistake, or even unprofessional behavior and breaches of ethical duties, is professionalism and civility.²⁰⁶

VIII. CONCLUSION

Although some attorneys search metadata in electronic documents received outside of formal discovery to root out fraud or learn the truth, other attorneys act unethically and search with the intention of discovering information protected by the attorney-client privilege or work product doctrine. Intentionally trying to find privileged or protected information is dishonest and is prejudicial to the administration of justice. Regardless of the reason for searching, however, the risk that

203. See Prof'l Ethics of the Fla. Bar, Op. 06-2 (2006) (holding, with a rule identical to MRPC 4.4(b), that it is impermissible for a receiving attorney to mine for metadata).

204. See WILLIAM M. SULLIVAN ET AL., EDUCATING LAWYERS: PREPARATION FOR THE PROFESSION OF LAW 131 (Jossey-Bass 2007) (citing WILLIAM H. SIMON, THE PRACTICE OF JUSTICE: A THEORY OF LAWYERS' ETHICS 9 (Harvard University Press 1998)).

205. See Hricik, *supra* note 177, at 232 (noting that lawyers "will fail to take appropriate technological safeguards" or "safeguards will fail despite the lawyer's best efforts"); see also Pa. Bar Ass'n Comm. on Legal Ethics and Prof'l Responsibility, Formal Op. 2007-500, at 9 (2007) ("Although a transmitting attorney has tools at his disposal that can minimize the amount of metadata contained in a document he or she is transmitting, those tools still may not remove all metadata."); N.Y. St. Bar Ass'n Comm. on Prof'l Ethics, Op. 749, at 1 (2001) (citing M. David Stone, *Deleting Your Deletions*, P.C. MAGAZINE, Nov.20, 2000) (effectively blocking metadata from receiving parties is a matter of debate among computer users); Cole, *supra* note 172; Microsoft, *supra* note 172 (noting that "there is no single method to remove . . . [metadata] from your documents"); Grossman, *supra* note 172 (warning attorneys not to assume that scrubbing software strips all metadata).

206. James E. Ferguson, *Professionalism and Civility: Necessary Tools of Effective Advocacy*, Lawyer to Lawyer: North Carolina Reflections on the Practice of Law, at 19, the N.C.Bar Ass'n Professionalism Comm., 2008.

the searching will result in the destruction of privileged or protected information is too great to permit attorneys to search.