

ARTICLE: THE ETHICS OF METADATA: A CRITICAL ANALYSIS AND A PRACTICAL SOLUTION

2010

Reporter

63 Me. L. Rev. 175

Length: 50659 words

Author: Hans P. Sinha*

* Clinical Professor of Law and Director of the Prosecution Externship Program with the National Center for Justice and the Rule of Law, University of Mississippi School of Law. B.A., University of Pennsylvania 1983; J.D., Tulane School of Law 1988; LL.M in Comparative and International Law (with distinction), Tulane School of Law 2001.

LexisNexis Summary

... With lines drawn on both sides of the issue-the original New York opinion representing the view that an attorney may not view or use metadata, and the ABA opinion representing the view that, in the absence of a rule to the contrary, an attorney is not prohibited from mining metadata, her only ethical obligation being to notify the sending attorney of the inadvertent transmission-these opinions fell into one of two camps: (1) Florida, Alabama, Arizona, Maine, and New Hampshire adopted the original New York prohibition against a receiving lawyer viewing or using material contained in transmitted metadata; and (2) Maryland, Colorado, and Vermont took the opposite view. ... In other words, while a sending attorney in a jurisdiction that permits mining could unilaterally provide the receiving attorney notice that the documents he sends have been scrubbed of metadata and that any remaining metadata is inadvertently included and should be considered confidential material, a receiving attorney in a jurisdiction that prohibits mining cannot unilaterally provide the sending attorney with a notice that he intends to mine any received documents and then ethically mine such metadata. ... The Committee reached this conclusion by addressing all of the topics raised in previous metadata ethics opinions, including the sender's duty, the receiving attorney's duties, and the interplay of Model Rules 1.1-Competence, 1.3-Diligence and Zeal, 1.6-Confidentiality of Information, 3.4-Fairness to Opposing Party and Counsel, 4.4(b)-Respect for Rights of Third Persons, and 8.4-Misconduct. ... After examining all previous metadata ethics opinions, pertinent Rules of Professional Conduct, and prior Colorado ethics opinions, the Ethics Committee of the Colorado Bar Association (Colorado Ethics Committee) concluded that "the ABA, Maryland, and District of Columbia opinions are better reasoned, and that the New York, Arizona, Alabama, and Florida opinions are based on incorrect factual premises regarding the nature of metadata." ... Thus, while the New Hampshire Ethics Committee may be correct that negotiated confidentiality agreements (outside of the formal discovery context) that address how to approach the possible disclosure of confidential information subsequent to discovery may be ineffective to the extent that the confidential or privileged information is then already disclosed, bilateral agreements between and amongst attorneys, or unilateral notices issued in jurisdictions

with different or no ethical guidelines as to the mining of metadata at the outset of, and especially before, any exchange of electronic documents, are if not necessary, highly desirable. ... In arguably one of the most thorough and logical metadata ethics opinions to date, Vermont fully adopted both the ABA notion that absent a prohibition on mining in the rules, an ethics committee such as the Vermont Section, is not free to find that such a prohibition exists, and the Pennsylvania view that adopting such a prohibition would negatively impact the ability and duty of the receiving lawyer to diligently represent her client. ... While the Federal Rules of Civil Procedure do not govern the electronic exchange of documents outside of the formal discovery process, they do provide a familiar source to which the legal profession can look for guidance in terms of how to improve the handling of metadata contained in electronically exchanged documents in the non-discovery realm. ... All jurisdictions, regardless of their view as to whether the mining of metadata is permitted, presumably agree with the comments to Model Rule 1.6 that "a fundamental principle in the client-lawyer relationship is that, in the absence of the client's informed consent, the lawyer must not reveal information relating to the representation."

Text

[*176]

I. Introduction

A. A Short Primer

Metadata is generally defined as being "data about data."¹ Metadata comes in two forms. One consists of non-visible data produced by a computer program, such as a word-processing software program, as that program is used to create visible data. This form of "metadata" generally contains information as to when the visible text was created, by whom, and when it was changed. It is created and stored within a document in a non-visible form regardless of what the author does.² The second type of metadata is author-created data in that an author generates it by employing common word-processing program features such as "track changes"

¹ David Hricik, I Can Tell When You're Lying: Ethics and Embedded Confidential Information, [30 J. Legal Prof. 79, 81 \(2006\)](#) (noting that "[m]etadata is 'data about data,'" and comparing it to the more familiar "fax band on a document received by facsimile," which typically shows the number the fax originated from, the number of pages, and when it was received). Viewed in this light, "[a] fax band is metadata, since it is data about data." *Id.* See Campbell C. Steele, Attorneys Beware: Metadata's Impact on Privilege, Work-Product, and the Ethical Rules, [35 U. Mem. L. Rev. 911, 935 \(2005\)](#) (describing metadata as "hidden data, or 'data about data'"). The word "metadata" itself was coined by Jack E. Myers, president of The Metadata Company, LLC, in 1969. It was registered as a trademark in 1986, and (theoretically) belongs to The Metadata Company. See Webster's Online Dictionary, <http://www.websters-online-dictionary.com/definitions/The+Metadata+Company?cx=partner-pub-0939450753529744%3Av0qd01-ttlq&cof=FORID%3A9&ie=UTF-8&q=The+Metadata+Company&sa=Search#937> (last visited Nov. 11, 2010). Black's Law Dictionary defines metadata as "[s]econdary data that organize, manage, and facilitate the use and understanding of primary data." Black's Law Dictionary 1080 (9th ed. 2009). Interestingly, and an indication of how quickly the concept has evolved in the last few years, the 2004 edition of Black's Law Dictionary did not contain a definition for metadata. See Black's Law Dictionary 1011 (8th ed. 2004) (indicated page where term metadata would have appeared).

² Bradley H. Leibert, Applying Ethics Rules to Rapidly Changing Technology: The D.C. Bar's Approach to Metadata, [21 Geo. J. Legal Ethics 893, 895 \(2008\)](#) (referring to "hidden" information).

or "insert comment." ³ Although the visible aspects of the latter type of data can be erased by the author prior to electronically sharing the document with someone [*177] else, these changes and comments may remain embedded in a hidden format within the metadata. ⁴ Metadata can be removed by employing features of the word- processing program on which it was created, ⁵ or by using special "scrubbing" programs to proactively remove metadata. ⁶ As technology advances, however, there is a concern as to whether someone attempting to remove metadata will ever be certain that he or she has successfully removed all metadata.

The process of searching metadata for information is referred to as "mining" metadata. ⁷ This process is generally carried out by an individual who deliberately [*178] sets out to discovery

³ The Sedona Principles: Best Practices Recommendations and Principles for Addressing Electronic Document Production, a project of The Sedona Conference Working Group, defines the two types of metadata as "application" and "system" metadata. The Sedona Principles note that "[a]pplication metadata is created as a function of the application software used to create the document or file," while "[s]ystem metadata reflects information created by the user or by the organization's information management system." The Sedona Principles (Second Edition) Addressing Electronic Document Production, The Sedona Conference, 60 (July 7, 2010), <http://www.thesedonaconference.org/dltForm?did=TSC> PRINCP 2nd ed 607.pdf (last visited Nov. 11, 2010).

⁴ In addition, Microsoft Word has features that allow and enable an author of a document to minimize the creation of metadata. See generally David Hricik & Chase Edward Scott, Metadata: The Ghosts Haunting e-Documents, Ga. B.J., Feb. 2008, at 16, 20-21 [hereinafter Hricik & Scott] (describing steps an author using Microsoft Word can take to avoid creating embedded data).

⁵ Both Microsoft Word 2003 and Microsoft Office 2007, for example, provide the user with means to "alter the types and amount of embedded information that will be stored in their documents." David Hricik & Edward Scott, Metadata: The Ghosts Haunting e-Documents, 82 Fla. B.J., Oct. 2008, at 32, 36 [hereinafter Metadata: The Ghosts Haunting e-Documents]. Hricik and Scott provide easy to follow procedures for users of Word 2003 (select "Options" from the "Tools" menu, and then checking the "Remove personal information from file properties on save" box in the "Security" tab) and Office 2007 (select "Prepare" from the Microsoft Office button, then "Inspect document," which in turn will provide an opportunity to deselect the types of metadata that will be included in the document) to minimize the amount of metadata created in the document. Id. at 36, 38. Microsoft's 2007 versions of Word, Office Excel, and PowerPoint provide a "Document Inspector" that is designed to help the user "find and remove different kinds of hidden data and personal information." See Remove Hidden Data and Personal Information from Office Documents, Microsoft Office Word, <http://office.microsoft.com/en-us/help/HA100375931033.aspx> (last visited Nov. 11, 2010).

⁶ Hricik & Scott, supra note 4, at 22 (describing ways to remove embedded data, including through the usage of commercially available "scrubbers" software, and noting that "[n]umerous 'scrubbers' can be found through Google, simply by searching for 'metadata' and 'scrubber.'" Id. at 25 n.35. An indication of the proliferation of metadata scrubbers is apparent from a Google search for "metadata scrubbers." Such a search on February 12, 2009 resulted in 40,600 "hits." Not all offered scrubbers. However, three selected at random indicated the existence and need for such programs: a program entitled "SendShield" promises to "automatically notif[y] you of metadata in your Word and Microsoft Office documents," and to assist the customer to identify, remove and convert into PDF format. Metadata Removal Software, SendShield, <http://www.sendshield.com/home/index.php> (last visited Nov. 11, 2010); Workshare Protect promises to "remove[] metatdata from your Word documents and keep[] sensitive information from leaking," Workshare, <http://www.workshare.com/go/metadata-software.aspx?kk-etaddata%20scrubber&kt=8a83113c-2ca1-45c4-878d-c6d966221fdc&gclid=CPzsoqWq15gCFRo-awodqCzadw> (last visited Nov. 11, 2010); and MetaReveal bills itself as a "Microsoft Office add-in software application that works within Word, Excel and Outlook to analyze and remove metadata and hidden data." M e t a R e v e a l , <http://www.beclegal.com/products.aspx?id=64&gclid=CJb4hPyq15gCFSUGDQodmTzaeA> (last visited Nov. 11, 2010). Considering the iniquitousness of metadata, as well as the readily available means to guard against the inadvertent transmittal of metadata, it is increasingly difficult not to assume that an attorney's duty of competence includes knowledge of the possible dangers associated with metadata, as well as the possible remedies.

⁷ "Mining" used in the metadata context has been defined as "the process by which attorneys intentionally and actively search for data hidden within a document." Bradley H. Leiber, Applying Ethics Rules to Rapidly Changing Technology: The D.C. Bar's

information contained in an electronic document's metadata. Such attempts normally involve using the features commonly found on the software program that produced the metadata. In a Word document, this can be as simple as turning on the "Track Changes" feature. It can also involve using more technologically advanced methods not readily available to a lay person. One can also discover metadata through innocuous means such as placing the computer cursor over a portion of the text. If, for example, hidden comments were inserted there, they may become visible on the screen.

Much, if not most, of the metadata produced is innocuous or irrelevant to any legal proceeding. When and by whom, for example, the word "it's" was changed to "its" in a legal document, is likely not to be relevant or considered confidential or privileged. However, the draft of a contract circulated within a law firm wherein several attorneys insert comments regarding case strategy, as well as the client's bottom-line settlement amount, would be highly relevant if not critical, and would constitute confidential and privileged information. If the lawyer who circulated that original document erased the visible text of those comments, but failed to "scrub" (remove the non-visible metadata) the document before electronically transferring a copy of it to opposing counsel, two issues have potentially been created. First, the sending lawyer, (the lawyer with whom the electronic document originated and who electronically transmitted it to opposing counsel) may have failed to adequately preserve client confidences and disclosed privileged information.⁸ Second, the receiving lawyer, (the lawyer who received the electronic document containing metadata from opposing counsel), is faced with an ethical choice. He can choose to read only the visible text in the document. In doing so, he would not be "mining" the metadata contained in the document for information. Or, he could choose to mine the metadata for the non-visible information contained therein.⁹ With the exception of metadata that appears automatically when the cursor is moved over a portion of the text, an attorney who chooses to examine the material contained in metadata would do so through a conscious decision to mine such metadata.

The ethical issue associated with metadata thus contains two distinct and intertwined acts. The first is the failure on the part of the sending lawyer to ensure that the document he or she electronically transmitted to opposing counsel did not contain confidential and privileged

Approach to Metadata, 21 Geo. J. Legal Ethics 893, 897 (2008). Alabama defines mining as "[t]he act of deliberately seeking out and viewing metadata embedded in a document." Ala. State Bar Ethics Op. RO-2007-02, 1 (March 14, 2007), <http://www.alabar.org/ogc/PDF/2007-02.pdf> (last visited Nov. 11, 2010) [hereinafter Ala. Op. 2007-02]. The term "mining" per se does carry some pejorative baggage, leading one state's ethics committee to use the more neutral term "search" instead. See Vt. Bar Ass'n Prof'l Ethics Responsibility Section, Ethics Op. 2009-1, 1 (Sept. 2009), <http://www.vtbar.org/Upload%20Files/WebPages/Attorney%20Resources/aeopinions/Advisory%20Ethics%20Opinions/Electronic%20Documents/09-01.pdf> (last visited Nov. 11, 2010) [hereinafter Vt. Op. 2009-1].

⁸ The duty of an attorney to safeguard client confidences and not reveal information relating to the representation of a client is "a fundamental principle in the client-lawyer relationship." See Model Rules or Prof'l Conduct R. 1.6 (2010).

⁹ How common it is for attorneys who receive electronically transmitted documents to engage in mining is hard to gauge. However, a possible indication of the ease with which attorneys may choose to mine once they know about the concept of metadata as whole, are found in the comments of the 2004 chair of the ABA's Cyberspace Law Committee, Vincent Polly. Mr. Polly noted that "[t]he first thing lawyers need to know about metadata is that there is such a thing." He then went on to admit that "[t]he first thing I do when I get something is look for [metadata] like the author's name, revisions and history." Jason Krause, Hidden Agendas: Unlocking Electronic Codes Can Reveal Deleted Text, Revisions, 90 A.B.A.J. 26 (2004).

information within the document's metadata. [*179] This step involves the attorney's duty to provide competent representation to a client, and above all, the attorney's duty to preserve the confidentiality of information pertaining to the representation of a client. Second is the conscious act on the part of the receiving lawyer to actively seek out and review, or "mine," metadata embedded in the electronically received document. This step involves the attorney's duty to respect the rights of third parties, his duty not to engage in fraudulent conduct, as well as the attorney's duty to zealously represent his client.

The ease with which documents can be transmitted over the internet via e-mail has led to the exchange of legal documents between attorneys in electronic format (generally as attachments to an e-mail) on a daily basis. While some exchanges of electronic documents occur in a formal discovery context, governed by formal rules of discovery or court-orders, the vast majority of electronic documents exchanged between attorneys occurs in the non-formal discovery context: two or more attorneys simply exchanging contract drafts, memoranda, letters-documents pertaining in one way or another to the representation of their clients-between and amongst each other. This Article examines the ethical issues these lawyers face with regard to the metadata contained in such documents. It does so by first discussing the general ethical dilemma surrounding metadata. The Article next provides an in-depth examination and critical analysis of the legal community's view of the ethical parameters surrounding metadata, as seen through fourteen ethics opinions issued by thirteen states and the American Bar Association (ABA) as of August, 2010. The fourteen jurisdictions that have issued such ethics opinions, listed in alphabetical order, are: Alabama, Arizona, Colorado, the District of Columbia, Florida, Maine, Maryland, Minnesota, New Hampshire, New York, Pennsylvania, Vermont, and West Virginia, and the ABA.

An examination of these ethics opinions show that two predominant views have emerged. One view holds that mining of metadata constitutes an impermissible attempt by the receiving attorney to breach what the profession holds dearest: the confidentiality between an attorney, in this context the sending attorney, and his client. The focus in this regard is the act of mining by the receiving attorney. This view leads to the conclusion that the mining of metadata is ethically prohibited. The second view holds that the duty to protect the confidentiality between the sending attorney and his client falls on the shoulders of the sending attorney, rather than the receiving attorney. The focus here is on the sending attorney's duty to preserve client confidentiality. This view also emphasizes that, absent a clear prohibition of metadata mining in the rules of professional conduct, finding such conduct to be ethically impermissible would discipline attorneys for doing what in other respects would be laudable-zealously representing their clients. This view leads to the conclusion that the mining of metadata is not ethically prohibited. Both views are supported by reasonable interpretations of the applicable language of each jurisdiction's ethical rules. As such, one is hard-pressed to find that one view is more "correct" than the other.

Regardless of the "correctness" of a particular view, this Article propounds that having two inopposite and completely contradictory views in terms of what is ethically permissible and prohibited in an area such as the electronic exchange of documents, something that occurs not only on a daily basis between attorneys in the same state, but also between attorneys in

different states, is an undesirable [*180] situation. Recognizing this as an untenable situation in the legal profession, this Article looks to the Federal Rules of Civil Procedure and the inadvertent disclosure of confidential material in the formal discovery context, and proposes a parallel practical solution to the ethical conundrum surrounding metadata in the non-formal discovery context. This practical solution suggests the voluntary use of bi or multilateral agreements amongst attorneys engaged in the exchange of electronic documents outside of the formal discovery context as a practical means to ensure a uniform approach with regard to the mining of metadata by attorneys. It also suggests the use of unilateral notices as a means by which an attorney may preclude the mining of metadata contained in electronic documents transmitted to another attorney, even in the event the receiving attorney is located in a jurisdiction where mining is ethically permissible.

B. The Ethical Dilemma

Judging from the numerous articles that discuss electronic discovery and metadata in legal periodicals such as Bar Journals,¹⁰ the many Continuous Legal Education seminars offered on the subject,¹¹ and the fact that the ABA and thirteen state bar associations have issued advisory opinions discussing the ethics of electronic discovery and metadata since 2001,¹² the notion that metadata presents a [*181] special ethical challenge is no longer a novel concept

¹⁰ See Steven Nichols, Metadata Minefield, Utah Rules, Utah B.J., Sept.- Oct. 2009, at 14; Hunter H. Twilford, III & John T. Rouse, E-Discovery and the Ethics of Metadata, Miss. Law. May-June 2008, at 14; David Hricik & Chase Edward Scott, Metadata: Ethical Obligations of the Witting and the Unwitting Recipient, Ga. B.J., Apr. 2008, at 30; Mark E. Porada, Ethics and Metadata: The Pitfalls of Digging Too Deeply, 24 Me. Bar. J. 86 (2009); H. Craig Hall, Jr., Dealing with Metadata in the Non-Discovery Context, Utah B.J., Mar.-Apr. 2008, at 24; Nicole O'Neal, Metadata: The Future Impact of Invisible Data in E-Discovery on Florida, Fla. B.J., Dec. 2007, at 21; James T. Yand, The Mining of Metadata-Navigating the Hidden Ethical Dangers of Discovering Hidden Information in Electronic Documents, 62 Wash. St. B. News 12 (2008). See also Hricik & Scott, supra note 4, and Metadata: The Ghosts Haunting e- Documents, supra note 5. It is interesting to note, and another indication of the emergence of this issue, that nine metadata articles have appeared in Bar Journals, periodicals written primarily by and for practicing lawyer since 2007. A search for similar metadata ethics articles before 2007 produced no results. Search for Metadata Ethics, Heinonline, <http://heinonline.org> (last performed July 7, 2010).

¹¹ Lorman Education Services has, for example, offered a continuing legal education teleconference focusing on the ethical issues surrounding metadata for the past several years. See Robert D. Brownstone, Metadata Scrubbing and Mining: Legal, Ethical and Practical Implications, Lorman Education Services (Aug. 17, 2010), <http://www.lorman.com/teleconference/386456?&pc=18103> (last visited Nov. 11, 2010); Lorman Education Services, http://www.lorman.com/bookstore/bookstore_details.php?sku=385741 (last visited Nov. 11, 2010) (resource library for past conference); Lorman Education Services, http://www.lorman.com/bookstore/bookstore_details.php?sku=385131 (last visited Nov. 11, 2010) (resource library for past conference).

¹² The thirteen state bar associations, (counting the District of Columbia) that have issued ethics opinions pertaining to ethics and metadata are: Alabama, Arizona, Colorado, District of Columbia, Florida, Maine, Maryland, Minnesota, New Hampshire, New York, Pennsylvania, Vermont, and West Virginia. See Ala. Op. 2007-02, supra note 7; Ariz. Ethics Op. 07-03 (Nov. 2007), <http://www.myazbar.org/Ethics/opinionview.cfm?id=695> (last visited Nov. 11, 2010) [hereinafter Ariz. Op. 07-03]; Colo. State Bar Ass'n Comm'n on Ethics, Ethics Op. 119 (May 17, 2008), <http://www.cobar.org/index.cfm/ID/386/subID/23789/CETH/> (last visited Nov. 11, 2010) [hereinafter Colo. Op. 119]; D. C. Bar Legal Ethics Comm'n, Ethics Op. 341 (Sept. 2007), <http://www.dcbar.org/> for lawyers/ethics/legal ethics/opinions/opinion341.cfm (last visited Nov. 11, 2010) [hereinafter D.C. Op. 341]; Fla. Ethics Op. 06-02 (Sept. 15, 2006), <http://www.floridabar.org/tfb/tfbetopin.nsf/SearchView/ETHICS,+OPINION+06-2?opendocument> (last visited Nov. 11, 2010) [hereinafter Fla. Op. 06-02]; Me. Prof'l Ethics Comm'n, Op. No. 196, (October 21, 2008), <http://www.maine.gov/tools/whatsnew/index.php?topic=e-bar> overseers ethics opinions&i d=63338&v=article (last visited Nov. 11, 2010) [hereinafter Me. Op. 196]; Md. State Bar Ass'n Comm'n on Ethics Op. 2007-09 (Oct. 19, 2006), <http://icw.lexisnexis.com/applieddiscovery/LawLibrary/CourtRulesArticles/MarylandEOonMetadata.pdf> [(last visited Nov. 11, 2010) hereinafter Md. Op. 2007-09]; Minn. Lawyers Prof'l Responsibility Bd. Op. No. 22 (March 26, 2010),

to lawyers. Bar Associations, lawyers, academicians, and commentators, however, still grapple with what is the correct ethical approach to this emerging issue.¹³

The problem confronting the profession is simple: Should a lawyer, who receives an electronic document from another lawyer outside the realm of a court sanctioned or supervised discovery process, be able to look beyond the visible text of the document by using computer technology to "mine" its metadata? Such metadata could reveal non- visible information contained within the text of the document, information that could be regarded as confidential or privileged.

Thirteen state bar ethics commissions and the ABA have sought to provide guidance on this issue.¹⁴ The result, however, can be characterized as myopic, with no consensus having emerged among the various jurisdictions. In fact, as if to emphasize the discord among the legal profession as a whole, the opinions have been uniformly inconsistent, each subsequent opinion rejecting the approach of the immediately preceding opinion.¹⁵

[*182]

Although diversity of thought could be celebrated as a reminder that we remain a union of sovereign states, thus arguably making differing approaches to certain ethical issues acceptable, the ethics of metadata and electronic discovery is not one of those issues. Unlike, for example,

<http://lprb.mncourts.gov/rules/LPRBOpinions/Opinion%2022.pdf> (last visited Nov. 11, 2010) [hereinafter Minn. Op. 22]; N. H. Bar Ass'n Ethics Comm. Op. 2008- 2009/4 (April 16, 2009), <http://www.nhbar.org/uploads/pdf/EthicsOpinion2008-9-4.pdf> (last visited Nov. 11, 2010) [hereinafter N.H. Op. 2008-2009/4]; N.Y. State Bar Ass'n Comm. on Prof'l Ethics Op. 749 (Dec. 14, 2001), <http://www.nysba.org/AM/Template.cfm?Section=EthicsOpinions&TEMPLATE=/CM/ContentDisplay.cfm&CONTENTID=6533> (last visited Nov. 11, 2010) [hereinafter N.Y. Op. 749]; Pa. Bar Ass'n Formal Op. 2007-500 (Nov. 20, 2007) (on file with the author), [hereinafter Pa. Op. 2007-500]; Vt. Op. 2009-1, *supra* note 7; W. Va. Lawyer Discipline Legal Ethics Op. 2009-1 (June 10, 2009), <http://www.wvdc.org/pdf/lei/LEI%2009-01.pdf> (last visited Nov. 11, 2010) [hereinafter W. Va. Op. 2009-01]. In addition, the American Bar Association and the New York County Lawyers Association have issued ethics opinions on metadata. See *infra* notes 20, 107. The ABA opinion and the various state and the District's opinions are discussed *infra* in the chronological order they were issued, with the exception that the two metadata opinions issued by Pennsylvania are discussed together.

¹³ Emerging and quickly developing technology has historically presented ethical dilemmas for the profession as a whole. The challenges the Bar is facing today with the confluence of ethics and metadata in electronically exchanged documents is similar to the challenges the legal profession faced with the development of facsimile and mobile telephone communications. See generally Steele, *supra* note 1, at 929-32 (discussing state bar associations ethical guidance in response to emerging communication technologies such as facsimile, email, and cell telephone usage).

¹⁴ See *supra* text accompanying note 12.

¹⁵ The ethical opinions issued on this topic have been chronologically consistent in their differing conclusions. New York, in 2001, working under the now replaced Rules of Professional Conduct, first opined that mining is impermissible, the ABA next held mining is permissible, Florida said no, Maryland said yes, Alabama adopted the New York and Florida approach while the District of Columbia followed, adopting the ABA mindset. The District of Columbia was, naturally, followed by Arizona adhering to the you-may-not-mine philosophy. Arizona in turn was followed by Pennsylvania who chose an approach that could possibly be termed you-may-mine or you- may-choose-not-to-mine. Colorado followed Pennsylvania and adopted the ABA approach that mining is permissible. Finally, just as if to continue this perfect flip-flop symmetry, the final five opinions, Maine, New Hampshire, West Virginia, Vermont, and Minnesota, continue this trend of jurisdictions examining the same issue reaching opposite conclusion with Maine and New Hampshire prohibiting mining, West Virginia somewhat ambivalently permitting mining, while Vermont, the last state to issue an opinion in 2009, concluded that mining is permissible. Minnesota, the first (and as of August 2010 the only) state to issue a metadata ethics opinion in 2010, while affirming the duty of safeguarding confidential material when sending electronic documents, declined to provide guidance to the receiving attorney in terms of searching for metadata. See discussion *infra*, Part II.

differing ethical approaches with regard to a general issue such as a lawyer's relation with the media,¹⁶ or a very specific issue such as whether a prosecutor has a duty to ensure a defendant is advised of his or her constitutional rights,¹⁷ both of which only affect intra-state conduct, the exchange of electronic documents by its nature reaches across state boundaries. The ethical concerns surrounding the potential mining of metadata is an area that directly affects inter-state conduct.

Admittedly, much of the exchange of electronic documents occurs between attorneys in the same jurisdiction. Attorneys practicing in one of the thirteen jurisdictions that have provided guidance on the ethics of metadata will (or should) be aware of their ethical obligations, and that of opposing counsel, when transmitting and receiving electronic documents containing metadata. However, the exchange of electronic documents is also very likely to cross jurisdictional borders and an attorney's ethical obligations will, as a result, be governed by the divergent and contradictory ethics opinions that have been issued by various state bar associations with regard to the mining of metadata. Thus, it is likely, if not certain, that on a daily basis, electronic documents are, for example, transmitted [*183] between attorneys in Arizona and attorneys in Colorado. The attorneys in Arizona may not mine documents received from attorneys in Colorado. The attorneys in Colorado, on the other hand, not only may mine the electronic documents received from Arizona attorneys, but in furtherance of their zealous advocacy for their clients, may be expected to mine those documents.¹⁸ Similarly, attorneys licensed in the thirty-eight jurisdictions that have yet to issue ethics opinions addressing metadata may very well look to the ABA's view that under the Model Rules, mining of metadata is ethically permissible,¹⁹ and decide to mine documents received from attorneys in New York,

¹⁶ For example, the Model Rules, Illinois, Iowa, and Mississippi, all address the ethically permissible parameters pertaining to attorneys discussing cases with the media in their respective versions of Model Rule 3.6-Trial Publicity. Although discussing the same issue, these jurisdictions differ from each other in varying respects, as well as from the Model Rules. See Model Rules of Prof'l Conduct R. 3.6 (2009); Ill. Rules of Prof'l Conduct R. 3.6 (2010), available at <http://www.state.il.us/court/SupremeCourt/Rules/ArtVIII/defaultNEW.asp> (last visited Nov. 11, 2010) (language identical to the Model Rules version); Iowa Rules of Prof'l Conduct R. 3.6 (2005), available at <http://www.iowacourts.gov/wfdata/frame2395-1066/File3.pdf> (last visited Nov. 11, 2010) (sub-section (e) is an addition to the Model Rules version); Miss. Rules of Prof'l Conduct R. 3.6 (2005), available at <http://www.mssc.state.ms.us/rules/msrulesofcourt/rules> of professional conduct.pdf (last visited Nov. 11, 2010) (substantive differences from the Model Rule).

¹⁷ Model Rule 3.8(b), for example, makes it mandatory for a prosecutor to "make reasonable efforts to assure that the accused has been advised of the right, and the procedure for obtaining counsel" Model Rules of Prof'l Conduct R. 3.8. Hawaii and Ohio, on the other hand, omit this sub-section from their rules. See Haw. Rules of Prof'l Conduct R. 3.8 (2002), available at <http://www.state.hi.us/jud/ctrules/hrpcond.htm> (last visited Nov. 11, 2010); Ohio Rules of Prof'l Conduct R. 3.8 (2007), available at <http://www.supremecourt.ohio.gov/LegalResources/Rules/ProfConduct/profConductRules.pdf> (last visited Nov. 11, 2010). Ohio notes in a comparison to the Model Rules that section (b) is deleted partly "because ensuring that the defendant is advised about the rights to counsel is a police and judicial function" Ohio Rules of Prof'l Conduct R. 3.8. Regardless of the reason for the divergent rules, the ethical duty is one that involves conduct affecting only intra-state conduct. Divergent ethical guidance in such an area can thus not cause conflict among two attorneys in different jurisdictions working on the same case. This is in complete contrast to the ethical duties pertaining to metadata contained in electronically exchanged documents between attorneys in different jurisdictions, inter-state transmissions.

¹⁸ See discussion *infra*.

¹⁹ See ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 06- 442,(2006), <http://www.pdfforallawyers.com/files/06442.pdf> (last visited Nov. 11, 2010) [hereinafter ABA Op. 06-442] .

²⁰ Florida, ²¹ Alabama, ²² Arizona, ²³ Maine, ²⁴ and New Hampshire; ²⁵ states that have unequivocally banned that practice.

The existence of such dissimilar and inapposite ethical guidelines for the same conduct is far from desirable. Judging from the differing ethics opinions that have emerged from various state bar associations, it may, however, be an inevitable result. This is not because any one jurisdiction's approach is per se wrong or per se right. In fact, with the exception of some noticeable pre-ordained outcomes resulting from the initial framing of the issue, ²⁶ most ethics opinions are soundly and logically argued. Different ethics commissions simply reach different conclusions.

It may very well be that the varying outcomes by equally dedicated ethics committees point to the fact that the mining of metadata simply presents a situation wherein technology has transcended the applicability of certain Rules of Professional Conduct that were written for an era prior to the current ease and use of electronic document exchange. There is no reason to believe that if one were to wait for the remaining thirty-eight jurisdictions to issue their metadata ethics opinions, the legal profession as a whole would be presented with greater ethical uniformity than what has been provided by the ethics opinions issued as of 2010. Rather, judging from the see-saw approach of the current ethics opinions, ²⁷ the end [*184] result is likely to be a patchwork of approaches wherein some jurisdictions permit mining under all circumstances, some under limited circumstances, some never, and some leaving it up to the individual attorneys to determine the proper approach given the circumstances of a particular situation. Although this may be acceptable for some ethical issues, it is not acceptable for a subject matter that by its very nature involves the exchange of documents between attorneys in different jurisdictions; a situation that invariably involves opposing counsels working on the same matter while being governed by different, and in some instances, completely opposite ethical rules.

²⁰ See N.Y. Op. 749, *supra* note 12. Note, however, that with New York adopting the New York Rules of Professional Conduct in 2009, the mining of metadata is arguably no longer ethically prohibited in New York. See *infra* text accompanying note 293.

²¹ See [Fla. Op. 06-02](#), *supra* note 12.

²² See Ala. Op. 2007-02, *supra* note 12.

²³ See Ariz. Op. 07-03, *supra* note 12.

²⁴ See Me. Op. 196, *supra* note 12.

²⁵ See N.H. Op. 2008-09/4, *supra* note 12.

²⁶ The New York metadata ethics opinion arguably presents the starkest example of a pre-ordained outcome based upon how the initial question was framed. See N.Y. Op. 749, *supra* note 12.

²⁷ By happenstance, with almost perfect symmetry, each metadata ethics opinion adopted the opposite view of the immediately preceding opinion. Thus, New York (12/01) prohibited mining, the ABA (8/06) permitted mining, Florida (9/06) prohibited, Maryland (10/06) permitted, Alabama (3/07) prohibited, the District of Columbia (9/07) (generally) permitted, Arizona (11/07) prohibited, Pennsylvania (11/07 and 4/09) permitted, Colorado (5/08) permitted, Maine (10/08) prohibited, New Hampshire (4/09) prohibited, West Virginia (6/09) ambiguously prohibited, Vermont (9/09) permitted, and Minnesota (3/10) declined to provide guidance on the ethical obligations of mining metadata. See opinions cited *supra* note 12. With regard to New York, note that with the 2009 adoption of the New York Rules of Professional Conduct, the 2001 ethics opinion prohibiting mining is, arguably, no longer supported by the language of the Rules. See sources cited, *supra* note 12.

C. The Practical Solution: Attorney Agreements

In light of this foreseeable lack of uniformity, and in light of the fact that no one side is demonstrably wrong, this Article suggests a simple solution to the problem: Counsels involved in a matter wherein documents will be electronically exchanged simply enter into an agreement detailing whether the mining of metadata is to be permitted. All metadata ethics opinions, whether they permit or prohibit mining, implicitly or explicitly acknowledge that the parties, through conduct or agreement, may remove the justifications for an ethical ban on mining, or in the latter scenario, may mandate one where none previously existed. Thus, jurisdictions that permit mining should have no objection when two or more attorneys agree not to mine the metadata in the electronic documents they exchange. Similarly, jurisdictions that permit mining only under certain circumstances do not prohibit opposing attorneys from lifting such limitations or imposing stricter limitations. Indeed, even jurisdictions that ban mining outright do so based upon notions of dishonesty stemming from the perceived surreptitious nature of mining itself. Thus, if both parties are aware of and have approved mining, it is neither dishonest nor surreptitious, and consequently should not be considered unethical. Similarly, in all jurisdictions, including those that do not find mining per se unethical, if both parties have agreed not to mine, a violation of such an agreement through subsequent mining by one party would constitute ethical misconduct in and of itself.²⁸

While the above agreements would be bi or multilateral, one attorney transmitting electronic documents could also unilaterally affect the receiving attorney's ability to mine such documents. This could be effectuated by the sending attorney including appropriate language in the "confidentiality" notice of the e-mail to which the document was attached. A paragraph expressly declaring that the sending attorney has sought to remove all confidential or privileged information contained in any metadata, that any remaining metadata that may contain confidential and privileged material was inadvertently transmitted, and that [*185] the receiving attorney does not have permission to view such information, should, in the absence of a bilateral agreement to the contrary, be sufficient under all jurisdictions' ethics opinions to prevent opposing counsel (regardless of his or her jurisdiction's view on metadata) from mining such material. When lawyers recognize the import of the various and differing opinions governing attorneys across the nation, the inclusion of a metadata disclaimer in all e-mails to which electronic documents are attached should quickly become the norm.

The suggested adoption of a wholly new and unfamiliar concept to solve a problem or concern could be characterized as novel or even unrealistic. The solution suggested by the Author, however, while innovative, is not entirely novel and certainly not unrealistic.²⁹ Rather, as is further explained in Part III of this Article, this solution looks toward a concept encapsulated in rules familiar to most, if not all practicing attorneys: the Federal Rules of Civil Procedure. The

²⁸ At the very minimum, an attorney who enters into an agreement with other attorneys as to conduct they will all abide by, and who then knowingly and deliberately breaches such conduct, would be guilty of professional misconduct as dictated by Model Rule 8.4, and specifically Rule 8.4(c) for conduct involving dishonesty, and arguably (d) for conduct prejudicial to the administration of justice. See Model Rules of Prof'l Conduct R. 8.4. (c)-(d).

²⁹ See Hricik & Scott, *supra* note 4, at 24 (discussing unintended disclosure agreements as a "less technical way to avoid the problems associated with embedded data . . .").

Federal Rules of Civil Procedure, governing attorney conduct in the realm of formal discovery, not only envision opposing counsels entering into similar agreements, but in some instances require it. The Rules, in other words, provide established guidelines for how attorneys exchanging documents outside of the formal discovery realm could draft their agreements concerning metadata. The solution suggested by the Author to what otherwise appears to be an insolvable problem is an obvious one: look to the discovery realm for guidance and solutions to metadata issues in the non- discovery realm. A careful review of all ethics opinions issued thus far on the subject suggests that this proposed solution to an otherwise intractable problem is both a workable and easily adoptable solution.

II. Metadata Ethics Opinions

A. New York: From Prohibiting to Permitting Mining

New York was the first jurisdiction to issue an ethics opinion addressing the ethical concerns surrounding metadata.³⁰ Interpreting the New York Lawyer's Code of Professional Responsibility,³¹ the New York State Bar Association Committee on Professional Ethics (N.Y. Ethics Committee), in 2001, concluded that mining was prohibited. In 2009, however, New York replaced its Code of [*186] Professional Responsibility with the New York Rules of Professional Conduct.³² As such, Rule 1.6-Confidentiality of Information,³³ replaced the language of DR 4-101-Preservation of Confidences and Secrets of a Client,³⁴ and, more importantly, Rule 4.4-Respect for Rights of Third Persons, and specifically sub-section (b) of Rule 4.4 was adopted.

³⁰ See N.Y. Op. 749, *supra* note 12. Note that this opinion was issued while New York lawyers were governed by the New York Disciplinary Rules of the Code of Professional Responsibility. The New York Code was replaced by the Model Rules- based New York Rules of Professional Responsibility, effective April 1, 2009. With the adoption of the New York Model Rules, and specifically the inclusion of unique language in the comments to New York Rule 4.4(b), a strong case can be made for the proposition that New York has moved from a jurisdiction banning the mining of metadata, to a jurisdiction that declines to make such mining a disciplinary offense. Thus, were the New York Bar Association Committee on Professional Ethics to revisit this area, a different result would very likely be the final outcome.

³¹ N.Y. Lawyer's Code of Prof'l Responsibility (2007), available at <http://www.nysba.org/Content/NavigationMenu/ForAttorneys/ProfessionalStandardsforAttorneys/LawyersCodeDec2807.pdf> (last visited Nov. 11, 2010).

³² N.Y. Rules of Prof'l Conduct (2010) (effective April 1, 2009), available at <http://www.nysba.org/Content/NavigationMenu/ForAttorneys/ProfessionalStandardsforAttorneys/RulesofProfessionalConduct.pdf> (last visited Nov. 11, 2010).

³³ N.Y. Rules of Prof'l Conduct R. 1.6(a) reads in relevant part: A lawyer shall not knowingly reveal confidential information, as defined in this Rule, or use such information to the disadvantage of a client or for the advantage of the lawyer or a third person, unless (1) the client gives informed consent, as defined in Rule 1.0(j); (2) the disclosure is impliedly authorized to advance the best interest of the client and is either reasonable under the circumstances or customary in the professional community; or (3) the disclosure is permitted by paragraph (b). Sub-section (b) contains six different exceptions when disclosure is permitted. See N.Y. Rules of Prof'l Conduct R. 1.6(b). New York Rule 1.6(a) incorporates and differs from both the New York Code's applicable predecessor language of DR 4-101 and Model Rule 1.6. See N.Y. Lawyer's Code of Prof'l Responsibility DR 4-101; Model Rules of Prof'l Conduct R. 1.6.

³⁴ DR 4-101 of the New York Code consisted of four sub-sections: (a) defined "confidence" and "secret"; (b) contained the prohibitions on disclosing confidences and secrets; (c) contained the exceptions when disclosure could be made; and (d) pertained to a lawyer's duty to ensure employees and associates do not divulge confidences and secrets. N.Y. Lawyer's Code of Prof'l Responsibility DR 4- 101. Sub-section (b) read that except when permitted by sub-section (c), "a lawyer shall not knowingly: (1) Reveal a confidence or secret of a client. (2) Use a confidence or secret of a client to the disadvantage of the

³⁵ As discussed below, while the language of New York's Rule 4.4(b) was identical to the Model Rule language, New York also adopted unique language in the comments to Rule 4.4(b). This language gives a clear indication that, with the adoption of the Rules of Professional Conduct, attorneys in New York who view and use metadata are not subject to professional discipline. ³⁶ Although the N.Y. Ethics Committee has not visited this area subsequent to the adoption of the New York Rules of Professional Conduct, were it to do so, in light of the comments to newly adopted Rule 4.4(b), it is clear that it would be compelled to repeal its ethical opinions banning mining, which were issued pursuant to the old Code of Professional Responsibility, and adopt the ABA view that mining is not ethically prohibited. New York thus provides a fascinating study of one jurisdiction's path from prohibiting to (arguably) permitting the review and use of metadata.

New York also suggested attorney agreements as a means to solve the general dilemma of inadvertently sent documents, including "emails and other [*187] electronically stored information subject to being read or put into readable form," ³⁷ a category that includes metadata. This Article thus examines both New York's ban on mining under the Code and the new mining-permitted approach under the new Rules.

When the N.Y. Ethics Committee issued N.Y. Op. 749 in 2001, the first ethics opinion to address the dilemma surrounding the electronic exchange of documents, it did so without mentioning the term "metadata." ³⁸ Although New York did not use the terminology of subsequent ethics opinions, the New York opinion is often seen as representing the view that the mining of metadata is prohibited. ³⁹ While this is correct, N.Y. Opinion 749 is not as clear as subsequent like-minded opinions, due in large part to the way the N.Y. Ethics Committee framed the issue. The process of finding and reviewing metadata was limited to "sophisticated users" who "get behind" the visible information in electronically transmitted documents. ⁴⁰ As such, the opinion

client. (3) Use a confidence or secret of a client for the advantage of the lawyer or of a third person, unless the client consents after full disclosure." *Id.* at DR 4-101(b).

³⁵ It is the language of New York's Rule 4.4(b) that is generally looked to for guidance in terms of what the ethical duties are for an attorney who receives an inadvertently sent document. The language of New York's Rule 4.4(b) is identical to the Model Rule 4.4(b), and reads in its entirety: "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." N.Y. Rules of Prof'l Conduct R. R 4.4(b). Accord Model Rules of Prof'l Conduct R. 4.4(b).

³⁶ N.Y. Rules of Prof'l Conduct R. 1.6, cmt.3 (2010) ("Because there are circumstances where a lawyer's ethical obligations should not bar use of the information obtained from an inadvertently sent document, however, this Rule does not subject a lawyer to professional discipline for reading and using that information.") (emphasis added).

³⁷ *Id.*

³⁸ N.Y. Op. 749, *supra* note 12. The New York Bar Association did, however use the term "metadata" four years later in Ethics Opinion 782 (Dec. 8, 2004) addressing the duties of a lawyer not to reveal confidential information when transmitting "documents that contain 'metadata.'" N.Y. State Bar Ass'n Comm. on Prof'l Ethics, Op. 782 (Dec. 8, 2004), <http://www.nysba.org/AM/Template.cfm?Section=Ethics+Opinions&CONTENTID=6871&TEMPLATE=/CM/ContentDisplay.cfm> (last visited Nov. 11, 2010) [hereinafter N.Y. Op. 782].

³⁹ See, e.g., Pa. Bar Ass'n Formal Op. 2009-100 (April, 2009) [hereinafter Pa. Op. 2009-100] (noting that the ABA Committee held "that it is unethical for receiving attorneys to use technology to secretly view and use metadata" and that "[t]he Professional Ethics Committees of the Florida Bar and Alabama State Bar Office of General Counsel have reached similar conclusions").

⁴⁰ N.Y. Op. 749, *supra* note 12, at 1.

ignored the possibility of a receiving attorney discovering metadata by innocuous means such as simply moving the cursor over the text of the electronic document.

Additionally, the issue of mining metadata was not addressed independently, but rather was lumped together with the placing of "bug[s]" in e-mail messages that permit the sending lawyer to learn the identity of those with whom the recipient shares the e-mail, as well as the "comments that these persons may make about it."⁴¹ Finally, in establishing the parameters of the issue examined, the N.Y. Ethics Committee pointed out that it is "unclear" how one can "block" recipients from mining metadata and that it is "virtually impossible" to make one's e-mail system "bug proof."⁴² At least with regard to the former, this is arguably no longer true because software is now available that can remove metadata from documents prior to those documents being electronically transmitted.⁴³

While the terminology and phraseology of the background section of N.Y. Op. 749 certainly foreshadowed the eventual conclusion of the N.Y. Ethics Committee, the choice of words in the question presented virtually guaranteed the outcome. The Committee did not ask whether an attorney may view metadata, but rather whether an attorney may use "technology to surreptitiously examine and trace e- [*188] mail and other electronic documents in the manner described."⁴⁴ It would be unimaginable for any state ethics committee to approve attorney conduct characterized as "surreptitious."⁴⁵ Not surprisingly, the Committee concluded that "[a] lawyer may not make use of computer software applications to surreptitiously 'get behind' visible documents or to trace e-mail."⁴⁶

The N.Y. Ethics Committee's choice of words, however, does not on its face, detract from its reasoning. The opinion did note that "new technology," presumably both the ability to mine metadata and the ability to "bug" e-mails, does potentially permit "a user [receiving attorney] to access confidential communications . . . including 'confidences' and 'secrets' within the scope of DR 4-101"⁴⁷ of the New York Lawyer's Code of Professional Responsibility, then in effect.

⁴¹ Id.

⁴² Id. at 1-2.

⁴³ See, e.g., O'Neal, *supra* note 10, at n.29 (listing "a number of software programs called 'scrubbers' that automatically remove metadata from documents").

⁴⁴ N.Y. Op. 749 *supra* note 12, at 3 (emphasis added). The exact wording of the question presented was: "May a lawyer ethically may (sic) use available technology to surreptitiously examine and trace e-mail and other documents in the manner described?" Id. at 1.

⁴⁵ The Author's, and likely a reader's, instinctive negative reaction to the word "surreptitious" is confirmed by its definition as "kept secret, esp. because it would not be approved of." The New Oxford American Dictionary 1711 (Elizabeth J. Jewell & Frank Abate eds., Oxford University Press 2001). This reaction is further confirmed by its late Middle English origin of "obtained by suppression of the truth." Id. Considering their eventual decision, it would be hard for the New York Committee on Professional Ethics to be more prescient in their choice of words in framing the issue.

⁴⁶ N.Y. Op. 749, *supra* note 12, at 4.

⁴⁷ Id. at 2. DR 4-101 (in effect at the time) defined "confidence" as "information protected by the attorney-client privilege," and "secret" as "other information gained in the professional relationship that the client has requested be held inviolate or the disclosure of which would be embarrassing or would be likely to be detrimental to the client." N.Y. Lawyer's Code of Professional Responsibility DR 4- 101(A).

Emphasizing the "strong public policy in favor of preserving . . . confidentiality," ⁴⁸ the Committee noted that the "use of technology to surreptitiously obtain information that may be protected by the attorney-client privilege, the work product doctrine or that may otherwise constitute a 'secret' of another lawyer's client," would violate both the letter and spirit of the prohibition against a lawyer engaging in conduct "involving dishonesty, fraud, deceit or misrepresentation," and of engaging in "conduct that is prejudicial to the administration of justice." ⁴⁹

Surmising that absent a direct indication to the contrary, a sending lawyer only intends for the receiving lawyer to get the "visible" document and not the material "hidden" in such a document, the N.Y. Ethics Committee looked to the area of inadvertent and unauthorized disclosure of confidential information for guidance. ⁵⁰ In doing so, the Committee noted that with regard to "inadvertent or careless" disclosure of confidential material, a balance needed to be struck between encouraging more careful conduct on behalf of the attorney possessing the material, and the duty of zealous representation on the part of the attorney who learns of [*189] such confidential material. ⁵¹ However, characterizing the disclosure of information contained in metadata as "unknowing and unwilling," as opposed to "inadvertent or careless," the Committee reasoned that "[n]o such balance need be struck . . . because it is a deliberate act by the receiving lawyer, not carelessness on the part of the sending lawyer" ⁵² that leads to the disclosure of client confidences and secrets. The Committee, in other words, fully recognized the implications of the sending attorney's actions and corresponding duties and the corresponding duties and actions of the receiving attorney. However, N.Y. Op. 749 equated the latter search and review of metadata with "surreptitious acquisition and use of confidential or privileged information." ⁵³ The opinion leaves no room for the possibility that the receiving lawyer may discover the metadata without "surreptitiously" searching for it, or for the possibility that the metadata may not include either confidential or privileged material. Painting with such broad strokes, the Committee understandably concluded with an equally broad prohibition: "A lawyer may not make use of computer software applications to surreptitiously 'get behind' visible documents or to trace e-mail." ⁵⁴

The 2001 New York ethics opinion thus framed the question in very stark and clear terms, and issued a similarly direct and easy to follow prescription. The opinion's focus on the receiving attorney may be understandable, considering the relatively unknown nature of metadata at the

⁴⁸ N.Y. Op. 749, *supra* note 12, at 2.

⁴⁹ *Id.* at 3 (quoting N.Y. Lawyer's Code of Professional Responsibility DR 1-102(A)(4), (5)). DR 1-102(A)(4) held that it is misconduct to "[e]ngage in conduct involving dishonesty, fraud, deceit, or misrepresentation," while DR 1-102(A)(5) held that it is misconduct to "[e]ngage in conduct that is prejudicial to the administration of justice." N.Y. Lawyer's Code of Professional Responsibility DR 1-102(A)(4), (5). This language is the same as the Model Rule equivalent language of Rules 8.4(c) and (d). See Model Rules of Professional Conduct R. 8.4(c)-(d).

⁵⁰ N.Y. Op. 749, *supra* note 12, at 3.

⁵¹ *Id.*

⁵² *Id.*

⁵³ *Id.*

⁵⁴ *Id.* at 4.

time, and the N.Y. Ethics Committee's combined review of the practice of planting bugs through the use of e-mail messages and the mining of non-visible material in electronic documents. In this regard, however, the opinion is as noteworthy for what it does not discuss as for what it does. While the opinion does note the need for "all lawyers to exercise care in using Internet based e-mail,"⁵⁵ N.Y. Op. 749 does not explicitly discuss the sending lawyer's duty to preserve client confidences. Subsequent ethics opinions explore both the receiving attorney's ethical duty and the sending attorney's ethical duty.⁵⁶ N.Y. Op. 749 focused solely on the actions of the receiving attorney.

Three years later, however, the N.Y. Ethics Committee did address the sending attorney's duties. The New York Lawyer's Code of Professional Responsibility mandated that a lawyer shall not knowingly "reveal a confidence or secret of a client."⁵⁷ In Ethics Opinion 782, the Committee expanded on its reasoning in Opinion 749, maintaining that "[l]awyers have a duty under DR 4-101 to use reasonable care when transmitting documents by e-mail to prevent the disclosure of metadata containing client confidences or secrets."⁵⁸ In a dramatically more [*190] nuanced opinion than N.Y. Op. 749, the Committee used the term "metadata," and acknowledged that not all metadata necessarily contains client confidences or secrets.⁵⁹ However, the Committee also noted that when confidences or secrets are contained in the metadata of electronic documents sent by one attorney to another, the consequences can be potentially devastating.⁶⁰ Consequently, the Committee noted that New York lawyers who seek to transmit documents by e-mail have a duty to "exercise reasonable care to ensure that he or she does not inadvertently disclose his or her client's confidential information."⁶¹ Concomitant with this duty, the sending lawyer also has a duty to "stay abreast of technological advances" with regard to his or her chosen means of transmission.⁶² Read alone, N.Y. Op. 749 is limited and outcome determinative. Read together, New York Ethics Opinions 749 and 782 provide a balanced view of the ethical duties of attorneys who exchange electronic documents: the

⁵⁵ Id. The opinion referenced an earlier New York ethics opinion pertaining to the use of e-mails for communication by attorneys, which noted in part that "lawyers must always act reasonably in choosing to use e-mail or . . . for confidential communications, as with any other means of communication." N.Y. State Bar Ass'n Comm. on Prof'l Ethics, Op. 709, 4-5 (Sept. 16, 1998), <http://www.nysba.org/AM/Template.cfm?Section=Ethics> Opinions&CONTENTID=6317&TEMPLATE=/CM/ContentDisplay.cfm (last visited Nov. 11, 2010) [hereinafter N.Y. Op. 709].

⁵⁶ See generally Colo. Op. 119, *supra* note 12; Pa. Bar Ass'n Formal Op. 2009-100, *supra* note 39.

⁵⁷ N.Y. Lawyer's Code of Prof'l Responsibility DR 4-101(B)(1).

⁵⁸ N.Y. Op. 782, *supra* note 38, at 3.

⁵⁹ Id. at 2.

⁶⁰ Id. The Committee gave two examples, the first being the commonly referenced situation wherein prior edits and comments in the metadata of a document amount to privileged attorney-client communications. The second example, however, concerned a criminal context wherein a "prosecutor using a cooperation agreement signed by one confidential witness may use the agreement as a template in drafting the agreement for another confidential witness," the inclusion of the name of the original cooperating witness in the metadata of the second draft thus potentially exposing "that witness to extreme risks." Id. The latter example is noteworthy because it both shows the potential dramatic effect of disclosure of confidential material, and because out of all ethics opinions on metadata, N.Y. Op. 782 is the only opinion to put the potential damage disclosure of metadata can bring in a criminal scenario.

⁶¹ Id.

⁶² Id. at 3.

sending attorney must exercise reasonable care to prevent the disclosure of metadata, and the receiving attorney may not mine, seek out, or review metadata in an electronic document.

Although N.Y. Op. 782 tempered and improved upon N.Y. Op. 749, the rationale for N.Y. Op. 749's prohibition on mining, i.e., an aversion to the perceived surreptitiousness of an attorney "get[ing] behind" an electronic document to obtain information he was not intended to see, remained intact. Considering this rationale, it seems apparent that two or more attorneys, following the guidance of New York Ethics Opinions 749 and 782 (both of which were issued under the old New York Code), could agree that the mining of any electronic documents transmitted between them would be permissible. If such an agreement existed, the act of mining by either party would no longer be surreptitious nor would it be an impermissible act of "get[ting] behind" the visible text. As such, neither N.Y. Op. 749 nor N.Y. Op. 782 would apply, and the mining of documents exchanged by those attorneys would not be deemed unethical. It is important to note that this would not be a result of the attorneys "contracting" out of an ethical obligation. Rather, the suppositions made by the N.Y. Ethics Committee in reaching the particular ethical prohibition would simply no longer apply.⁶³

The ability of New York attorneys to solve the dilemma of whether metadata can or should be mined by proactively addressing the issue in attorney created agreements has arguably been enhanced by the adoption of the New York Rules of Professional Conduct in 2009. As discussed in more detail below, the language of Model Rule 4.4(b) only requires an attorney who receives an inadvertently sent document relating to his client to notify the sender.⁶⁴ Based upon this, and in looking to the history of Model Rule 4.4(b) and prior ABA ethics opinions, the ABA in 2006 issued what subsequently became the standard-bearer opinion for the view that mining of metadata is ethically permissible.⁶⁵ Thus, when New York adopted the language of Model Rule 4.4(b) in 2009, one could surmise that if the N.Y. Ethics Committee were to revisit the metadata issue, it would likely follow the ABA approach and find that mining is ethically permissible. However, because ethics committees in jurisdictions with the same or equivalent language have reached the opposite conclusion,⁶⁶ it is only after one has examined the unique language found in the comments to New York Rule 4.4 that the conclusion can be drawn that the mining of metadata is no longer ethically prohibited in New York.

Rule 4.4(b) of both the Model Rules and the New York Rules of Professional Conduct states: "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

⁶³ An instance where attorneys might want to be able to mine electronically transmitted documents would be where the formula used to calculate data in a Word Excel datasheet was relevant to settlement negotiations.

⁶⁴ See Model Rules of Prof'l Conduct R. 4.4(b).

⁶⁵ See ABA Op. 06-442, *supra* note 19. The ABA opinion first phrased the issue as to "whether the ABA Model Rules of Professional Conduct permit a lawyer to review and use embedded information contained in e-mail and other electronic documents," and then answered that "the Rules generally permit a lawyer to do so." *Id.* at 1-2. While the ABA opinion was the first to follow the New York opinions (N.Y. Ops 749 and 782), by the date of the ABA opinion, Florida was in the process of issuing its ethical opinion, having issued its advisory opinion for comments. *Id.* at n.10.

⁶⁶ Florida, for example, although adhering to the Model Rule language of Rule 4.4(b), concluded in 2006 that mining was not ethically permissible. See *infra*.

sender."⁶⁷ The ABA interpreted this to mean that notification is the only requirement, and that in the absence of an affirmative prohibition in the Rules on viewing or using information inadvertently received, doing so with regard to metadata is ethically permissible.⁶⁸ After April 1, 2009, however, an attorney in New York no longer needs to surmise, despite the lack of a specific prohibition in the language of Rule 4.4(b), as to whether viewing or using information contained in the metadata of an inadvertently received document is ethically permissible. The comments to the rule make it clear that (1) the word "document," for the purposes of the rule, "includes e-mail and other electronically stored information subject to being read or put into readable form,"⁶⁹ a category that clearly includes metadata, and (2) that while the rule requires (only) that the lawyer promptly notify the sender, the rule "does not require that the lawyer refrain from reading or continuing to read the document."⁷⁰ In fact, the comments clarify that "[b]ecause there are circumstances where a lawyer's ethical obligations should not bar use of the information obtained from an inadvertently sent document . . . this Rule does not subject a lawyer to professional discipline for reading and using that information."⁷¹ Substantive law, procedural rules, and possible court sanctions, such as disqualification or evidence-preclusion, may all [*192] play a role in either requiring a lawyer to refrain from reviewing such material, or persuading the attorney not to review the material.⁷² However, the rule does not prohibit the review and use, i.e., mining, of metadata per se. The New York Rules of Professional Conduct, in other words, do not make the act of mining ethically impermissible. The attorney may, however, decide as a matter of "professional judgment" to "refrain from reading such documents or to return them, or both."⁷³ But, only a failure to notify the sender of the receipt of inadvertently transmitted documents constitutes an ethical violation.

New York, in the comments to Rule 4.4(b), has in essence adopted the rationale of the jurisdictions that have found the mining of metadata to be ethically permissible. New York, however (and only New York), went one step further and affirmatively suggested a solution to what the Chair of the New York State Bar Association's Committee on Standards of Attorney Conduct has termed the "dilemma" presented when "a lawyer inadvertently discloses confidential information to an adversary."⁷⁴ Rather than waiting for an inadvertent disclosure and then grappling with the correct remedy, the comments to New York's new Rule 4.4(b) suggest that "[o]ne way to resolve this situation is for lawyers to enter into agreements containing explicit provisions as to how the parties will deal with inadvertently sent documents."⁷⁵ New York, in other words, with the adoption of the Rules of Professional Conduct, not only moved from viewing the mining of metadata as being ethically impermissible to it being conduct

⁶⁷ N.Y. Rules of Prof'l Conduct R. 4.4(b); Model Rules of Prof'l Conduct R. 4.4(b).

⁶⁸ ABA Op.06-442, *supra* note 19, at 3.

⁶⁹ N.Y. Rules of Prof'l Conduct R. 4.4(b), cmt. 2 (2010).

⁷⁰ *Id.*

⁷¹ *Id.* at cmt. 3 (emphasis added).

⁷² *Id.* at cmts. 2, 3.

⁷³ *Id.* at cmt. 3.

⁷⁴ Steven C. Krane, In With the Rules, Out with the Code, N.Y. St. B.J., June, 2009, at 27.

⁷⁵ N.Y. Rules of Prof'l Conduct R. 4.4(b), cmt. 2.

which "does not subject a lawyer to professional discipline,"⁷⁶ but also pushed the envelope by affirmatively suggesting a common sense solution: preempting the dilemma caused by inadvertent disclosure through voluntary agreements between attorneys that spell out agreed upon actions, remedies, and safeguards to follow in the event such a disclosure occurs. In this regard, New York, although a late-comer to the mining-permitted view, has taken the lead in advocating a solution to the dilemma as opposed to merely finding the act of mining to be ethically permissible.

B. American Bar Association: Mining Permitted-Notice Requirement

In the half decade since New York first grappled with the ethical concerns surrounding metadata (albeit without mentioning the term itself) and issued a blanket prohibition on mining metadata, thirteen subsequent ethics opinions have been issued concerning metadata. The ABA was the first to take up the gauntlet after New York. In a 2006 opinion, the ABA Committee on Ethics and Professional Responsibility (ABA Ethics Committee), applying the Model Rules, rejected the original New York approach and concluded that the Rules generally "permit a lawyer to review and use embedded information contained in e-mail and other electronic documents."⁷⁷ The ABA approach to metadata has consistently been rejected and then lauded in an alternating fashion by subsequent state ethics [*193] opinions.⁷⁸

Like the N.Y. Ethics Committee, the ABA Ethics Committee issued a simple directive. However, the similarities between the two opinions end there. In concluding that mining was ethically impermissible under the former New York Code of Professional Responsibility, New York focused on the actions of the receiving attorney; characterizing the mining of metadata as surreptitious, dishonest, and conduct prejudicial to the administration of justice. New York, in other words, sought to prevent the dissemination of confidential material found within metadata by prohibiting the receiving attorney from mining metadata. The ABA, on the other hand, finding nothing in the Rules that supported an ethical ban on mining, sought to prevent the dissemination of confidential material at the outset and placed the burden on the sending attorney to ensure that any transmitted metadata does not contain confidential information.

The ABA Ethics Committee noted that lawyers "routinely receive electronic documents" from opponents, and that these documents "often contain 'embedded' information."⁷⁹ Possibly reflecting both the increased prevalence of electronic document exchange and a broader understanding of the accompanying technology since 2001, the ABA not only employed the

⁷⁶ Id. at cmt. 3.

⁷⁷ See ABA Op. 06-442, *supra* note 19.

⁷⁸ The ABA approach has also been strongly criticized, skewered might be an apt description, by academicians. See Colloquium, Speakers Examine Metadata Phenomenon And Explore Whether Lawyers Should Fear It, *Law. Manual on Prof'l Conduct*, June 13, 2007, at 306 [hereinafter *Colloquium*] (Professor David Hricik opined at the June 2, 2007 ABA National Conference on Professional Responsibility that metadata mining should not be permitted, and commented that "the ABA opinion is shameful").

⁷⁹ Id. at 1.

term "metadata," but also engaged in a thorough explanation of what metadata is.⁸⁰ Acknowledging that "metadata is ubiquitous,"⁸¹ the Committee noted that a sending attorney can take simple steps to minimize the inclusion of metadata in documents that are transmitted to opposing counsel.⁸² The Committee's suggestions ranged from simply turning off certain features in a word processing program when creating a document, to removing such metadata through "scrubbing" prior to the transmission of the document.⁸³

Depending upon the nature of the metadata contained within the transmitted document, the sending attorney may have an ethical obligation to follow any or all of the suggestions made by the ABA Ethics Committee. In fact, although the Model Rules do not specifically address whether a receiving attorney is permitted to mine metadata, Rule 1.6 of the Model Rules directs that "[a] lawyer shall not reveal information relating to the representation of a client" ⁸⁴ While the ABA [*194] opinion did not specifically cite Rule 1.6, it did quote the admonition of comment 16 to Rule 1.6 that "[a] lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure."⁸⁵

Contrasting the existence of a rule specifically pertaining to the sending attorney's duty not to reveal confidential information (Model Rule 1.6) with the lack of a rule governing the receiving attorney's conduct, the ABA Ethics Committee noted that "the Rules do not contain any specific prohibition against a lawyer's [sic] reviewing and using embedded information in electronic documents."⁸⁶ The Committee did, however, identify Rule 4.4(b), which addresses the duties inherent with a lawyer's receipt of inadvertently sent information, as being both "the most closely applicable rule," while also acknowledging that Rule 4.4(b) is not directly on point.⁸⁷ However, even assuming that transmitted metadata was to be categorized as "inadvertently sent,"⁸⁸ Model Rule 4.4(b) provides no guidance as to whether a receiving lawyer may review or use such material. The only guidance Rule 4.4(b) provides is that "[a] lawyer who receives a document relating to the representation of the lawyer's client and knows or reasonably should

⁸⁰ Id. at 2. The opinion mentioned information possibly contained within metadata as including: last date and time a document was saved; date accessed; owner of computer who created the document, including the date and time of creation as well as who saved it last; review and edits through so called "redline" function; and comments embedded in the document. Id. The opinion also noted that using "extraordinary investigative measures sometimes might permit the retrieval of embedded information that the provider of the electronic documents either did not know existed or thought was deleted." Id.

⁸¹ Id.

⁸² Colloquium, *supra* note 78, at 5.

⁸³ Id.

⁸⁴ Model Rules of Prof'l Conduct R. 1.6 (2010). Model Rule 1.6(a) reads in its entirety: "A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b)." Id.

⁸⁵ ABA Op. 06-442 *supra* note 19, at n.4 (quoting Model Rules of Prof'l Conduct R.1.6, cmt. 16 (2010)).

⁸⁶ Id. at 5.

⁸⁷ Id. at 3. See also Model Rules of Prof'l Conduct R. 4.4(b) ("A lawyer who receives a document relating to the representation of the lawyer's client and knows or reasonably should know that the document was inadvertently sent shall promptly notify the sender.").

⁸⁸ The ABA declined to "characterize the transmittal of metadata either as inadvertent or advertent" observing instead that "the subject may be fact specific." ABA Op. 06-442, *supra* note 19, at n.7.

know that the document was inadvertently sent shall promptly notify the sender." ⁸⁹ Rule 4.4(b) does not, nor does any other Model Rule, require the receiving attorney to return the material or to abide by any instructions the sending attorney may issue once she discovers the transmission of the metadata either by her own accord or subsequent to the receiving attorney notifying her as per Rule 4.4(b). ⁹⁰

The ABA, applying a literal interpretation of the most applicable Model Rule, and drawing an inference from the absence of rules otherwise on point, thus concluded that the Model Rules indeed "permit a lawyer to review and use embedded information contained in e-mail and other electronic documents." ⁹¹ The ABA specifically rejected the original New York approach of viewing metadata as falling "under the rubric of a lawyer's honesty," ⁹² and declined to find that a [*195] receiving lawyer who reviewed metadata violated either Model Rule 8.4(c) ⁹³ or 8.4(d). ⁹⁴ Although some subsequent ethics opinions have declined to follow the ABA's reasoning for removing metadata ethics from the rubric of dishonesty, ⁹⁵ the ABA's rationale for finding Rule 4.4(b) to be applicable by default, has also received criticism. ⁹⁶ The criticism has centered on the ABA's contention that Rule 4.4(b) simply means what it says, i.e., that in a situation where a document has been inadvertently transmitted, the only ethical requirement is for the receiving attorney to notify the sending attorney. ⁹⁷ In fact, according to the ABA, "[t]he clarity of [Rule 4.4(b)'s] requirement" led the ABA Ethics Committee to withdraw two previous Formal Ethics Opinions. ⁹⁸ One was ABA Ethics Opinion 92-368, which mandated that a lawyer, who inadvertently received material that on its face appeared to be confidential, not only had to notify the sending attorney, but also had to refrain from reviewing the material and had to abide

⁸⁹ Model Rules of Prof'l Conduct R. 4.4(b).

⁹⁰ *Id.*

⁹¹ ABA Op. 06-442, *supra* note 19, at 1-2. The ABA Committee did, however, note that the fact the rules do not require a receiving lawyer to do more than notify the sending attorney does not mean the lawyer is prohibited from doing more. In fact, the opinion specifically noted that Comment 3 to Model Rule 4.4 indicates that unless directed otherwise by applicable law, "a lawyer who receives an inadvertently sent document ordinarily may, but is not required to, return it unread, as a matter of professional judgment." *Id.* at 3.

⁹² *Id.* at 4 & n.10.

⁹³ Model Rule 8.4(c) holds that it is professional misconduct for a lawyer to "engage in conduct involving dishonesty, fraud, deceit or misrepresentation." Model Rules of Prof'l Conduct R. 8.4(c) (2010).

⁹⁴ Model Rule 8.4(d) holds that it is professional misconduct for a lawyer to "engage in conduct that is prejudicial to the administration of justice." Model Rules of Prof'l Conduct R. 8.4(d) (2010).

⁹⁵ Colorado has followed the ABA on the honesty point, however, Alabama, Arizona, and Florida have declined to follow the ABA on that issue had have emulated New York's approach. See ethics opinions, *supra* note 12.

⁹⁶ See, e.g., N.H. Op.2008-2009/4, *supra* note 12, at 5 (noting that in reference to the ABA's conclusion that the Model Rules "do not contain any specific prohibition against a lawyer's reviewing and using the embedded information contained in electronic documents," the N.H. Ethics Committee "does not ascribe to the view that the lack of an express prohibition in the Rules defines the extent of a receiving lawyer's obligation").

⁹⁷ *Id.*

⁹⁸ ABA Op. 06-442, *supra* note 19, at n.9.

by the sending attorney's instructions.⁹⁹ Faced with the clear language of Rule 4.4(b) and the withdrawal of Formal Opinion 92-368's three-part requirement, it would have been difficult for the ABA Ethics Committee to have reached on alternative conclusion in Formal Opinion 06-442.

The ABA has received harsh criticism for its opinion, with one academic going so far as to characterize it as "shameful."¹⁰⁰ The Author finds this criticism [*196] misplaced. If anything, the ABA opinion is a literal interpretation of its rules. Just as it would have been difficult for the New York Committee in 2001 to find that mining was permitted once the question was phrased in terms of "surreptitiousness," so it would have been difficult for the ABA to find that the language of recently adopted Model Rule 4.4(b) did not mean what it says: that the only affirmative requirement is notification. In addition, the ABA did note that attorneys are free to do more; the Rules simple do not require more.¹⁰¹

Additionally, the ABA also offered, as a possible solution, that attorneys could "negotiate a confidentiality agreement or, if in litigation, a protective order, that will allow her or her client to 'pull back,' the document or information contained therein."¹⁰² This is the approach offered by the Federal Rules of Civil Procedure.¹⁰³ While the ABA opinion did not specifically envision attorneys entering into bilateral agreements pertaining to the mining of metadata contained in transmitted electronic documents, such agreements do not fall far from the proposed confidentiality agreements. As such, while attorneys under the ABA view are free to mine metadata, were the attorneys to pro-actively enter into an agreement wherein both sides agreed to (1) refrain from mining metadata; (2) to remove all metadata prior to transmitting a document; and (3) that any remaining metadata is to be considered confidential material, it

⁹⁹ ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 92-368 (1992) [hereinafter ABA Op. 92-368]. ABA Op. 92-368 was withdrawn by the ABA in 2005. See ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 05-437 (2005), [https://www.lexisnexis.com/applieddiscovery/lawlibrary/CourtRulesArticles/ABA 05 437.pdf](https://www.lexisnexis.com/applieddiscovery/lawlibrary/CourtRulesArticles/ABA%2005%20437.pdf) (last visited Nov. 11, 2010) [hereinafter ABA Op. 05-437] (explaining that Rule 4.4(b), added to the Model Rules in November of 2002, "not only directly addressed the precise issue discussed in Formal Opinion 92-368, but narrowed the obligations of the receiving attorney" and that "Rule 4.4(b) thus only obligates the receiving lawyer to notify the sender of the inadvertent transmission promptly. The rule does not require the receiving lawyer either to refrain from examining the materials or to abide by the instructions of the sending lawyer"). Because ABA Op. 92-368 required refraining from viewing, notification, and abiding by the sending attorney's instructions, and Rule 4.4(b) "only obligates the receiving lawyer to notify the sender of the inadvertent transmission promptly," ABA Op. 92-368 was in conflict with the amended Rule 4.4 and the opinion therefore had to be withdrawn. See ABA Op. 05-437, *supra*, at 2. See also ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 06-440 (2006) (withdrawing a separate ethics opinion on similar grounds); ABA Op. 06-442, *supra* note 19, at n. 9.

¹⁰⁰ See *supra* text accompanying note 78.

¹⁰¹ ABA Op. 06-442 specifically noted that "[c]omment [3] to Model Rule 4.4 indicates that, unless other law requires otherwise, a lawyer who receives an inadvertently sent document ordinarily may, but is not required to, return it unread, as a matter of professional judgment." ABA Op. 06-442, *supra* note 19, at 3 (emphasis added). Comment 3 to Model Rule 4.4 reads in its entirety: 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 (2010).

¹⁰² ABA Op. 06-442, *supra* note 19, at 5.

¹⁰³ See *Fed. R. Civ. P. 26(f)*, advisory committee's note (recommending two solutions to the possible disclosure of confidential material through the exchange of documents during discovery: a quick peek arrangement and a claw back provision).

would be difficult for one side to ethically justify any subsequent mining of the other side's metadata. Not only would a knowing violation of an agreement between attorneys be deemed unprofessional,¹⁰⁴ but it would also constitute "conduct involving dishonesty, fraud, deceit or misrepresentation" in violation of Rule 8.4(c).¹⁰⁵

Similarly, a unilateral notice, included by the sending attorney in the electronic transmission indicating that she has sought to remove all confidential and privileged metadata in the attached electronic document, and that any such remaining metadata is inadvertently transmitted, would arguably have a similar, **[*197]** although admittedly not as compelling, effect. While an attorney who received an electronic document that included such a unilateral notice under the ABA Model Rules would have an affirmative obligation to notify the sending attorney of any metadata he or she discovers, the receiving attorney would only reach this stage if she deliberately ignored the sending attorney's request and affirmatively set out to discover material that has already been termed confidential by the sending attorney. Admittedly, the unilateral notification scenario would not constitute an ethical violation as clearly as would a breach of a bilateral agreement. However, it would certainly be difficult for the receiving attorney to justify her acts of mining as being ethical or professional under such circumstances.

That being said, a sending attorney who chooses to include a unilateral notice in her electronic transmissions does not in any way alleviate her duty of competence under Rule 1.1, or her duty of confidentiality under Rule 1.6. The inclusion of a unilateral notice only affects the future actions of the receiving attorney; it does not relieve the sending attorney of her duty to know when metadata may be created or how to remove such metadata, both of which are crucial if the attorney is to ensure she does not "reveal information relating to the representation of a client."¹⁰⁶

Subsequent to the ABA's metadata ethics opinion (ABA Op. 06-442) of August, 2006, twelve additional jurisdictions issued opinions in quick succession.¹⁰⁷ With lines drawn on both sides of the issue—the original New York opinion representing the view that an attorney may not view or use metadata, and the ABA opinion representing the view that, in the absence of a rule to the

¹⁰⁴ At a very minimum, such conduct would not constitute "honest dealings with others" as envisioned by the Preamble of the Model Rules, to wit "[a]s negotiator, a lawyer seeks a result advantageous to the client but consistent with requirements of honest dealings with others." Model Rules of Prof'l Conduct, pmbl.

¹⁰⁵ See Model Rules of Prof'l Conduct R. 8.4(c) (2010). Although a breach of such an agreement in the formal discovery context would also clearly constitute a violation of Rule 8.4(d) as conduct prejudicial to the administration of justice, the applicability of that sub-paragraph in the non-formal discovery context may be less tenuous.

¹⁰⁶ Model Rules of Prof'l Conduct R. 1.6.

¹⁰⁷ The ABA opinion was preceded by N.Y. Op. 749, *supra* note 12. Subsequent to the ABA opinion, Florida, Maryland, Alabama, the District of Columbia, Pennsylvania, Colorado, Maine, New Hampshire, West Virginia, Vermont, and Minnesota have issued ethics opinions pertaining to metadata. See *supra* note 12. In addition to these state metadata opinions, the New York County Lawyers Association issued an ethics opinion pertaining to the ethics of "[s]earching inadvertently sent metadata in opposing counsel's electronic documents." See N.Y. Cnty. Law. Ass'n Comm. on P r o f ' l E t h i c s , O p . N o . 7 3 8 (2 0 0 8) , <http://www.nycla.org/siteFiles/Publications/Publications11540.pdf> (last visited Nov. 11, 2010) [hereinafter NYCLA Op. 738]. Similar to N.Y. Op. 749, the NYCLA opinion held that while sending attorneys have a duty to ensure documents they send are free from metadata, a receiving attorney "may not ethically take advantage of a breach in the [sending] attorney's care by intentionally searching for this metadata." NYCLA Op. 738, *supra*, at 1.

contrary, an attorney is not prohibited from mining metadata, her only ethical obligation being to notify the sending attorney of the inadvertent transmission-these opinions fell into one of two camps: (1) Florida, Alabama, Arizona, Maine, and New Hampshire adopted the original New York prohibition against a receiving lawyer viewing or using material contained in transmitted metadata; and (2) Maryland, Colorado, and Vermont took the opposite view. Maryland in essence adopted the ABA reasoning. However, because the Maryland Rules of Professional Conduct do not contain an equivalent to Model Rule 4.4(b), Maryland does not impose the same notification requirement as the ABA. Colorado and Vermont rejected the New York view and attacked the reasoning of N.Y. Op. 749, resulting in a full and comprehensive jettison of New York's conclusion by both states. The District of Columbia also joined the mining-prohibited camp, but only if the receiving attorney has actual knowledge metadata was inadvertently sent. [*198] West Virginia, in a somewhat ambiguous opinion, seems to have followed the District of Columbia's actual knowledge approach. Pennsylvania, showing the faith entrusted to members of the Pennsylvania Bar, acknowledged the issue, explored the various jurisdictions' ethics positions, and issued two opinions, concluding that each situation is best resolved by the individual attorney using her judgment as suggested in the Preamble of the Pennsylvania Rules of Professional Conduct. Minnesota followed the Pennsylvania approach, to an extent, in that it emphasized the notice requirement, but declined to provide additional guidance in terms of whether the mining of metadata is ethically permitted.

C. Florida: Mining Prohibited

Six weeks after the ABA issued its formal ethics opinion, the Florida Bar Professional Ethics Committee (Florida Ethics Committee) issued Ethics Opinion 06- 02.¹⁰⁸ The opinion was in response to a directive by the Board of Governors of the Florida Bar to "issue an opinion to determine ethical duties when lawyers send and receive electronic documents in the course of representing their clients."¹⁰⁹ As a result, the issue presented to the Committee was both broader and more balanced than the outcome laden terminology used by the N.Y. Ethics Committee in 2001.¹¹⁰ While the Florida Ethics Committee reached the same conclusion as the N.Y. Ethics Committee, in terms of whether a receiving attorney may mine metadata, it did so in a more reasoned and balanced fashion, addressing both the sending lawyer's duties and the receiving lawyer's duties. In this regard, Fla. Op. 06-02 is more akin to the combined approach of N.Y. Op. 749 and N.Y. Op. 782, as opposed to the outcome determinative approach of N.Y. 749 standing alone.

The Florida Ethics Committee succinctly defined metadata as "information about information"¹¹¹ and made it clear that the opinion only addressed the exchange of metadata in the

¹⁰⁸ [Fla. Op. 06-02, supra](#) note 12.

¹⁰⁹ *Id.*

¹¹⁰ See *supra* text accompanying note 44.

¹¹¹ [Fla. Op. 06-02, supra](#) note 12. The Committee further adopted the Sedona Guidelines' definition of metadata as "information describing the history, tracking, or management of an electronic document." *Id.* (quoting The Sedona Guidelines: Best Practice Guidelines and Commentary for Managing Information and Records in the Electronic Age, app. f., The Sedona Conference, <http://www.thesedonaconference.org> (last visited Nov. 11, 2010) (follow "Publications" hyperlink under WGI:

non-discovery context.¹¹² Having dispensed with the preliminaries, the opinion fulfilled its mandate and looked to Florida Rules of Professional Conduct Rules 4-1.6(a),¹¹³ 4-4.4(b),¹¹⁴ and 4-1.1.¹¹⁵

[*199]

The Florida Ethics Committee noted that Rule 4-1.6(a) prohibits a lawyer from revealing "information relating to the representation of a client,"¹¹⁶ and that in order to do so, "Florida lawyers must take reasonable steps to protect confidential information in all types of documents and information that leave the lawyers' office" ¹¹⁷ As such, the sending lawyer has "an obligation to take reasonable steps to safeguard the confidentiality of all communications sent by electronic means to other lawyers . . . including information contained in metadata."¹¹⁸ The opinion did not expand further on what such "reasonable steps" would entail, either in terms of preventing the creation of metadata or in removing metadata once created in an electronic document prior to transmission.¹¹⁹ The opinion did note, however, that this obligation "may necessitate a lawyer's continuing training and education in the use of technology in transmitting and receiving electronic documents in order to protect client information under Rule 4-1.6(a)."¹²⁰

Having discussed the sending lawyer's duty, the opinion then framed "the recipient lawyer's concomitant obligation" as being "not to try to obtain from metadata information relating to the representation of the sender's client that the recipient knows or should know is not intended for

Electronic Document Retention and Production heading; scroll down to #24 and follow "RetGuide200409.pdf" hyperlink, then complete download information)).

¹¹² [Fla. Op. 06-02, supra](#) note 12. The opinion made clear that it did "not address the role of the lawyer acting as a conduit to produce documents in response to a discovery request." *Id.*

¹¹³ Florida Rule 4-1.6(a), "Confidentiality of Information," reads in full: "A lawyer shall not reveal information relating to representation of a client except as stated in subdivisions (b), (c), and (d), unless the client gives informed consent." Fla. Rules of Prof'l Conduct R. 4-1.6(a) (2010), available at <http://www.floridabar.org/divexel/rtfb.nsf/FV?Openview&Start=1&Expand=4#4> (last visited Nov. 11, 2010). Florida Rule 1.6 does not differ from Model Rule 1.6 in its prohibition against revealing client information, only in the permitted exceptions, none of which are applicable in the metadata situation.

¹¹⁴ Florida Rule 4-4.4(b) reads in full: "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." Fla. Rules of Prof'l Conduct R. 4.4(b). Florida's Rule 4.4(b) is thus identical to Model Rule 4.4(b).

¹¹⁵ Florida Rule 4-1.1 reads in full: "A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness, and preparation reasonably necessary for the representation." Fla. Rules of Prof'l Conduct R. 4-1.1. The language of the rule is identical to the language of Model Rule 1.1. See Model Rules of Prof'l Conduct R. 1.1 (2010) ("A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.").

¹¹⁶ [Fla. Op. 06-02, supra](#) note 12 (citing Fla. Rules of Prof'l Conduct R. 4-1.6(a)).

¹¹⁷ [Fla. Op. 06-02, supra](#) note 12.

¹¹⁸ *Id.*

¹¹⁹ Unlike the ABA, Florida does not discuss these or other technical aspects of metadata. See *id.*

¹²⁰ *Id.*

the recipient [lawyer]." ¹²¹ Florida and the Model Rules define "knows" as "denot[ing] actual knowledge of the fact in question." ¹²² While Florida does not define "should know," the Model Rules define "reasonably should know" as "denot[ing] that a lawyer of reasonable prudence and competence would ascertain the matter in question." ¹²³ Florida's opinion went on to state that "[a]ny such metadata is to be considered by the receiving lawyer as confidential information which the sending lawyer did not intend to transmit." ¹²⁴ Thus, the message to Florida lawyers is clear: the deliberate mining of metadata is ethically prohibited. ¹²⁵

[*200]

Florida came to the same conclusion New York reached in 2001 by finding it ethically impermissible to deliberately mine for information in metadata. Interestingly, however, Florida did so without framing the issue under the "rubric of a lawyer's honesty," as the ABA characterized the original New York approach. ¹²⁶ Indeed, while Florida reached the same conclusion as New York with regard to the deliberate mining of metadata, Florida reached the opposite conclusion of the ABA. This is despite the fact that Florida and the ABA had applied and interpreted rules with the exact same wording. The ABA declined to equate a lawyer's action of viewing or using metadata as involving the lawyer's honesty, thereby leaving out any discussion of the applicability of Model Rule 8.4. Florida, on the other hand, declined to address the ABA's view that the addition of Model Rule 4.4(b) to the Model Rules had replaced the prohibition of reviewing inadvertently received material with an affirmative duty to notify the sender of such information. Florida, in other words, skirted the ABA's conclusion that in the absence of other rules on point, the rule most relevant to a lawyer's situation must guide her ethical conduct. In fact, Florida failed to discuss ABA Op. 06-442 even though the ABA opinion was issued while Florida's opinion had been released for public comment ¹²⁷ and despite the fact that the State had adopted the language of Model Rule 4.4(b) prior to the issuance of Op.

¹²¹ Id.

¹²² Fla. Rules of Prof'l Conduct, pmbl.

¹²³ See Model Rules of Prof'l Conduct R. 1.0(j).

¹²⁴ [Fla. Op. 06-02, supra](#) note 12 (emphasis added).

¹²⁵ As under the Model Rules, in an instance of "inadvertent" discovery of information from metadata, (although not mentioned in the opinion, an example of such a discovery could result from the mere placement of the cursor over a word or section in an electronic document), the opinion looks to Florida Rule 4-4.4(b) and concludes that "the lawyer must 'promptly' notify the sender." [Fla. Op. 06-02, supra](#) note 12 (quoting Fla. Ethics Op. 93-3 (1994), <http://www.floridabar.org/tfb/tfbetopin.nsf/SearchView/ETHICS,+OPINION+93-3?opendocument> (last visited Nov. 11, 2010), which held that in cases of receipt of confidential information "as a result of an inadvertent release" the lawyer must notify the sender)). The language of Florida Rule 4.4(b) is the same as the language of Model Rule 4.4(b).

¹²⁶ See *supra* note 19.

¹²⁷ See ABA 06-442, *supra* note 19, at n.10 (noting that the proposed version of Fla. Op. 06-02 (June 23, 2006) had been submitted for comment by the time of the issuance of the ABA opinion). There is some confusion with regard to the footnote citation within the ABA opinion in that the opinion itself was issued on August 5, 2006, yet footnote 10 of the ABA opinion contains two references to websites having been visited subsequent (Sept. 15, 2006) to such date; the Florida proposed Op. 06-02 is one of these two websites. See *id.*

06-02.¹²⁸ This does not, of course, imply that Florida's opinion is incorrect or outcome determinative. It does, however, lend credence to the argument that regardless of whether one approves of the ABA opinion or not, its conclusion was the result of a logical application of the applicable rules in effect at the time.

Nevertheless, just as two attorneys under the ABA approach could agree not to mine, attorneys under Florida's approach could also agree that mining is permissible. Again, such a bilateral agreement would not constitute the attorneys contracting out of an ethical obligation derived from their rules of professional conduct. Rather, the Florida Ethics Committee's rationale for prohibiting mining focused on the intent of the sending attorney. In other words, as noted above, Florida concluded that "metadata is to be considered by the receiving lawyer as confidential information which the sending lawyer did not intend to transmit."¹²⁹ If two lawyers agreed that metadata contained in documents electronically transmitted between them was intentionally included, no basis for prohibiting the review of such metadata would exist. This is similar to the conclusion that even under the New York anti- mining stance, if the mining is done openly and with the approval of both attorneys, it would not be surreptitious, thereby removing the N.Y. [*201] Ethics Committee's 2001 rationale for prohibiting mining. In Florida, as in New York, a bilateral agreement would remove any notions of surreptitiousness and/or issues regarding the intent of the sending attorney. Under this scenario, mining would not be unethical in either state. Even so, because a Florida lawyer who inadvertently comes across information in metadata that "the recipient knows or should know was not intended for the recipient" must "promptly notify the sender,"¹³⁰ it would seem to follow that a receiving Florida lawyer also must notify the sending lawyer if he comes across similar confidential material through mutually permitted deliberate mining.

Although a bilateral agreement would permit both parties to mine in Florida, a unilateral notice by one party that he will mine all received electronic documents would not permit him to mine such documents. In other words, while a sending attorney in a jurisdiction that permits mining could unilaterally provide the receiving attorney notice that the documents he sends have been scrubbed of metadata and that any remaining metadata is inadvertently included and should be considered confidential material, a receiving attorney in a jurisdiction that prohibits mining cannot unilaterally provide the sending attorney with a notice that he intends to mine any received documents and then ethically mine such metadata. The intent of the sending attorney is not altered by a notice from the receiving attorney. The rationale underlying the Florida ban on mining would remain, and the receiving attorney would still be prohibited from mining metadata in electronic documents.

D. Maryland: Mining Permitted-Notice Not Required

A month after Florida concluded that the mining of metadata was ethically prohibited, Maryland issued an ethics opinion that took the opposite view. On October 19, 2006, the Maryland State

¹²⁸ Sub-section (b) of Florida Rule 4.4 was adopted on March 23, 2006 and went into effect on May 22, 2006, prior to the issuance of Fla. Op. 06-02 on September 15, 2005. Florida Rule 4.4, prior to May 22, 2006, did not contain sub- section (b). See [In re Amendments to the Rules Regulating the Fla. Bar, 933 So. 2d 417, 471-72 \(Fla. 2006\)](#); Fla. Rules of Prof'l Conduct R. 4.4(b).

¹²⁹ [Fla. Op. 06-02](#), *supra* note 11.

¹³⁰ See *supra* text accompanying note 125.

Bar Ethics Committee (Maryland Ethics Committee) issued Opinion 2007-09 regarding the ethical duties of attorneys and the transmittal of metadata.¹³¹ In a relatively succinct opinion, Maryland found that "there is no ethical violation if the recipient attorney . . . reviews or makes use of metadata without first ascertaining whether the sender intended to include such metadata."¹³² Without referencing ABA Op. 06-442, the Committee noted that the ABA had adopted Model Rule 4.4(b) in 2002.¹³³ Looking to ABA Ethics Opinion 05-437,¹³⁴ which in the wake of the adoption of Model Rule 4.4(b) found that a lawyer receiving inadvertently sent material is only required to notify the sending lawyer, and thus not prohibited from reviewing metadata, nor required to abide by the sending lawyer's instructions, the Committee noted that the Maryland Rules [*202] had not been amended to include Model Rule 4.4(b).¹³⁵ Consequently, the Committee concluded that a receiving attorney was not ethically prohibited from mining metadata.¹³⁶ Additionally, and again noting the absence of an equivalent to Model Rule 4.4(b) in Maryland, the Committee also concluded that the Maryland Rules "do not require the receiving attorney to notify the sending attorney that there may have been an inadvertent transmittal of privileged (or, for that matter, work product) materials."¹³⁷

In terms of the sending attorney's duties, the Maryland Ethics Committee, in answering the question of whether a sending attorney has a duty to remove metadata prior to transmitting a file,¹³⁸ looked to Rule 1.1-Competence and Rule 1.6-Duty not to Reveal Confidential Information, and concluded that "the sending attorney has an ethical obligation to take reasonable measures to avoid the disclosure of confidential or work product materials embedded in the electronic discovery."¹³⁹

¹³¹ Md. Op. 2007-09, *supra* note 12.

¹³² *Id.* at 1-2. In terms of the receiving attorney, the Maryland Committee answered and discussed two inquiries together, namely (1) whether a receiving attorney could ethically review and use metadata produced by another party, and (2) whether a receiving attorney had an ethical duty not to use or review metadata without first ascertaining if such metadata was inadvertently included. *Id.* at 1.

¹³³ *Id.* at 2.

¹³⁴ ABA Op. 05-437, *supra* note 99.

¹³⁵ Md. Op. 2007-09, *supra* note 12, at 2. Maryland Rule 4.4, like the ABA Model Rule 4.4, consists of two parts: sub-section (a) prohibits a lawyer in representing a client from using means that have no other purpose than embarrass a third party; sub-section (b) addresses a lawyer not seeking to obtain protected information when dealing with a third party. See Md. Rules of Prof'l Conduct R. 4.4 (2010), available at <http://www.law.cornell.edu/ethics/md/code/> (last visited Nov. 11, 2010). Maryland Rule 4.4(b) thus does not replicate the Model Rule 4.4(b) notice requirement. See *id.* Maryland Rule 4.4(b) reads in its entirety: In communicating with third persons, a lawyer representing a client in a matter shall not seek information relating to the matter that the lawyer knows or reasonably should know is protected from disclosure by statute or by an established evidentiary privilege, unless the protection has been waived. The lawyer who receives information that is protected shall (1) terminate the communication immediately and (2) give notice of the disclosure to any tribunal in which the matter is pending and to the person entitled to enforce the protection against disclosure. *Id.*

¹³⁶ Md. Op. 2007-09, *supra* note 12, at 1-2.

¹³⁷ *Id.* at 2. (parenthesis in original).

¹³⁸ *Id.* at 1.

¹³⁹ *Id.* at 3. Maryland Rules 1.1 and 1.6(a) are identical to the Model Rules. See Md. Rules of Prof'l Conduct R. 1.1 ("A lawyer shall provide competent representation to a client. Competent representation requires knowledge, skill, thoroughness and preparation reasonably necessary for the representation"); Md. rules of Prof'l Conduct R. 1.6(a) ("A lawyer shall not reveal

The Maryland Ethics Committee thus followed the reasoning of ABA Op. 06-442. Applying this reasoning to the absence of Rule 4.4(b) in Maryland, however, the Committee not only found that Maryland lawyers receiving metadata may review such material, but also that they are not obligated to notify a sending attorney of such receipt.¹⁴⁰ While this is a logical application of the ABA's reasoning, it also takes the ABA reasoning a step further. In other words, the ABA viewed the implementation of Rule 4.4(b) and the subsequent withdrawal of ABA [*203] Op. 92-368¹⁴¹ as support for its view that Rule 4.4(b) preempted any other possible ethical requirements. As such, the ABA reasoned, since Rule 4.4(b) only requires notice, that is the limit of the receiving attorney's ethical duty. Maryland, not having a similar prior requirement, looked to the absence of a Rule 4.4(b) equivalent as support for its conclusion that there is neither a notice requirement, nor a duty to refrain from viewing or abiding with a sending attorney's instructions in Maryland. And, unlike New York, Maryland did not consider a receiving lawyer's review of metadata to fall within the "rubric of a lawyer's honesty."¹⁴² Following the logic of the Maryland Ethics Committee, there is no basis for finding an ethical violation on the part of an attorney who mines inadvertently transmitted metadata.

Maryland did, however, include in its ethics opinion a discussion of how the then soon to be implemented Federal Rules of Civil Procedure could potentially impact a lawyer's "lack of an ethical obligation to notify the sender or to return the privileged or work-product documents to the sender."¹⁴³ The Maryland Ethics Committee specifically noted that the (at the time proposed) Federal Rules 16(b)(5)-(6) would require the parties to, among other things, attempt to reach agreements dealing with privileged or protected material produced through discovery, and that Rule 26(b)(5) governed the duties of attorneys where documents subject to privilege claims had been produced.¹⁴⁴ The Committee warned that a failure to abide by a Rule 16 agreement or a failure to abide by the provisions of Rule 26(b)(5) may constitute a violation of Rule 8.4(b), as it could be construed to be conduct prejudicial to the administration of justice.¹⁴⁵ While Maryland was not the only jurisdiction to note that a lawyer's duties may change depending upon whether they are in a discovery phase or outside of a discovery phase when transmitting electronic documents,¹⁴⁶ Maryland is the only jurisdiction to emphasize the

information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).").

¹⁴⁰ The Maryland Commission did, however, note that "the receiving lawyer can, and probably should, communicate with his or her client concerning the pros and cons of whether to notify the sending attorney and/or take such other action which they believe is appropriate." Md. Op. 2007-09, *supra* note 12, at 2.

¹⁴¹ See *supra* text accompanying note 99.

¹⁴² See ABA Op. 06-442, *supra* note 19, at 4.

¹⁴³ Md. Op. 2007-09, *supra* note 12. The pertinent amendments to the Federal Rules were set to go into effect on December 1, 2006, four months after the issuance of the opinion.

¹⁴⁴ *Id.* at 23.

¹⁴⁵ Md. Op. 2007-09, *supra* note 12. While the text of Md. Op. 2007-09 references Rule 8.4(b) in the discussion of the possible result of violating a Rule 16(b)(6) agreement, the discussion makes it clear the opinion meant Rule 8.4(d), i.e., conduct prejudicial to the administration of justice as opposed to committing a criminal act. See *id.*

¹⁴⁶ Alabama and the District of Columbia also recognized the non-discovery and formal discovery distinction in this regard. See *infra* notes 159, 202 and accompanying text.

potential significance Rule 16(b)(6) agreements may play with regard to the everyday exchanges of electronic documents.¹⁴⁷

As with any jurisdiction that permits the mining of metadata, two attorneys in Maryland could presumably enter into a bilateral agreement that provided neither would mine the other's transmitted electronic documents for metadata. Maryland attorneys would thus fall into the same scenario as would attorneys guided by the ABA Model Rule approach. While Maryland may not have adopted an equivalent [*204] to Model Rule 4.4(b), it has adopted the equivalent to Model Rule 8.4(c)-(d).¹⁴⁸ Presumably, an attorney who enters into an agreement with another attorney would have a professional duty to honor such an agreement under the Maryland rules or under the Model Rules. However, unlike an attorney working under the Model Rules, an attorney bound by the Maryland rules would not be required to notify the other attorney, (absent a clause to the contrary in the bilateral agreement), were he to inadvertently discover confidential material even while abiding by the bilateral agreement because Maryland lacks an equivalent to Model Rule 4.4(b). Having said this, Maryland attorneys, like all attorneys, are free to do more than that minimally prescribed by the Rules of Professional Conduct. As such, the Maryland Ethics Committee specifically cited to comment 3 to Model Rule 4.4 in acknowledging that an attorney's professional judgment may dictate that he take additional action.¹⁴⁹

Just as bilateral agreements could be used by Maryland attorneys to prevent the mining of metadata, so could a unilateral notice be used by a Maryland attorney to, if not prevent, at least clarify to the opposing attorney that electronically transmitted documents should not be mined.¹⁵⁰ Again, unlike an attorney under the Model Rules, a Maryland attorney would not be bound by the notification duty were he to come upon confidential material despite having entered into a unilateral agreement not to mine metadata.

E. Alabama: Mining Prohibited

Approximately six months after Florida and Maryland issued metadata ethics opinions the Disciplinary Commission of the Alabama Office of General Counsel (Alabama Commission) issued Alabama State Bar Ethics Opinion 2007-02.¹⁵¹ The Alabama ethics opinion set out to answer two questions: (1) whether "an attorney [has] an affirmative duty to take reasonable precautions to ensure that confidential metadata is properly protected from inadvertent or inappropriate production via an electronic document before it is transmitted";¹⁵² and (2)

¹⁴⁷ ABA Op. 06-442 did suggest lawyers consider negotiating confidentiality agreements as well. ABA Op. 06-442, *supra* note 19, at 5. Maryland, however, specifically referenced to Federal Rule 16(b)(6) agreements. *Id.* at 3.

¹⁴⁸ The language of Maryland Rule 8.4(c)-(d) is identical to its Model Rule counterpart in that a lawyer may not "engage in conduct involving dishonesty, fraud, deceit or misrepresentation" or "engage in conduct that is prejudicial to the administration of justice." Md. Rules of Prof'l Conduct R. 8.4(c)-(d); Model Rules of Prof'l Conduct R. 8.4(c)-(d).

¹⁴⁹ Md. Op. 2007-09, *supra* note 12, at n.1.

¹⁵⁰ See *supra* for a discussion pertaining to unilateral notices under Model Rule environment.

¹⁵¹ Ala. Op. 2007-02, *supra* note 7.

¹⁵² *Id.* at 1 (emphasis added).

whether it is "unethical for an attorney to mine metadata from an electronic document he or she receives from another party." ¹⁵³ Both questions were answered in the affirmative.

After framing the issue, the opinion noted that "[t]he recent proliferation of electronic discovery, e-filing, and the use of e-mail has created an ethical dilemma surrounding the disclosure and mining of metadata." ¹⁵⁴ The opinion provided two fairly typical examples of how such ethical dilemmas can occur. The first was an attorney who transmits an electronic document without realizing that, absent "scrubbing," invisible comments may be made visible to a receiving attorney who [*205] subsequently "mines" the document. ¹⁵⁵ The second example involved the use of templates or copies of documents in existing client files to produce a similar document for another client, the danger being that an "opposing party could mine the document and discover the original client's name and information." ¹⁵⁶

The Alabama Commission's starting point was Rule 1.6-Confidentiality of Information. Alabama Rule 1.6 is substantially the same as Model Rule 1.6. ¹⁵⁷ According to Alabama Rule 1.6, an Alabama lawyer may not "reveal information relating to representation of a client," except when done in relation to the representation or as exempted by the Rule. ¹⁵⁸ The comment to Alabama Rule 1.6 explains that Alabama lawyers have an ethical obligation "to hold inviolate confidential information of the client." ¹⁵⁹ The Commission cited these rules and noted that the comment to Alabama Rule 1.6 maintained that "[a] fundamental principle in the client-lawyer relationship is that the lawyer maintains confidentiality of information relating to the representation." ¹⁶⁰ The Commission then concluded that the sending attorney has "an ethical duty to exercise reasonable care when transmitting electronic documents to ensure that he or she does not disclose his or her client's secrets and confidences." ¹⁶¹

In seeking to provide guidance to Alabama attorneys as to what "reasonable care" meant, the Alabama Commission noted that it would differ depending upon the circumstances of each case, the nature of the metadata, the subject matter of the document, and what steps the

¹⁵³ Id.

¹⁵⁴ Id.

¹⁵⁵ Id. at 2.

¹⁵⁶ Id.

¹⁵⁷ Ala. Op. 2007-02, supra note 7.

¹⁵⁸ Ala. Rules of Prof'l Conduct R. 1.6 (2010). Rule 1.6(a) reads: "A lawyer shall not reveal information relating to representation of a client unless the client consents after consultation, except for disclosures that are impliedly authorized in order to carry out the representation, and except as stated in paragraph (b)." Id. Neither of the two exceptions in (b) relate to metadata.

¹⁵⁹ Ala. Rules of Prof'l Conduct R. 1.6, cmt. (2010). The Comment to Alabama Rule 1.6 notes that the observance of the ethical obligation to hold client confidences "inviolates" both facilitates "the full development of facts essential to proper representation of the client" and "encourages people to seek early legal assistance." Id. See also Ala. Op. 2007-02, supra note 7, at 3.

¹⁶⁰ Ala. Op. 2007-02, supra note 7, at 3 (quoting Ala. Rules of Prof'l Conduct R. 1.6, cmt.).

¹⁶¹ Ala. Op. 2007-02, supra note 7, at 3.

sending attorney had taken to prevent disclosure of confidential material through metadata.¹⁶² These areas are generally examined in determining what type of conduct constitutes reasonable care. Alabama, however, added a unique and interesting factor to the "reasonable care" determination: the intended recipient. Possibly acknowledging that the adversarial system may get the best of some attorneys, the Commission explained that an attorney needed to "exercise greater care" when transmitting electronic documents to an adversary party, as opposed to, for example, filing such documents with a court.¹⁶³ The Commission noted "[t]here is simply a much higher likelihood that an adverse party would attempt to mine metadata, than a neutral and detached court."¹⁶⁴

In answering the second question, whether it is permissible to mine metadata in Alabama, the Alabama Commission affirmatively held that just as a sending [*206] lawyer has an ethical duty to ensure she does not transmit confidential information, a "receiving lawyer also has an ethical obligation to refrain from mining an electronic document."¹⁶⁵ As such, the Commission noted that mining would constitute misconduct under Rule 8.4.¹⁶⁶ Interestingly, while Alabama and New York both concluded that mining would amount to conduct "involving dishonesty, fraud, deceit or misrepresentation," as well as "conduct that is prejudicial to the administration of justice,"¹⁶⁷ Alabama referenced "violat[ing] or attempt[ing] to violate the Rules of Professional Conduct," and "commit[ting] a criminal act that reflects adversely on the lawyer's honesty, trustworthiness or fitness as a lawyer in other respects."¹⁶⁸ While other mining-prohibiting jurisdictions have generally adopted the New York approach of viewing metadata under what the ABA termed the "rubric of a lawyer's honesty,"¹⁶⁹ only Alabama has gone so far as to imply that the mining of metadata may constitute a "criminal act" under Rule 8.4(b).¹⁷⁰

¹⁶² Id.

¹⁶³ Id.

¹⁶⁴ Id.

¹⁶⁵ Id.

¹⁶⁶ Ala. Op. 2007-02 specifically referenced sub-sections (a) through (d) of Rule 8.4. See *id.* These sub-sections dealing with violating the Rules of Professional Conduct (a), committing a criminal act (b), engaging in dishonest conduct (c), and engaging in conduct prejudicial to the administration of justice (d), are all identical to the Model Rules. See Ala. Rules of Prof'l Conduct R. 8.4(a)-(d); Model Rules of Prof'l Conduct R. 8.4(a)-(d). Sub-sections (e), implying ability to improperly influencing officials, and (f), engaging in conduct that adversely reflects on a lawyer's fitness to practice law, differ from the Model Rule 8.4(e)-(f). See Ala. Rules of Prof'l Conduct R. 8.4(e)-(f); Model Rules of Prof'l Conduct R. 8.4(e)-(f). However, those sections were not referenced by the Alabama ethics panel. See generally, Ala. Op. 2007-02, *supra* note 7.

¹⁶⁷ See Ala. Rules of Prof'l Conduct R. 8.4(c)-(d); N.Y. Lawyer's Code of Prof'l Responsibility DR 1-102(A)(4)-(5). Alabama Rule 8.4(c) holds that it is professional misconduct for a lawyer to "engage in conduct involving dishonesty, fraud, deceit or misrepresentation" while Rule 8.4(d) holds that it is professional misconduct for a lawyer to "engage in conduct that is prejudicial to the administration of justice." See Ala. Rules of Prof'l Conduct R. 8.4(c)-(d).

¹⁶⁸ Alabama Rule 8.4(a) holds that it is professional misconduct for a lawyer to "violate or attempt to violate the Rules of Professional Conduct, knowingly assist or induce another to do so, or do so through the acts of another," while Rule 8.4(b) holds that it is professional misconduct for a lawyer to "commit a criminal act that reflects adversely on the lawyer's honesty, trustworthiness or fitness as a lawyer in other respects[.]" See Ala. Rules of Prof'l Conduct R. 8.4(a)-(b).

¹⁶⁹ ABA Op. 06-442, *supra* note 19, at 4.

¹⁷⁰ See *id.* The District of Columbia, on the other hand, did recognize that removing metadata when in a discovery context, may indeed amount to a criminal offense. See D.C. Op. 341, *supra* note 12.

Regardless of whether the Alabama Commission meant to state that mining indeed could constitute a criminal act, or whether the Commission simply listed all of Rule 8.4's provisions, Alabama fully agreed with New York that mining violates both "the letter and spirit" of the Rules.¹⁷¹ Accordingly, the Commission found that "[t]he mining of metadata constitutes a knowing and deliberate attempt by the recipient attorney to acquire confidential and privileged information in order to obtain an unfair advantage against an opposing party."¹⁷²

While the Alabama opinion is essentially a wholesale adoption of the 2001 [*207] New York view and approach,¹⁷³ it is interesting to note that the opinion does not address the opposing ABA view; particularly the ABA's reasoning with regard to the impact of Model Rule 4.4(b)'s adoption. Although this may seem unusual, it is also fully understandable in light of the fact that when the Alabama Commission issued its opinion (in March 14, 2007), Alabama did not have a rule equivalent to Model Rule 4.4(b). However, in June 2008, Alabama adopted an expanded version of Model Rule 4.4(b) that departs from the original in that it requires a lawyer who receives an inadvertently sent document, that on its face appears to be privileged or confidential, to notify the sender and to either abide by the sender's instructions or submit the issue to a tribunal for a determination.¹⁷⁴ The question now becomes whether Alabama, like New York, has moved from the mining-prohibited camp to the mining-permitted camp.

Although this argument can certainly be made, there are two reasons why it would be incorrect to conclude that the 2008 amendments to Alabama's professional conduct rules have had the same effect in Alabama as the New York rule change had in that state. First and foremost, New York specifically excluded the act of viewing and using information inadvertently received as being subject to professional discipline in the comments to its version of Rule 4.4,¹⁷⁵ whereas Alabama declined to take a similar approach. Thus, there is no indication that Alabama has moved away from the view espoused by the Alabama Commission in Opinion 2007-02 that mining of metadata is a "knowing and deliberate attempt . . . to acquire confidential and privileged information" and as such is ethically prohibited.¹⁷⁶ Second, the 2008 version of Alabama Rule 4.4(b) was in essence an adoption of the pre-Rule 4.4(b) ABA approach, as articulated in former ABA Ethics Opinion 92-368: "[R]efrain from viewing, notify sender and

¹⁷¹ Ala. Op. 2007-02, *supra* note 7, at 4.

¹⁷² *Id.* The Alabama Commission did recognize the formal discovery context as an exception to the blanket rule that mining is ethically impermissible, noting that removing metadata from discovery documents may under certain circumstances be grounds for discipline. *Id.*

¹⁷³ In fact, the Alabama opinion not only notes that it is consistent with New York Opinions 749 and 782, but even acknowledges that some of the language of the opinion is derived from the New York opinions. *Id.* at 5.

¹⁷⁴ The 2008 amendment to Alabama Rule 4.4 reads: A lawyer who receives a document that on its face appears to be subject to the attorney-client privilege or otherwise confidential, and who knows or reasonably should know that the document was inadvertently sent, should promptly notify the sender and (1) abide by the reasonable instructions of the sender regarding the disposition of the document; or (2) submit the issue to an appropriate tribunal for a determination of the disposition of the document. Ala. Rules of Prof'l Conduct R. 4.4(b).

¹⁷⁵ N.Y. Rules of Prof'l Conduct R. 4.4(b), cmt. 3. .

¹⁷⁶ Ala. Op. 2007-02, *supra* note 7, at 4.

abide by sender's instructions." ¹⁷⁷ Unlike the ABA, however, which interpreted the adoption of Model Rules 4.4.(b)'s notice-only requirement as specifically removing the viewing of inadvertently received material from the ethically impermissible category, Alabama was not narrowing a greater pre-existing duty, but rather establishing a new duty. ¹⁷⁸ In the absence of language to the contrary in the comments to Alabama's Rule 4.4(b), and in the absence of the new rule narrowing [*208] a previously existing ethically duty, there is no reason to conclude that Alabama intended to change the view espoused in Alabama Ethics Opinion 2007-02 that the mining of metadata violates both the "letter and spirit" of Rule 8.4 and thus constitutes professional misconduct.

This does not mean, however, that Alabama attorneys could not remove the act of mining from this category through bilateral agreements, just as New York attorneys could have done under the old New York Code and New York Ethics Opinions 749 and 782. In other words, because the Alabama opinion is to a large extent an adoption of the 2001 New York view on the ethics of metadata, a similar analysis can be employed with regards to the use of bilateral agreements by opposing attorneys in either state who mutually agree to the mining of their respective documents. If Alabama attorneys were to form such an agreement, any subsequent mining of metadata would no longer "constitute[] a knowing and deliberate" attempt by one attorney to either "acquire confidential and privileged information" nor to "obtain an unfair advantage against an opposing party." ¹⁷⁹ The rationale underlying Alabama's prohibition on mining would be removed under a bilateral agreement that permitted mining. As was discussed above with regard to Florida, a unilateral notice by one attorney that he will mine documents received from an opposing attorney would not have the same effect. ¹⁸⁰ Such a notice by one attorney does not vitiate his conduct from being a deliberate attempt to acquire confidential material, nor his attempt to seek to obtain an unfair advantage over his opponent. If anything, it makes his intentions more clear and arguably his conduct more reprehensible. The rationale underlying Alabama's ban on mining would not be disturbed by the unilateral notice scenario.

F. District of Columbia: Mining Permitted-Actual Knowledge

The year 2007 was an active year for ethics opinions pertaining to metadata. Six months after Alabama issued its opinion, the Legal Ethics Committee of the District of Columbia Bar (D.C. Ethics Committee) issued Ethics Opinion 341-Review and Use of Metadata in Electronic Documents. ¹⁸¹ The opinion constitutes a compromise of sort between the original mining prohibited and mining permitted approaches. Rather than falling neatly into one of the two camps, the Committee focused on the receiving attorney's knowledge, finding that absent

¹⁷⁷ See supra note 78 and accompanying text.

¹⁷⁸ A review of previously promulgated Alabama ethics opinions from 1987 through 2009, and a search of "inadvertent disclosure" of all Alabama ethics opinions indicated that no prior Alabama ethics opinions have been issued on the inadvertent disclosure of material. See Office of General Counsel Formal Opinions, Ala. State Bar, <http://www.alabar.org/ogc/fopList.cfm> (last visited Nov.11, 2010).

¹⁷⁹ Ala. Op. 2007-02, supra note 7, at 4.

¹⁸⁰ See supra discussion pertaining to unilateral notices under Florida rules.

¹⁸¹ D.C. Op. 341, supra note 12.

actual knowledge that metadata was inadvertently sent, a receiving lawyer is not prohibited from reviewing such metadata.¹⁸² The Committee reached this conclusion by addressing all of the topics raised in previous metadata ethics opinions, including the sender's duty, the receiving attorney's duties, and the interplay of Model Rules 1.1-Competence, 1.3-Diligence and Zeal, 1.6-Confidentiality of Information, 3.4- Fairness to Opposing Party and Counsel, 4.4(b)-Respect for Rights of Third Persons, and 8.4-Misconduct. The Committee's opinion, however, went further in its scope by picking up on Maryland's references to the potential interplay between metadata ethics and the **[*209]** Federal Rules of Civil Procedure. Furthermore, the opinion provided an in-depth examination of how a sending and a receiving attorney's ethical duties change when the playing field moves from the exchange of documents outside the scope of formal discovery to within the discovery arena.

After describing metadata as "data about data,"¹⁸³ the opinion addressed the sending and receiving lawyers' duties outside of the discovery process. In terms of sending lawyers, the duty is simple: they have "an obligation under Rule 1.6¹⁸⁴ to take reasonable steps to maintain the confidentiality of documents in their possession."¹⁸⁵ This includes ensuring that documents that contain confidential material are not transmitted, as well as "employ[ing] reasonably available technical means to remove such metadata before sending the document."¹⁸⁶ The D.C. Ethics Committee did not expand upon what "reasonable steps" entailed, except to suggest that lawyers "acquire sufficient understanding of the software that they use."¹⁸⁷

Thus, the opinion disposed of the sending lawyer's duty with regard to metadata fairly succinctly: be mindful of the confidence requirement of Rule 1.6¹⁸⁸ **[*210]** and the competence

¹⁸² Id.

¹⁸³ While the Committee noted that metadata is often referred to as "data about data," it also provided a comprehensive definition of metadata as "electronically stored information, typically not visible from the face of the document as printed out or as initially shown on the computer screen, but which is imbedded in the software and retrievable by various means." Id. As an indication of the opinion's thoroughness, the opinion also included the Federal Judicial Center's definition of metadata as: Information about a particular data set or document which described how, when, and by whom the data set or document was collected, created, accessed, or modified; its size; and how it is formatted. Some metadata, such as file dates and sizes, can easily be seen by users; other metadata can be hidden from users but are still available to the operating system or the program used to process the data or document. Id. at n.1 (citing Barbara J. Rothstein, Ronald J. Hedges & Elizabeth C. Wiggins, *Managing Discovery of Electronic Information: A Pocket Guide for Judges*, Federal Judicial Center, 24-25 (2007) , [www.fjc.gov/public/pdf.nsf/lookup/eldscpkt.pdf/\\$file/eldscpkt.pdf](http://www.fjc.gov/public/pdf.nsf/lookup/eldscpkt.pdf/$file/eldscpkt.pdf) (last visited Nov. 11, 2010)).

¹⁸⁴ District of Columbia Rule 1.6 differs markedly from the Model Rule in terms of its language and structure. The basic prohibition that a lawyer shall not "reveal a confidence or secret of the lawyer's client," except when permitted, is the same, however. See D.C. Rules of Professional Conduct R. 1.6 (2008), available at [http://www.dcbart.org/lawyers/ethics/legal ethics/rules of professional conduct/amended rules/rule one/](http://www.dcbart.org/lawyers/ethics/legal%20ethics/rules%20of%20professional%20conduct/amended%20rules/rule%20one/) (last visited Nov. 11, 2010). District of Columbia Rule 1.6(a) reads in pertinent part: "Except when permitted under paragraph (c), (d), or (e), a lawyer shall not knowingly: (1) reveal a confidence or secret of the lawyer's client." Id.

¹⁸⁵ D.C. Op. 341, *supra* note 12.

¹⁸⁶ Id.

¹⁸⁷ Id.

¹⁸⁸ District of Columbia Rule 1.6 differs somewhat from the Model Rule. While the Model Rule mandates that a "lawyer shall not reveal" information relating to the representation of a client, the District's Rule 1.6 limits this prohibition to disclosures made "knowingly." Compare Model Rules of Professional Conduct R. 1.6, with D.C. Rules of Professional Conduct R. 1.6. Thus, in the District of

requirement of Rule 1.1.¹⁸⁹ However, a D.C. attorney receiving electronic documents outside of the discovery context needs to not only be mindful of D.C. Ethics Opinion 341, but also two prior ethical opinions, as well as Rules 8.4 and 4.4(b). And, the attorney must make a determination as to whether or not he has "actual knowledge" of the inadvertence of the transmitted document.

A receiving lawyer's duties in the District of Columbia hinges upon the lawyer's knowledge as to whether metadata was inadvertently transmitted. D.C. Ethics Opinion 341 agreed with New York and Alabama that Rule 8.4(c)¹⁹⁰ is "implicated when a receiving lawyer wrongfully 'mines' an opponent's metadata."¹⁹¹ The District of Columbia, however, differs from all preceding ethics opinions in finding that Rule 8.4 is implicated only when the receiving lawyer has "actual prior knowledge that the metadata was inadvertently provided."¹⁹² The D.C. Ethics Committee reasoned that given the "ubiquitous exchange" of electronic documents and the sending attorney's duty to avoid the inadvertent production of metadata, the "mere uncertainty" on the part of the receiving lawyer as to whether the metadata was inadvertently included does not trigger an ethical duty to refrain from reviewing such metadata.¹⁹³ However, if the receiving attorney has "actual prior knowledge" as to the inadvertence of the transmission, regardless as to whether such inadvertence was the result of "negligence or even an ethical lapse" on the part of the sending attorney, "the receiving lawyer's duty of honesty requires that he refrain from reviewing the metadata."¹⁹⁴ Additionally, D.C. Opinion 341 mandates that the receiving lawyer consult with the sending lawyer to ascertain whether the metadata includes privileged

Columbia, a lawyer who inadvertently discloses client confidences contained in an inadvertently released document would not be in violation of Rule 1.6. See D.C. Rules of Prof'l Conduct R. 1.6. However, if the same lawyer asked his junior associate (or secretary or paralegal) to handle the document exchange, and that junior associate through negligence caused the disclosure, the supervising attorney would be in violation of District Rule 1.6(f), which mandates: "A lawyer shall exercise reasonable care to prevent the lawyer's employees, associates, and others whose services are utilized by the lawyer from disclosing or using confidences or secrets of a client . . . [except as permitted]." See D.C. Rules of Prof'l Conduct R. 1.6(f). See also D.C. Bar Legal Ethics Comm., Ethics Op. 256 (1995), available at [http://www.dcbar.org/forlawyers/ethics/legal ethics/opinions/opinion256.cfm](http://www.dcbar.org/forlawyers/ethics/legal%20ethics/opinions/opinion256.cfm) (last visited Nov. 11, 2010) [hereinafter D.C. Op. 256] (interpreting the pre-February 1, 2007 rules, in which current section (f) appeared as section (e)); D.C. Rules of Prof'l Conduct R. 1.6 (2007), available at [http://www.dcbar.org/forlawyers/ethics/legal ethics/rules of professional conduct/fo rmer rules/ rule one/rule01 06.cfm](http://www.dcbar.org/forlawyers/ethics/legal%20ethics/rules%20of%20professional%20conduct/for%20former%20rules/rule%20one/rule0106.cfm) (last visited Nov. 11, 2010).

¹⁸⁹ D.C. Op. 342 did not specifically reference Rule 1.1. See D.C. Op. 342, *supra* note 12. However, the opinion does speak of attorneys "acquir[ing] sufficient understanding of the software they use[.]" which certainly falls under Rule 1.1's duty to "maintain the requisite knowledge and skill" needed to provide competent representation. See *id.*; D.C. Rules of Prof'l Conduct R. 1.1 (2008), available at [http://www.dcbar.org/forlawyers/ethics/legal ethics/rules of professional conduct/ amended rules/ rule one/rule01 01.cfm](http://www.dcbar.org/forlawyers/ethics/legal%20ethics/rules%20of%20professional%20conduct/amended%20rules/rule%20one/rule0101.cfm) (last visited Nov. 11, 2010). Comment 6 to the rule reads: "To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, and engage in such continuing study and education as may be necessary to maintain competence." See *id.* at cmt. 6.

¹⁹⁰ The District's Rule 8.4(c) is identical to the Model Rule. See D.C. Rules of Prof'l Conduct R. 8.4(c); Model Rules of Prof'l Conduct R. 8.4(c). District of Columbia Rule 8.4(c) states that it is professional misconduct to "[e]ngage in conduct involving dishonesty, fraud, deceit, or misrepresentation." D.C. Rules of Prof'l Conduct R. 8.4(c) (2008).

¹⁹¹ D.C. Op. 341, *supra* note 12.

¹⁹² *Id.* (emphasis added).

¹⁹³ *Id.*

¹⁹⁴ *Id.*

information. If so, the receiving lawyer must abide by the sending lawyer's instructions, reserving his or her right to challenge the claim of privilege as appropriate.¹⁹⁵

Accordingly, the District of Columbia focused its inquiry upon whether the [*211] receiving lawyer knew that the metadata was inadvertently transmitted prior to reviewing it. In doing so, D.C. Opinion 341 relied heavily upon its 1995 pre-metadata opinion regarding the inadvertent disclosure of privileged material in general. In D.C. Opinion 256, the District of Columbia Ethics Committee concluded that it was not unethical for a receiving lawyer to review a document containing confidences if such review was done in good faith before the receiving lawyer learned of the inadvertence.¹⁹⁶ However, when the receiving lawyer "knows of the inadvertence of the disclosure" before examining the documents, such an examination would constitute a violation of Rule 8.4(c). As the Committee in D.C. Ethics Opinion 256 noted, "[t]he line we have drawn between an ethical and an unethical use of inadvertently disclosed information is based on the receiving lawyer's knowledge of the inadvertence of the disclosure."¹⁹⁷ D.C. Opinion 341 maintained this distinction with regard to metadata.

The District of Columbia Ethics Committee also relied upon Rule 4.4(b) in reaching its conclusion that a lawyer's actual knowledge determines his or her ethical obligations. While the ABA looked to the adoption of Model Rule 4.4(b) with its lone notice requirement as support for its conclusion that it is ethically permissible to mine for metadata under the Model Rules, the District of Columbia likewise looked to its newly adopted Rule 4.4(b) as support for its conclusion that absent actual knowledge, mining is permissible.¹⁹⁸ Prior to February 1, 2007, the District of Columbia's Rule 4.4 consisted solely of what has subsequently become subsection (a): a prohibition on using means to embarrass or violate the rights of a third party.¹⁹⁹ However, on February 1, 2007, subsection (b) of Rule 4.4 went into effect. Unlike Model Rule 4.4(b), which only requires the receiving attorney to notify the sender, the District of Columbia's Rule 4.4(b) requires notification and compliance with the sender's instructions, but only if the receiving lawyer knows before reviewing the document that it was inadvertently sent.

¹⁹⁵ Id.

¹⁹⁶ D.C. Op. 256, *supra* note 188.

¹⁹⁷ Id. (emphasis added). D.C. Op. 256 concluded that a receiving lawyer who knew that the document containing client secrets or confidences had been inadvertently produced would be violating Rule 8.4(c), as well as Rule 1.15. See *id.* According to D.C. Op. 256, a receiving lawyer with such actual knowledge would have a duty under Rule 1.15(a) to safeguard the documents, and under Rule 1.15(b) to notify the sending attorney of his possession of such documents, and to return them if so requested. See *id.* Note that although D.C. Op. 256 was interpreting the pre- February 1, 2007 rules, the current versions of sub-sections (a) and (b) of District of Columbia Rule 1.15 have not changed. See D.C. Rules of Professional Conduct R. 1.15 (2008); *supra* text accompanying note 188.

¹⁹⁸ D.C. Op. 341, *supra* note 12.

¹⁹⁹ Before February 1, 2007 the District of Columbia's Rule 4.4 consisted of one paragraph that read in its entirety: "In representing a client, a lawyer shall not use means that have no substantial purpose other than to embarrass, delay, or burden a third person, or use methods of obtaining evidence that violate the legal rights of such a person." D.C. Rules of Professional Conduct R. 4.4 (2007). Interestingly and significantly, when the District adopted sub-section (b), effective as of February 1, 2007, it added a "knowing" element, so that Rule 4.4(a) now reads in its entirety: "In representing a client, a lawyer shall not use means that have no substantial purpose other than to embarrass, delay, or burden a third person, or knowingly use methods of obtaining evidence that violate the legal rights of such a person." D.C. Rules of Professional Conduct R. 4.4(a) (2008), available at [http://www.dcbbar.org/lawyers/ethics/legal ethics/rules of professional conduct/am ended rules/rule four/rule04 04.cfm](http://www.dcbbar.org/lawyers/ethics/legal%20ethics/rules%20of%20professional%20conduct/amended%20rules/rule%20four/rule04%2004.cfm) (last visited Nov. 11, 2010) (emphasis added).

²⁰⁰ While the [*212] Committee noted that Rule 4.4(b) was meant to "address the inadvertent disclosure of entire documents (whether electronic or paper)," it saw no reason why the rule "would not also apply to an inadvertently transmitted portion of a writing that is otherwise intentionally sent," i.e., metadata. ²⁰¹

The District of Columbia Ethics Opinion, unlike metadata opinions before it, did not limit its discussion to the non-discovery context. Rather, after having exhaustively analyzed the sending and the receiving lawyer's duties in the non-discovery realm, D.C. Ethics Op. 341 delved into the discovery realm. Here, the District of Columbia Ethics Committee laid the groundwork by noting that when metadata is provided, either in discovery or pursuant to a subpoena, the lawyers must be concerned with additional rules: not only should lawyers be aware of applicable Federal Rules of Civil Procedure, ²⁰² but certain additional Rules of Professional Conduct also become applicable when moving into the discovery/subpoena context. For example, a sending lawyer who in the non-discovery context seeks to comply with his or her duty to safeguard client confidences by scrubbing metadata before transmitting a document may violate Model Rule 3.4's prohibition on unlawfully obstructing another party's access to evidence. ²⁰³ Indeed, the Committee noted that the removal of metadata may be prohibited by the Rules and under some circumstances, may also constitute a crime. ²⁰⁴

The parameters also change for the receiving lawyer in a discovery or subpoena context. In light of the sending lawyer's Rule 3.4 duties, the receiving lawyer in the discovery context "is generally justified in assuming that the metadata was provided intentionally." ²⁰⁵ In fact, not only is a receiving lawyer in the District of Columbia justified in assuming the metadata was intentionally provided when in the discovery/subpoena context, but pursuant to Rules 1.1 and 1.3, the lawyer may [*213] have an obligation to review and examine such metadata. ²⁰⁶ Indeed, D.C. Ethics Op. 341 noted that in so far as an electronic documents is substantially the

²⁰⁰ District of Columbia Rule 4.4(b) reads in its entirety: 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. D.C. Rules of Prof'l Conduct R. 4.4(b) (2008).

²⁰¹ D.C. Op. 341, supra note 12.

²⁰² The opinion specifically mentioned [F.R. Civ. P. 16\(b\)](#), [26\(f\)](#), [33\(d\)](#), [34\(a\)](#), and [37\(f\)](#); the Author would also add Rule 26(b)(5)(B). See D.C. Op. 341, supra note 12. Indeed, the Commission noted that when laboring within the Federal discovery rules, a failure to abide by such rules in and of itself could constitute a violation of Rule 3.4(c), which prohibits a lawyer from "knowingly disobey[ing] an obligation under the rules of the tribunal." See D.C. Op. 341, supra note 12; D.C. Rules of Prof'l Conduct R. 3.4(c) (2008).

²⁰³ District of Columbia instructs, in relevant part, that: A lawyer shall not: (a) Obstruct another party's access to evidence or alter, destroy, or conceal evidence, or counsel or assist another person to do so, if the lawyer reasonably should know that the evidence is or may be the subject of discovery or subpoena in any pending or imminent proceeding. D.C. Rules of Prof'l Conduct R. 3.4(a) (2008). Note that impermissible scrubbing in a discovery context might indeed also constitute the altering, destroying or concealing evidence as well.

²⁰⁴ See D.C. Op. 341, supra note 12 (citing D.C. Rules of Prof'l Conduct R. 3.4, cmt. 4, which illustrates potential federal criminal violations).

²⁰⁵ Id. (emphasis added).

²⁰⁶ Rule 1.1(a) provides: "A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness, and preparation reasonably necessary for the representation." D.C. Rules of Prof'l

same as a tangible piece of evidence, a receiving lawyer laboring within the discovery/subpoena context, in order to fulfill his or her zealous advocacy duty, may even be required to "consult with a computer expert" in order to determine how to most effectively mine the metadata, much in the same way "a lawyer does with a finger-print expert."²⁰⁷

However, even when in the discovery/subpoena context, and even considering a receiving lawyer's zealous advocacy duty, if that lawyer has actual knowledge that the metadata was inadvertently provided, the lawyer is not free to mine such metadata. Instead, a lawyer under those circumstances must advise the sending lawyer, and if it is determined that the information is confidential, abide by the sending lawyer's instructions.²⁰⁸ The receiving lawyer would, of course, be entitled to take protective measures to ensure that the information was not destroyed and to challenge any claim of privilege by the sending lawyer.²⁰⁹

The District of Columbia's reliance upon "actual prior knowledge" as the linchpin for when the mining of metadata becomes unethical makes the District amenable to the concept of attorney-created agreements with regard to metadata. In other words, if two attorneys engaged in a matter agree through a bilateral agreement that any and all metadata that may be contained in electronic documents they exchange was inadvertently included in those documents, both attorneys would possess the requisite actual prior knowledge to make any mining of such metadata a violation of Rule 8.4. Thus, as with all jurisdictions that generally permit mining, District of Columbia attorneys can readily "opt out" of mining being ethically permitted, and ensure that mining becomes ethically impermissible with regard to their documents. If anything, the District of Columbia's overt reliance on the prior actual knowledge of inadvertence has made bilateral agreements prohibiting the mining of metadata particularly appealing within that jurisdiction.

The more interesting result of the District of Columbia's unique incorporation of an actual knowledge standard is that it also enables a sending attorney to [*214] unilaterally prohibit a receiving attorney from mining metadata. Applying the District of Columbia Ethics Committee's rationale, a sending lawyer could include specific language in a unilateral notice accompanying an electronically transmitted document that any metadata contained in the document was inadvertently included. While such a notice would function to prohibit a receiving lawyer in any jurisdiction from mining the document, in the District of Columbia, considering the Committee's

Conduct R. 1.1(a). Rule 1.3(a) provides, in part, that: "A lawyer shall represent a client zealously and diligently within the bounds of the law." D.C. Rules of Prof'l Conduct R. 1.3(a) (2008). Notwithstanding the reference to competent and zealous representation, the Committee pointed out, in a footnote, that "in concluding that a lawyer may review metadata in documents produced in discovery . . . we do not intend to suggest that a lawyer must undertake such a review." D.C. Op. 341, *supra* note 12, at n.9. Rather, the Committee suggested such a decision "might be a matter on which consultation with the client may be necessary." *Id.* (quoting D.C. Op. 256, *supra* note 188, at n.7).

²⁰⁷ D.C. Op. 341, *supra* note 12.

²⁰⁸ *Id.* The Opinion noted that a failure to do so would constitute a violation of Rule 8.4(c), and noted that D.C. Ethics Op. 256 had explained with regard to this point that, at a minimum, a lawyer should "seek guidance from the sending lawyer and, if that lawyer confirms the inadvertence of the disclosure and requests return of the material, unread, the receiving lawyer should do so. In our view, a failure to do so would be a dishonest act, in violation of Rule 8.4(c)." See *id.*; D.C. Op. 256, *supra* note 188. Such conduct would also arguably constitute a violation of Rule 4.4(b).

²⁰⁹ D.C. Op. 341, *supra* note 12.

emphasis on actual knowledge of inadvertence, it would be virtually impossible for a receiving attorney to argue that he could ethically mine such a document. This is especially true given the fact that D.C. Opinion 341 made it clear that actual knowledge exists even if the inadvertence was the result of negligence or by way of an ethical lapse on the part of the sending attorney. The focus is not why metadata may have been included; the focus is upon the receiving attorney's "actual knowledge" of the inadvertence of the transmission of the document. Certainly, a unilateral notice from the sending attorney that any metadata was inadvertently included, received contemporaneously with the document, i.e., before the receiving attorney has had a chance to review the document, would suffice to meet the "actual knowledge" threshold, thus prohibiting the receiving attorney from mining the document.

G. Arizona: Mining Prohibited

Arizona became the seventh jurisdiction (including the ABA) to issue an ethics opinion pertaining to metadata in 2007. In November of that year, noting "the importance of this subject matter," the State Bar of Arizona Ethics Committee (Arizona Ethics Committee) issued a sua sponte opinion to provide guidance for Arizona lawyers with regard to "the ethical duties of lawyers who send and receive electronic communications."²¹⁰ Arizona joined the original New York, Florida, and Alabama views and acknowledged but "respectfully declin[ed] to follow the ABA position" in concluding that a sending lawyer must take "reasonable precautions" to prevent the disclosure of confidential material when sending electronic communications, and that a receiving lawyer may not examine such a document "for the purpose of discovering the metadata embedded in it."²¹¹

In discussing the sending attorney's duties, the opinion looked to Arizona Rule 1.6-Confidentiality of Information, and in particular, comment 20 to Rule 1.6, which explains that "[w]hen transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients."²¹² The opinion explained that what is reasonable depends upon factors such as the sensitivity of the information, the potential consequences of an inadvertent disclosure, and whether disclosure is restricted by statute, **[*215]** protective order, confidentiality agreement or client instructions.²¹³

Arizona, like all jurisdictions, emphasized the sender's obligation to protect confidential material. Despite this obligation on the part of the sending attorney, an obligation that lies at the very

²¹⁰ Ariz. Op. 07-03, supra note 12.

²¹¹ Id. (emphasis added).

²¹² Id. (emphasis added) (citing Ariz. Rules of Prof'l Conduct R. 1.6, cmt. 20 (2010), available at <http://www.myazbar.org/Ethics/rules.cfm> (last visited, Nov. 11, 2010)). The text of Arizona R. 1.6(a) reads: "A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted or required by paragraphs (b), (c) or (d), or ER 3.3(a)(3)." Ariz. Rules of Prof'l Conduct R. 1.6(a) (2010).

²¹³ Ariz. Op. 07-03, supra note 12.

heart of the legal profession,²¹⁴ Arizona accepted the proposition that lawyers will not always be successful in doing so. In fact, the opinion acknowledged the possibility of a sending lawyer failing to fulfill her Rule 1.6 duties. The opinion noted that "[t]he sender of the document may not be aware of the metadata embedded within the document or that it remains in the electronic document despite the sender's good faith belief that it was 'deleted.'" ²¹⁵ Similarly, in discussing the receiving attorney's duties, the opinion accepted that despite a sending attorney's "thorough precautions, and even with the best of intentions, it may not be possible for the sending attorney to be absolutely certain that all of the potentially harmful metadata has been 'scrubbed' from the document before it is transmitted electronically." ²¹⁶ Maybe because of this acknowledgment that attorneys in Arizona will be unable to comply with both the mandates of competence ²¹⁷ and confidentiality,²¹⁸ the opinion wisely counseled attorneys who are asked by a colleague to comment upon a document that may eventually be forwarded to an opposing counsel "to consider whether the comment is the type that should be included within the draft." ²¹⁹ Similarly, and very astutely, the opinion also cautioned attorneys that any document electronically transmitted to an opposing counsel may eventually be distributed to a non-lawyer who would not be governed by the same ethical rules that would prohibit an attorney from mining the metadata. ²²⁰

Having warned a sending attorney of the pitfalls surrounding metadata and after outlining the ethical parameters he needs to be aware of, the opinion affirmatively (yet respectfully) rejected the ABA approach, which permitted a receiving attorney to mine metadata. ²²¹ Arizona based this rejection of the ABA position on the notion that sending attorneys will not be able to remove all [*216] metadata. ²²² As such, "the sending lawyer would be at the mercy of the recipient

²¹⁴ Id. Indeed, Ariz. Op. 07-03 termed this duty of confidentiality a "fundamental principle" of the client-lawyer relationship. Id.

²¹⁵ Id.

²¹⁶ Id.

²¹⁷ Arizona Rule 1.1 reads in full: "A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation." Ariz. Rules of Prof'l Conduct R. 1.1 (2010). .

²¹⁸ See supra text accompanying note 212.

²¹⁹ Ariz. Op. 07-03, supra note 12.

²²⁰ Id. If the receiving attorney deliberately forwarded the electronic document to a non-lawyer for the purpose of that non-lawyer to mine the metadata for confidential information, i.e., to do what the lawyer could not do, that lawyer would be in violation of Rule 8.4(a), which makes it unethical for a lawyer to do through others what he himself cannot do. See generally David D. Dodge, *Reacting to Inadvertent Disclosure*, Ariz. Attn'y, July-Aug. (2008), at 10 (noting that under Arizona Rule 8.4(a), it is unethical to attempt to do through others that which cannot be done ethically by one's self). Arizona Rule 8.4 states: "It is professional misconduct for a lawyer to : (a) violate or attempt to violate the Rules of Professional Conduct, knowingly assist or induce another to do so, or do so through the acts of another." Ariz. Rules of Prof'l Conduct R. 8.4(a).

²²¹ Ariz. Op. 07-03, supra note 12 ("We respectfully decline to follow the ABA position.").

²²² Id. It is astounding that Arizona, and other jurisdictions that ban the mining of metadata, accept the acknowledgment that their attorneys when sending electronic documents will invariably fail to comply with Rules 1.1 and 1.6. Indeed, the minimization of the sending attorney's duties in relation to the receiving attorney's duties can be seen in the terminology used by the Arizona opinion: while the receiving lawyer is affirmatively told he or she has a "duty not to 'mine,'" the opinion notes that under the

lawyer," ²²³ possibly leading attorneys to conclude that in order to be safe, they will have to forego exchanging documents electronically entirely. ²²⁴ Rather than taking this chance, ²²⁵ Arizona joined Florida and Alabama in prohibiting a receiving attorney from mining a document (absent specific circumstances). ²²⁶

The Arizona Ethics Committee also noted that Arizona Rule 4.4(b) differs from Model Rule 4.4(b). While Model Rule 4.4(b) only requires notification, ²²⁷ Arizona Rule 4.4(b) requires a lawyer who receives a document and knows or reasonably should know that the document was inadvertently sent, to notify the sender and preserve the status quo in order to enable the sender to take appropriate protective action. ²²⁸ The opinion dismissed as "an insubstantial distinction," the argument that Arizona Rule 4.4(b) is inapplicable in the metadata context because only the metadata, not the document containing the metadata, was inadvertently sent. Indeed, the opinion maintained that a receiving lawyer who discovers ²²⁹ metadata he knows or should know "is revealing confidential or privileged information," must both notify and preserve the status quo for a reasonable period of time in order to permit the sending attorney to take protective measures. ²³⁰

The exceptions to the ban on mining metadata in Arizona are limited to situations where the receiving attorney has consent of the sender and when mining is allowed by a court, rule, or other law. ²³¹ However, even when a lawyer is mining metadata under one of those exceptions, if that lawyer uncovers information that he knows or reasonable should know the sending lawyer did not intend for him to see, Arizona Rule 4.4(b) mandates that the receiving lawyer notify the sending lawyer and preserve the status quo for a reasonable period of time to permit the [*217] sending lawyer to take protective measures. ²³²

position taken by New York, Florida, Alabama, and Arizona, the sending lawyer is "reminded of the duty to take reasonable steps to prevent the inadvertent disclosure of confidential or privileged information." *Id.* (emphasis added).

²²³ *Id.*

²²⁴ *Id.*

²²⁵ The opinion notes the possibility of lawyers abandoning the use of electronic document transmission entirely is not "realistic or necessary." *Id.*

²²⁶ *Id.* See *infra* for a discussion of special circumstances when mining is permissible.

²²⁷ See Model Rules of Prof'l Conduct R. 4.4.

²²⁸ *Ariz. Op. 07-03*, *supra* note 12. Arizona Rule 4.4(b) reads in its entirety: "A lawyer who receives a document and knows or reasonably should know that the document was inadvertently sent shall promptly notify the sender and preserve the status quo for a reasonable period of time in order to permit the sender to take protective measures." *Ariz. Rules of Prof'l Conduct R. 4.4(b)* (2010).

²²⁹ The opinion recognized that some metadata can be discovered "through inadvertent or relatively innocent means such as right clicking a mouse or holding the cursor over certain text in a document." *Ariz. Op. 07-03*, *supra* note 12. As such, all activity that constitutes mining "does not rise to a level of ethical concern." *Id.* However, regardless of how metadata is discovered, if it contains confidential material, Arizona Rule 4.4(b) must be followed. *Id.*

²³⁰ *Id.*

²³¹ *Id.*

²³² *Id.*

Arizona thus falls squarely within the New York, Alabama, and Florida camp in prohibiting the purposeful mining of metadata.²³³ None of these jurisdictions agree with the District of Columbia's focus on the actual knowledge of the receiving attorney as to whether the metadata was inadvertently sent.²³⁴ However, because Arizona Ethics Op. 07-03 came on the heels of D.C. Ethics Opinion 341, only Arizona addressed the District of Columbia's approach head-on. Arizona characterized the District's view as "an effort to reach a middle ground between the position of the ABA, on the one hand, and the positions of Alabama, Florida, and New York on the other hand," but then firmly, yet "respectfully," disagreed with the opinion.²³⁵ In doing so, Arizona held that a lawyer receiving electronic documents, absent falling within one of the specific exceptions, "should not be engaged in the intentional examination of the document's metadata in the first place" ²³⁶ Indeed, the opinion noted, any lawyer who did discover metadata through an intentional act of mining would bear the burden of proving that the initial examination was for a legitimate purpose (presumably one of the approved exceptions) and not a purposeful attempt to discover confidential material.²³⁷

Thus, the Arizona Ethics Committee adopted a very strong position against the mining of metadata. It also, however, formalized the ability of attorneys to "opt out" of this ethical ban using attorney-agreements. Ariz. Op. 07-03 acknowledged that one of the "specific circumstances" in which an Arizona attorney may ethically mine metadata is when "he or she has the consent of the sender."²³⁸ Clearly then, two Arizona attorneys exchanging electronic documents can bilaterally agree that either attorney may mine the other's electronic documents. In fact, there does not need to be a bilateral agreement to this effect. One attorney, the sending attorney, can unilaterally consent to the receiving attorney mining metadata in documents the sending attorney transmits. Arizona's acknowledgement of the desirability of permitting attorneys to opt out of the general ban on mining makes sense. There will, after all, be times when a sending attorney wants the receiving attorney to be able to read the information contained in metadata, whether it be formulas used to create data in an Excel spreadsheet, or proposed changes or edits in a contract. However, even under such circumstances, Arizona, like all jurisdictions, warned that should the receiving attorney who is mining come "across information that the lawyer knows or reasonably should know was not intended to be transmitted by the sender,"²³⁹ the receiving attorney's Rule 4.4(b) duties to notify and preserve come into play.

The fact that Arizona formalized the ability of attorneys to opt out of the **[*218]** ethical ban on mining does not mean that the opposite is true. In other words, there is nothing in the Arizona opinion that would permit the receiving attorney to unilaterally give notice that he will mine

²³³ Although only Arizona specifically addressed the possibility of an accidental discovery of metadata, it is unlikely New York, Alabama or Florida would disagree with Arizona's position that innocuous discovery of metadata by placement of a cursor over text, for example, does not necessarily "rise[] to a level of ethical concern." *Id.*

²³⁴ See D.C. Op. 341, *supra* note 12.

²³⁵ Ariz. Op. 07-03, *supra* note 12, at n.1.

²³⁶ *Id.*

²³⁷ *Id.*

²³⁸ See *id.*, *supra* note 12.

²³⁹ *Id.*

metadata. Any such unilateral attempt on the part of the receiving attorney, absent consent by the sending attorney, would, in the view of Arizona, constitute the type of conduct the opinion sought to discourage through its general ban on the mining of metadata; i.e., "conduct which amounts to an unjustified intrusion into the client-lawyer relationship" between an opposing attorney and his or her attorney.²⁴⁰

H. Pennsylvania: Mining Permitted-Professional Courtesy

Pennsylvania has the distinction of being the only jurisdiction that has issued two opinions specifically aimed at providing guidance to its attorneys pertaining to their ethical duties surrounding metadata.²⁴¹ The first opinion, Pennsylvania Formal Ethics Opinion 2007-500,²⁴² focused on the duty of the receiving attorney. Despite that limitation, the Pennsylvania Committee on Legal Ethics and Professional Responsibility (Pennsylvania Ethics Committee) provided both a reasoned analysis of ethics and metadata in terms of the Pennsylvania Rules of Professional Conduct, as well as a thorough review of six of the seven opinions published prior to its issuance.²⁴³ Pennsylvania differentiated itself from all previous metadata ethics opinions, as well as those issued since, and declined to establish a bright-line rule regarding the mining of metadata. Instead, the Committee chose to rely on the independent professional judgment of the members of the Pennsylvania Bar. The Committee pointed to the very fountain of ethics and professionalism and concluded that "each attorney must, as the preamble to the Pennsylvania Rules of Professional Conduct states, "resolve [the issue] through the exercise of sensitive and moral judgment guided by the basic principles of the Rules' and determine for him or herself whether to utilize the metadata." ²⁴⁴ This [*219] non-directive conclusion was subsequently criticized by other ethics committees for not "adopt[ing] a conclusive view," ²⁴⁵ and as "arriv[ing] at a default." ²⁴⁶ While not directly responding to such criticisms, ²⁴⁷ the Pennsylvania Committee in 2009 concluded that its "prior opinion provided insufficient guidance to recipients of documents containing metadata and did not provide correlative guidance to

²⁴⁰ Id.

²⁴¹ New York, as discussed above, has also issued two ethics opinions relevant to metadata, N.Y. Op. 749 and N.Y. Op. 782. See *supra* notes 12 and 38. N.Y. Op. 749, however, did not specifically address metadata *per se*.

²⁴² Pa. Op. 2007-500, *supra* note 12. The original opinion is only available to members of the Pennsylvania Bar Association at the Pennsylvania Bar Association website's "Ethics Digest" column, available at <http://www.pabar.org/> (last visited Nov. 11, 2010). Surprisingly, the Pennsylvania Bar Association does not make its full ethics opinions available to the public. A slightly edited version of Pa. Op. 2007-500 without the original footnotes appears in Pa. Law. Jan.-Feb. (2008), at 46.

²⁴³ Pa. Op. 2007-500, *supra* note 12 (examining the ethics opinions of the American Bar Association, the District of Columbia, New York, Florida, Alabama, and Maryland, while Arizona's metadata ethics opinion is excluded from the discussion).

²⁴⁴ Id. at 1 (quoting from Pa. Rules of Prof'l Conduct, pmbi. (2008), available at <http://www.padisciplinaryboard.org/documents/Pa%20RPC.pdf> (last visited Nov. 11, 2010) (alterations in original)). Interestingly, part of the preamble notes that "[t]hese principles includes the lawyer's obligation to zealously protect and pursue a client's legitimate interests, within the bounds of the law, while maintaining a professional, courteous and civil attitude towards all persons involved in the legal system." Id. It is precisely this duty of a receiving attorney to her client in the metadata context that the Pennsylvania Committee on Legal Ethics and Professional Responsibility emphasized and elevated in relation to any duty the receiving attorney might have to help protect the sending attorney's duty to preserve her client's confidential material in its second metadata ethics opinion. See Pa. Op. 2009-100, *supra* note 39.

²⁴⁵ See N.H. Op. 2008-2009/4, *supra* note 12.

²⁴⁶ See Me. Op. 196, *supra* note 12.

attorneys who send such documents." ²⁴⁸ Thus, in 2009, Pennsylvania issued Formal Ethics Opinion 2009-100, ²⁴⁹ which, in contrast to Pa. Op. 2007-500, addressed the duties of both the receiving attorney and the sending attorney. While the 2009 opinion did provide additional guidance to the receiving lawyer in terms of how to exercise his or her independent professional judgment, the Committee declined to provide a bright-line rule as to whether a receiving attorney may ethically mine metadata. This is not surprising considering this was the firm conclusion of the well-reasoned opinion issued a mere two years earlier. However, Pa. Op. 2009-100 differs from Pa. Op. 2007-500 and from prior jurisdictions' metadata ethics opinions in the Committee's exploration of the receiving attorney's ethical duties to his own client in addition and in relation to the sending attorney's confidentiality duty owed to his client. As noted below, the Pennsylvania Ethics Committee concluded that "the [receiving] lawyer's duty to the lawyer's own client trumps any theoretical responsibility to protect the right of confidentiality as between another lawyer and that lawyer's client." ²⁵⁰

Pennsylvania noted in 2007 that there is no Pennsylvania Rule of Professional Conduct that specifically addresses the ethical obligations of an attorney who receives inadvertently transmitted metadata. ²⁵¹ The opinion did reference Pennsylvania Rules 1.6-Confidentiality of Information ²⁵² and 4.4(b)-Respect for Rights of Third Persons, ²⁵³ as well as the applicable comments. ²⁵⁴ These rules and [*220] comments are effectively identical to the Model Rule

²⁴⁷ Pennsylvania's second metadata ethics opinion did note that since the issuance of Pa. Op. 2007-500, "other state bar ethics committees and commentators have reviewed this issue and presented further guidance on the topic," and that the Committee had "carefully reviewed the available guidance." Pa. Op. 2009-100, *supra* note 39, at 1. As with the Pa. Op. 2007-500, the original opinion is only available to members of the Pennsylvania Bar Association at the Pennsylvania Bar Association web site's "Ethics Digest" column. See *supra* text accompanying note 242. Pa. Op. 2009-100 is undated, however, it was released in April of 2009. See E-mail from Victoria L. White, Pa. Bar Assoc., to Author (August 4, 2009, 1:45 pm) (on file with author).

²⁴⁸ Pa. Op. 2009-100, *supra* note 39, at 1.

²⁴⁹ See *id.*

²⁵⁰ *Id.* at 10.

²⁵¹ *Id.* at 1. Interestingly, and unique among the various ethics opinions, Pennsylvania also noted that there is no rule "requiring the receiving lawyer to assess whether the opposing lawyer has violated any ethical obligation to the lawyer's client." *Id.* (emphasis added).

²⁵² Pennsylvania Rule 1.6(a) reads: "A lawyer shall not reveal information relating to representation of a client unless the client gives informed consent, except for disclosures that are impliedly authorized in order to carry out the representation, and except as stated in paragraphs (b) and (c)." Pa. Rules of Prof'l Conduct R. 1.6(a) (2008). Although the language of Pennsylvania Rules 1.6 and the Model Rule 1.6 differ in presentation, the prophylactic emphasis upon not divulging confidential information remains the same in both rule versions. Compare *id.*, with Model Rules of Prof'l Conduct R. 1.6.

²⁵³ Pennsylvania Rule 4.4(b) reads: "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." Pa. Rules of Prof'l Conduct R. 4.4(b) (2008). The Pennsylvania language and the Model Rule language of Rule 4.4(b) are identical. See *id.*; Model Rules of Prof'l Conduct R. 4.4(b).

²⁵⁴ The Pennsylvania opinion included verbatim comments 2, 3, 4, 23, and 24 to Rule 1.6 and comments 2 and 3 to Rule 4.4. See Pa. Op. 2007-500, *supra* note 12.

versions.²⁵⁵ After acknowledging these two rules and their pertinent comments, the Pennsylvania Ethics Committee opined that "it is possible to conclude that the Pennsylvania Supreme Court has determined that attorneys in Pennsylvania who receive inadvertently disclosed documents have an ethical obligation to notify the sender promptly in order to permit that person to take protective measures."²⁵⁶

Having noted this possibility, the Pennsylvania Ethics Committee then looked to other jurisdictions' metadata ethics opinions for guidance. After an extensive review, the Pennsylvania opinion, in what was up to that point the most complete analysis of the then existing body of metadata ethics opinions, noted that "[t]hese various opinions reach different conclusions, although each offers a persuasive rationale."²⁵⁷ In light of this, and in light of the Committee's belief that "it would be difficult to establish a rule applicable in all circumstances," the Committee concluded that "the final determination of how to address the inadvertent disclosure of metadata should be left to the individual attorney and his or her analysis of the applicable facts."²⁵⁸

While the Pennsylvania Ethics Committee concluded in 2007 that "each attorney must 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,"²⁵⁹ the Committee also sought to provide Pennsylvania attorneys with some guidance in how to reach such a decision. The 2007 opinion listed several factors to consider, including the lawyer's judgment; the particular facts of the situation; the lawyer's view of his or her obligation under Rule 1.3-Diligence;²⁶⁰ the nature of the information received, how and from whom the information was received; the attorney-client privilege and work product rules; as well as "[c]ommon sense, reciprocity and professional courtesy."²⁶¹

Pennsylvania's initial approach is laudable for two reasons. First, it recognized that although the various jurisdictions differ in their approaches to the issue, all are based on persuasive rationales. As such, absent an initial outcome determinative approach, it is, and will remain, difficult for the legal profession as a whole to reach a consensus as to the appropriate way to

²⁵⁵ While Pennsylvania Rule 4.4(b) is identical to the Model Rule language, Pennsylvania Rule 1.6 differs slightly in the wording from the Model Rule although the import remains the same. Compare Pa. Rules of Prof'l Conduct R. 1.6, 4.4(b), with Model Rules of Prof'l Conduct R. 1.6, 4.4(b).

²⁵⁶ Pa. Op. 2007-500, *supra* note 12, at 5.

²⁵⁷ *Id.* at 9.

²⁵⁸ *Id.*

²⁵⁹ *Id.*

²⁶⁰ Pennsylvania Rule 1.3 provides: "A lawyer shall act with reasonable diligence and promptness in representing a client." Pa. Rules of Prof'l Conduct R. 1.3. The language of Pennsylvania Rule 1.3 is identical to the language of Model Rule 1.3. See *id.*; Model Rules of Prof'l Conduct R. 1.3.

²⁶¹ Pa. Op. 2007-500, *supra* note 12, at 1-2.

meld ethics and [*221] metadata.²⁶² Second, the opinion re-affirmed the trust placed in attorneys as ethical professionals in the Preamble of the Pennsylvania Rules of Professional Conduct. In fact, as can be seen from the differing approaches taken by other jurisdictions, the confluence of metadata and ethics may precisely be the kind of "difficult ethical problem" that the Preamble to the Pennsylvania Rules explains should be "resolved through the exercise of sensitive professional and moral judgment guided by the basic principles underlying the Rules."²⁶³ As such, not coming down on one side or the other with regard to the ethics of mining metadata is just as reasonable as choosing either the yes or no side.

There was, however, an unspoken concern with the initial Pennsylvania approach in that it did not provide adequate guidance beyond referencing the lofty language of the Preamble and suggesting a number of factors to consider. As acknowledged by Pa. Op. 2007-500, whether an attorney may mine metadata received in an electronically transferred document depends upon many factors. None of these factors, however, are singled out as being of more import than others. However, the admonition, and possible effect, of the comments to Pennsylvania Rule 1.3 for an attorney to act "with zeal in advocacy upon the client's behalf"²⁶⁴ cannot be discounted. The fact is, some attorneys in Pennsylvania, after having read the Pennsylvania Ethics Committee's 2007 opinion, could conclude that based on their analysis of the factors listed in Pa. Op. 2007-500, the language of the opinion and their Rule 1.3 duty to zealously represent their clients, they not only may, but should, mine the metadata in electronically transmitted documents. Knowing this, it would be very difficult for an opposing attorney to reach a contrary conclusion. While a lawyer is, of course, not "bound . . . to press for every advantage that might be realized for a client,"²⁶⁵ [*222] mining metadata in a document sent to him by opposing counsel neither involves "offensive tactics" nor treating anyone within the legal process with a disrespectful or discourteous manner, all factors that an attorney would consider

²⁶² Indeed, the Pennsylvania opinion itself is a perfect example of how different outcomes can come from the same or similar rules. The applicable Pennsylvania rules, and preamble, are virtually identical to the Model Rules. Yet, Pennsylvania found one way and the American Bar Association another.

²⁶³ Preamble 9 of the Pennsylvania Rules reads: In the nature of law practice, however, conflicting responsibilities are encountered. Virtually all difficult ethical problems arise from conflict between a lawyer's responsibilities to clients, to the legal system and to the lawyer's own interest in remaining an ethical person while earning a satisfactory living. The Rules of Professional Conduct often prescribe terms for resolving such conflicts. Within the framework of these Rules, however, many difficult issues of professional discretion can arise. Such issues must be resolved through the exercise of sensitive professional and moral judgment guided by the basic principles underlying the Rules. These principles include the lawyer's obligation zealously to protect and pursue a client's legitimate interests, within the bounds of the law, while maintaining a professional, courteous and civil attitude toward all persons involved in the legal system. Pa. Rules of Prof'l Conduct, pmbl. 9. The Pennsylvania Preamble is identical to the Model Rules Preamble in this regard. See *id.*; Model Rules of Prof'l Conduct, pmbl. 9 (2010).

²⁶⁴ See Pa. Rules of Prof'l Conduct R. 1.3, cmt. 1. The Model Rule 1.3 comments are identical to the Pennsylvania Rule in this regard. See *id.*; Model Rules of Prof'l Conduct R. 1.3, cmt. 1.

²⁶⁵ Comment 1 to Pennsylvania Rule 1.3 explains that a lawyer has an affirmative duty to act zealously on behalf of his or her client, and that a lawyer may place limits on this zealous advocacy. See Pa. Rules of Prof'l Conduct R. 1.3, cmt. 1. The comment suggests offensive tactics, courtesy and respect as some yard measures for such self-imposed limits, stating: A lawyer is not bound, however, to press for every advantage that might be realized for a client. For example, a lawyer may have authority to exercise professional discretion in determining the means by which a matter should be pursued. See Rule 1.2. The lawyer's duty to act with reasonable diligence does not require the use of offensive tactics or preclude the treating of all persons involved in the legal process with courtesy and respect. *Id.*

in not pressing for an advantage.²⁶⁶ In other words, by not taking a definitive stance one way or the other in its first metadata ethics opinion, Pennsylvania may have unwittingly unleashed the proverbial "race to the bottom,"²⁶⁷ ensuring that mining in Pennsylvania would become the norm.

As noted above, in 2009 the Pennsylvania Ethics Committee determined that its 2007 opinion both "provided insufficient guidance to recipients of documents containing metadata and did not provide correlative guidance to attorneys who send such documents."²⁶⁸ Reviewing both the sending and the receiving attorney's duties, the Committee introduced the subject in Pa. Op. 2009-100 by reaffirming the general consensus that "an attorney has an obligation to avoid sending electronic materials containing metadata."²⁶⁹ The Committee, however, from the outset, also reaffirmed its 2007 conclusion that "an attorney who receives such inadvertently transmitted information from opposing counsel may generally examine and use the metadata for the client's benefit without violating the Rules of Professional Conduct."²⁷⁰

Turning to the duties of the sending lawyer,²⁷¹ the 2009 Pennsylvania Ethics Committee noted that in the absence of a specific rule addressing the handling of metadata, "the inadvertent disclosure of metadata is analogous to the inadvertent disclosure of a document and not an act consciously undertaken by counsel."²⁷² **[*223]** Having framed the issue in such a fashion, and in clear contrast to the mining- prohibited jurisdictions that center their analyses around the view that it is precisely the deliberate act by the receiving lawyer that both frames the issue and distinguishes it from a traditional inadvertent disclosure of a document,²⁷³ the Committee looked to Rules 1.1-Competence and Rule 1.6- Confidentiality in support of its position that an

²⁶⁶ Id.

²⁶⁷ A Pennsylvania attorney who does decide he or she is ethically and professionally warranted to mine metadata and finds material that appears to be confidential and/or privileged would, presumably, be bound by Rule 4.4(b) to notify the sending attorney if he discovers metadata. As the Pennsylvania Committee on Ethics and Professional Responsibility noted in its 2009 opinion, if the receiver knows or reasonable should know that the document was inadvertently sent, he or she should "treat such metadata as an inadvertent communication under Rule 4.4(b) and promptly notify the sender of the receipt of the materials." Pa. Op. 2009-100, *supra* note 39, at 2. Similarly, Rule 8.4(c) and (d) would prohibit that attorney from reviewing or using such confidential material, and an attorney choosing to mine metadata who comes across confidential material that cannot be "put back in the bag," would run the risk of being disqualified from the case. See [RICO v. Mitsubishi Motors Corp., 171 P.3d 1092 \(Cal. 2007\)](#).

²⁶⁸ Pa. Op. 2009-100, *supra* note 39, at 1.

²⁶⁹ Id.

²⁷⁰ Id.

²⁷¹ Prior to beginning its discussion of the sending lawyer's duties, the Ethics Commission in 2009 again defined metadata as "data about data," and noted that while some metadata may contain confidential or privileged material, most metadata does not. Id. at 2. See Pa. Op. 2007-500, *supra* note 12, at 2. In an interesting side-note, the Pennsylvania Committee also noted in its 2009 opinion that metadata is "most commonly found in documents created in Microsoft Word," but can also be found in Corel WordPerfect documents. See id. at 2.

²⁷² Pa. Op. 2009-100, *supra* note 39, at 3 (emphasis added).

²⁷³ See, e.g., N.Y. Op. 749, *supra* note 12, at 4 (framing the issue as one involving "a deliberate act by the receiving attorney, not carelessness on the part of the sending attorney").

attorney has "an obligation to avoid sending electronic materials containing metadata," ²⁷⁴ and for its conclusion that "the primary burden of keeping client confidences lies with the sending attorney." ²⁷⁵ This view is in clear contrast to mining-prohibited jurisdictions that focus upon the perceived surreptitious (and to them objectionable) act of the receiving attorney in mining inadvertently transmitted metadata, while only giving lip service to the sending lawyer's sacred duty to protect his client's confidential and privileged material.

The 2009 Pennsylvania Ethics Committee, in a slight expansion of its 2007 opinion's discussion pertaining to the sending lawyer's duty of confidentiality, looked to the language of Rules 1.1 and 1.6(a), as well as to the applicable comments to support its conclusion that the primary duty of protecting a client's confidences lies with that client's attorney, not opposing counsel. In terms of Rule 1.1, the Committee noted that competent representation, which generally "requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation," ²⁷⁶ when applied to the transmittal of electronic documents, includes "insur[ing] that information that would negatively affect the client's case is not provided to an opposing party by any means, including by inadvertently embedded metadata." ²⁷⁷ Dovetailing an attorney's duty to act competently with his or her duty to protect confidentiality pursuant to Rule 1.6, ²⁷⁸ the Committee noted that comment 23 to Rule 1.6 made it clear that the "protection of a client's confidential information under Rule 1.6 is one element of competent representation under Rule 1.1." ²⁷⁹ In fact, Rule 1.6's prohibition on not revealing confidential information includes information that is clearly confidential, and as the Committee noted, extends beyond information disclosed by the client or learned during the representation of the client to "material which provides access to such protected content." ²⁸⁰ The Committee made it clear that "[e]xcept in situations in which [*224] metadata is intentionally included in a transmitted document, metadata will generally fall within this category." ²⁸¹ Finally, in support of its directive that the sending lawyer has an obligation to avoid sending metadata, the Pennsylvania Ethics Committee noted that comment 24 to Rule 1.6, "without reference to the term 'metadata,' speaks clearly to the lawyer's duty to protect the client's information in transmitting electronic

²⁷⁴ Pa. Op. 2009-100, supra note 39, at 1-2.

²⁷⁵ Id. at 2 (emphasis added).

²⁷⁶ Pennsylvania Rule 1.1 provides: "A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation." Pa. Rules of Prof'l Conduct R. 1.1.

²⁷⁷ Pa. Op. 2009-100, supra note 39, at 4.

²⁷⁸ See supra text accompanying note 252.

²⁷⁹ Pa. Op. 2009-100, supra note 39, at 4. Comment 23 to Pennsylvania Rule 1.6 reads: "A lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision." Pa. Rules of Prof'l Conduct R.1.6, cmt. 23.

²⁸⁰ Pa. Op. 2009-100, supra note 39, at 4 (emphasis added). Comment 4 to Pennsylvania Rule 1.6 reads, in relevant part: "Paragraph (a) prohibits a lawyer from revealing information relating to the representation of a client. This prohibition also applies to disclosures by a lawyer that do not in themselves reveal protected information but could reasonably lead to the discovery of such information by a third person." Pa. Rules of Prof'l Conduct R. 1.6, cmt. 4.

²⁸¹ Pa. Op. 2009-100, supra note 39, at 4 (emphasis added).

documents" ²⁸² by mandating that "[w]hen transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients." ²⁸³

Thus, the 2009 Pennsylvania ethics opinion adopted the unanimous view among ethics committees that the sender has an ethical duty to take reasonable precautions to avoid disclosing confidential material through the transmission of electronic documents. In contrast to other ethics opinions, however, Pennsylvania did not shirk from the confidentiality duty imposed upon the sending attorney in relation to the perceived duty of the receiving attorney to not engage in conduct (mining) that might negatively affect or breach the sending attorney's duty to protect his client's confidentiality. Rather, regardless of what the sending attorney may do, Pennsylvania affirmatively held that the primary duty of protecting client confidences lies with the attorney who is transmitting electronic documents that may contain client confidences.

Having affirmed the duty on the part of the sending lawyer to preserve his client's confidences, the Pennsylvania Ethics Committee turned to the related duties of the receiving attorney. Here, as with its discussion of the duties of the sending attorney, the Committee resisted the temptation to limit its focus to the issue of how the receiving attorney's conduct may interfere with or affect the sending lawyer's duty to protect his client's confidences, and chose instead to expand its analysis to cover the receiving lawyer's duties to his client. In doing so, the Committee looked not only to Rule 4.4(b), ²⁸⁴ but also to the receiving attorney's competence duties under Rule 1.1, ²⁸⁵ the appropriate allocation of [*225] authority between the attorney and the client in terms of the receiving attorney abiding by the client's wishes concerning the objectives of the representation under Rule 1.2, ²⁸⁶ and the attorney's duty to keep the client informed pursuant to Rule 1.4. ²⁸⁷

²⁸² Id. at 5.

²⁸³ Id. (quoting Pa. Rules of Prof'l Conduct R. 1.6, cmt. 24). Paragraph 24 of Pennsylvania Rule 1.6 reads in its entirety: When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule. Id.

²⁸⁴ Pa. Rules of Prof'l Conduct R. 4.4(b).

²⁸⁵ Pa. Rules of Prof'l Conduct R. 1.1.

²⁸⁶ Pennsylvania Rule 1.2 consists of four sections. See Pa. Rules of Prof'l Conduct R. 1.2. The Pennsylvania Bar Association Committee on Legal Ethics and Professional Responsibility, in Pa. Op. 2009-100, excerpted the first part of Rule 1.2, section (a), as the pertinent part for metadata: Subject to paragraphs (c) and (d), a lawyer shall abide by a client's decisions concerning the objectives of representation and, as required by Rule 1.4, shall consult with the client as to the means by which they are to be pursued. A lawyer may take such action on behalf of the client as is impliedly authorized to carry out the representation. Pa. Op. 2009-100, *supra* note 39, at 6 (quoting Pa. Rules of Prof'l Conduct R. 1.2(a)).

²⁸⁷ Pennsylvania Rule 1.4 is comprised of three sections: sections (a) and (b) are applicable in this context; section (c) deals with a lawyer not having professional liability insurance informing the client of such. See Pa. Rules of Prof'l Conduct R. 1.4. Section (a), quoted in part by Pa. Op. 2009-100, mandates that a Pennsylvania lawyer shall: [P]romptly inform the client of any

The Pennsylvania Ethics Committee noted in 2007-500 that it was "possible" for an attorney who receives inadvertently disclosed documents to have an ethical obligation to notify the sender.²⁸⁸ The 2009 Committee re-stated this notion more affirmatively in Pa. Op. 2009-100 when it opined that Rule 4.4(b), and its comments, "demonstrate that attorneys in Pennsylvania who receive inadvertently disclosed documents have an ethical obligation to promptly notify the sender."²⁸⁹ The Committee also concluded, as it had in 2007, that "any action other than reporting is purely a matter of intra-professional courtesy and the lawyer's sound judgment or substantive law."²⁹⁰ The Committee specifically cited to comments 2 and 3 of Pennsylvania Rule 4.4 in support of this conclusion.²⁹¹ With the exception [*226] of moving from a possibility to an affirmative duty to notify the sending attorney of inadvertently received material, the overall conclusion arrived at in the 2009-100 opinion did not differ from the 2007-100, nor did it stray from the general view previously espoused by mining-permitted jurisdictions such as the ABA, Maryland, the District of Columbia, and Colorado. Where the 2009-100 opinion differed from both Pa. Op. 2007-500 and other prior metadata ethics opinions, however, was in its discussion of the overall pertinent and applicable duties that should be considered. Although prior decisions had focused on the sending attorney's duty of confidentiality to his client, and a perceived duty on the part of the receiving attorney not to use inadvertently transmitted metadata because such use would, as New York put it, "violate the letter and the spirit" of the rules,²⁹² Pa. Op. 2009-100 also considered the receiving lawyer's duty to his own client, and concluded that "the lawyer's duty to the lawyer's own client trumps any theoretical responsibilities to protect the right of confidentiality as between another lawyer and that lawyer's client."²⁹³ The Pennsylvania Ethics Committee did not arrive at this conclusion in a vacuum. Instead, it looked to the applicable existing rules that, in the opinion of the Committee, clearly spelled out the duty of the receiving attorney towards his own client in the metadata context. First, the

decision or circumstances with respect to which the client's informed consent, as defined in Rule 1.0(e), is required by these Rules; (2) reasonably consult with the client about the means by which the client's objectives are to be accomplished; (3) keep the client reasonably informed about the status of the matter; and (4) promptly comply with reasonable requests for information; and (5) consult with the client about any relevant limitation on the lawyer's conduct when the lawyer knows that the client expects assistance not permitted by the Rules of Professional Conduct or other law. See *id.*; Pa. Op. 2009-100, *supra* note 39, at 7-8. Section (b), also quoted in Pa. Op. 2009-100, mandates that "[a] lawyer shall explain to the extent necessary to permit the client to make informed decisions regarding the representation." See Pa. Rules of Prof'l Conduct R. 1.4; Pa. Op. 2009-100, *supra* note 39, at 8.

²⁸⁸ Pa. Op. 2007-500, *supra* note 12, at 5.

²⁸⁹ Pa. Op. 2009-100, *supra* note 39, at 6.

²⁹⁰ *Id.*

²⁹¹ *Id.* Comments 2 and 3 to Pennsylvania Rule 4.4 contain language specifically on point and support the Committee's conclusion in this regard. See Pa. Rules of Prof'l Conduct R. 4.4, cmts. 2-3. Comment 2 provides, in relevant part: If a lawyer knows or reasonably should know that a document was sent inadvertently, then this Rule requires the lawyer to promptly notify the sender in order to permit that person to take protective measures. Whether the lawyer is required to take additional steps, such as returning the original document, is a matter of law beyond the scope of these Rules . . . *Id.* at cmt. 2 (emphasis added). Similarly, Comment 3 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. *Id.* at cmt. 3 (emphasis added).

²⁹² N.Y. Op. 749, *supra* note 12, at 3.

²⁹³ Pa. Op. 2009-100, *supra* note 39, at 10 (emphasis added).

Committee categorized "unintentionally embedded metadata as an inadvertent disclosure" falling under the purview of Rule 4.4(b).²⁹⁴ The Committee, however, acknowledged the "knows or reasonably knows" qualification contained therein and noted that as a result, Rule 4.4(b) must be read in conjunction with the "knowing," "reasonable or reasonably," and "reasonably should know" definitions of Rule 1.0.²⁹⁵ Thus, the first step a Pennsylvania attorney must take when faced with the receipt of an electronic document that includes metadata is to discern whether the "extra-textual information was intended to be deleted or scrubbed from the document prior to transmittal."²⁹⁶ The mere existence of metadata does not warrant a conclusion of inadvertence.²⁹⁷ Rather, the Committee, possibly harking back to the view espoused in Pa. Op. 2007-500 that Pennsylvania lawyers truly are able to "resolve hical issues] through the exercise of sensitive and moral judgment guided by the [*227] basic principles of the Rules,"²⁹⁸ held that a conscious effort to discern whether the metadata was inadvertently included be undertaken by the receiving attorney. The Committee suggested that inadvertence would be obvious-such as when the information is accessible "only by means such as viewing tracked changes or other mining techniques," while other times the deliberate inclusion of the metadata would be equally obvious-such as "where a covering document may advert to the intentional inclusion of metadata."²⁹⁹ Regardless, and as noted above, once a Pennsylvania attorney concludes that metadata was inadvertently included, he or she has a duty under Rule 4.4(b) to notify the sending attorney of the receipt of such material.³⁰⁰ Up to that point, Pa. Op. 2009-100 had been similar, albeit more detailed and comprehensive in its rationale, to most mining-permissible jurisdictions.³⁰¹ What Pa. Op. 2009-100 suggested next, however, was unique. Once an attorney has decided whether Rule 4.4(b) requires notification, the lawyer must then determine whether his duties to his own client, as prescribed by Rules 1.1, 1.2, and 1.4, "require the attorney to either disclose to or withhold from the client the fact and content of the inadvertently transmitted document."³⁰² If the applicable tribunal, current or future, may find use of the metadata improper or if such use may negatively impact

²⁹⁴ Id. at 5.

²⁹⁵ Pa. Rules of Prof'l Conduct R. 1.0 provides the following definitions: (f) "Knowingly," "Known," or "Knows" denotes actual knowledge of the fact in question. A person's knowledge may be inferred from circumstances; (h) "Reasonable" or "Reasonably" when used in relation to conduct by a lawyer denotes the conduct of a reasonably prudent and competent lawyer; (j) "Reasonably should know" when used in reference to a lawyer denotes that a lawyer of reasonable prudence and competence would ascertain the matter in question. Id.

²⁹⁶ Pa. Op. 2009-100, *supra* note 39, at 6.

²⁹⁷ Id.

²⁹⁸ Pa. Op. 2007-500, *supra* note 12, at 1 (quoting Pa. Rules of Prof'l Conduct pmbl. 9).

²⁹⁹ Pa. Op. 2009-100, *supra* note 39, at 6.

³⁰⁰ Id. As in 2007, the Pennsylvania Bar Association Committee on Legal Ethics and Professional Responsibility did note that whether any additional action is warranted by the attorney in addition to notifying the sending attorney is left to the receiving attorney's sound professional judgment. Pa. Op. 2007-500, *supra* note 12, at 6; Pa. Op. 2009-100, *supra* note 39, at 6. The 2009 opinion, however, also acknowledged and discussed the significance of the confluence of additional rules upon this decision making process. See Pa. Op. 2009-100, *supra* note 39, at 7.

³⁰¹ Out of the mining-permitted jurisdictions, Maryland is unique in that its Rules do not impose a notification requirement upon an attorney receiving inadvertently transmitted information.

³⁰² Pa. Op. 2009-100, *supra* note 39, at 7.

future dealings with opposing counsel, both or either potentially resulting in adverse consequences to the client, "the attorney may refrain from disclosing or using" the information.³⁰³ On the other hand, if the information gleaned from the inadvertently received metadata is beneficial to the client and can be used without adverse impact, "then Rule 1.1 may require that the attorney do so."³⁰⁴

While Pa. Op. 2009-100 acknowledged that an attorney may decide not to inform his or her client about the received metadata, his duties to his client pursuant to Rule 1.2-Scope of Representation and Allocation of Authority Between Client and Lawyer,³⁰⁵ and Rule 1.4-Communication,³⁰⁶ may combine to require disclosure to his client. Under Rule 1.4, the lawyer is required to inform his client of significant developments pertaining to the case, as well as provide sufficient information to enable the client to make informed decisions concerning the objectives of representation pursuant to Rule 1.2.³⁰⁷ Even in situations where **[*228]** the lawyer concludes that "disclosure of the substance of the metadata to the client may negatively affect the process or outcome of the case,"³⁰⁸ in most cases the attorney still has a duty to advise the client of the receipt of the metadata and the reason for his nondisclosure.³⁰⁹ At that point, "[t]he client may then make an informed decision whether the advantages of examining or utilizing the metadata outweigh the disadvantages of doing so."³¹⁰ Regardless of the conclusion reached by the attorney, the significance in terms of metadata ethics opinion jurisprudence is that the duties he must consider and apply are the duties he owes to his client. In the metadata ethics context, it is the emphasis placed on this duty that makes the Pennsylvania approach both unique in its own right, and more thorough than all prior and subsequent metadata ethics opinions.

I. Colorado: Mining Permitted

Colorado joined the metadata ethics fray in May of 2008. After examining all previous metadata ethics opinions, pertinent Rules of Professional Conduct, and prior Colorado ethics opinions, the Ethics Committee of the Colorado Bar Association (Colorado Ethics Committee) concluded that "the ABA, Maryland, and District of Columbia opinions are better reasoned, and that the New York, Arizona, Alabama[,] and Florida opinions are based on incorrect factual premises regarding the nature of metadata."³¹¹ As such, in Colorado, "a [r]eceiving [l]awyer generally

³⁰³ Id.

³⁰⁴ Id.

³⁰⁵ See supra text accompanying note 286.

³⁰⁶ See supra text accompanying note 287.

³⁰⁷ Pa. Op. 2009-100, supra note 39, at 7.

³⁰⁸ Id. at 8.

³⁰⁹ Id.

³¹⁰ Id.

³¹¹ Colo. Op. 119, supra note 12.

may ethically search for and review metadata embedded in an electronic document" received from opposing counsel or a third party.³¹²

The Colorado opinion initially noted that not all metadata is of significance, and that not all metadata is confidential. Some metadata, however, "such as hidden comments or redlines," can be confidential information.³¹³ For purposes of the opinion, the Colorado Ethics Committee defined "[c]onfidential [i]nformation" to "include information that is subject to a legally recognized exemption from discovery and use in civil, criminal, or administrative action or proceeding, even if it is not privileged."³¹⁴ The opinion then discussed the contrasting duties of the sending lawyer and the receiving lawyer in the traditional fashion, and firmly rejected the original New York view that mining of metadata is surreptitious and prohibited.

In terms of the sending lawyer's duties, Colorado noted that a sending lawyer has a duty to "take steps to reduce the likelihood that metadata containing [c]onfidential [i]nformation" is included in electronically transmitted documents.³¹⁵ Joining all prior ethics opinions on the matter, Colorado noted that this duty stems **[*229]** from the sending lawyer's Rule 1.6 duty to safeguard client information,³¹⁶ the lawyer's Rule 1.1 competence requirement,³¹⁷ and a lawyer's Rule 5.1 and 5.3 duties³¹⁸ "to ensure that the lawyer's firm, including lawyers and non-lawyers, conform to the rules."³¹⁹ These rules together, "require 'a [s]ending [l]awyer to use reasonable care to ensure that metadata that contain [c]onfidential [i]nformation are not disclosed to a third party.'"³²⁰ What constitutes "reasonable care" will depend upon the facts and circumstances of a given situation. Therefore, appropriate precautions could include:

³¹² Id.

³¹³ Id.

³¹⁴ Id. (citing Colo. State Bar Ass'n Comm. on Ethics, Formal Op. 108 (2000), <http://www.cobar.org/index.cfm/ID/386/subID/1830/CETH/Ethics-Opinion-108:-Inadvertent-Disclosure-of-Privileged-or-Confidential-Documents,-05/20/00/> (last visited Nov. 11, 2010) [hereinafter Colo. Op. 108]).

³¹⁵ Colo. Op. 119, supra note 12.

³¹⁶ Colorado's Rule 1.6 is substantially similar to the Model Rule 1.6, the differences occurring in sub-section (b) dealing with the instances when a lawyer may reveal information relating to the representation of a client, none of which are applicable in this context. Compare Colo. Rules of Prof'l Conduct R. 1.6 (2008), available at <http://www.cobar.org/index.cfm/ID/384/CETH/Colorado-Rules-of-Professional-Conduct> (last visited Nov. 11, 2010), with Model Rules of Prof'l Conduct R. 1.6. Paragraph (a) of Colorado Rule 1.6 provides: "A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation, or the disclosure is permitted by paragraph (b)." Colo. Rules of Prof'l Conduct R. 1.6(a).

³¹⁷ Colorado Rule 1.1 is identical to the Model Rule 1.1, providing: "A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation." See Colo. Rules of Prof'l Conduct R. 1.1; Model Rules of Prof'l Conduct R. 1.1.

³¹⁸ Colorado Rule 5.1 requires, in part, that law firm partners and supervisory attorneys ensure that lawyers, over whom they have control conform to the Rules of Professional Conduct, while Rule 5.2 similarly requires that law firm partners and supervisory attorneys ensure that non-lawyers retained or associated with the lawyer's actions are compatible with the professional obligations of the lawyer. See Colo. Rules of Prof'l Conduct R. 5.1, 5.3.

³¹⁹ Colo. Op. 119, supra note 12.

³²⁰ Id. In a nod to the unanimity of thought on this point, the opinion cited to all prior ethics opinions regardless of their ultimate conclusion in terms of whether mining is permissible or not, as well as to prior Colorado Ethics Opinions 108 and 90. See Colo. Op. 108, supra note 314; Colo. State Bar Ass'n Comm. on Ethics, Formal Op. 90 (1992), available at

avoiding the creation of certain metadata by "choosing not to use redlining or hidden comments" in a document that will be electronically transmitted; using programs to scrub the metadata; or simply printing out electronic document "in order to ensure absolutely that no unseen metadata of any kind are included."³²¹ The latter extreme would be appropriate in circumstances when "it is vital that no metadata be transmitted."³²² The opinion also noted that lawyers may want to retain experts in computer software and hardware to aid them in this regard.³²³

Regardless of the methods a sending lawyer uses to ensure compliance with his ethical duties pursuant to Rules 1.6, 1.1, 5.1, and 5.3, what differentiates the Colorado Ethics Committee's view from the jurisdictions prohibiting mining is its focus on the actions of the sending attorney. The Committee noted that "[t]he [*230] ultimate responsibility for control of metadata rests with the [s]ending [l]awyer."³²⁴ While other jurisdictions place the burden on the receiving lawyer and prohibit mining based on the astounding assumption that a sending lawyer will not be able to fulfill his competence and confidentiality obligations pursuant to Rules 1.1 and 1.6,³²⁵ the Committee firmly rejected this view, noting that "a [s]ending [l]awyer may not limit the duty to exercise reasonable care in preventing the transmission of metadata that contain [c]onfidential [i]nformation by remaining ignorant of technology relating to metadata or failing to obtain competent computer support."³²⁶ Colorado, in other words, recognized that, contrary to the belief that unless mining is banned, "the sending lawyer would be at the mercy of the recipient lawyer,"³²⁷ it is the sending lawyer who controls whether metadata is transmitted in the first place. As a result, the solution is simple: expect all attorneys to comply with their ethical duties, including the duty of competence and the duty to preserve client confidences.

Although Colorado emphasized that the initial burden falls on the sending lawyer, the opinion also recognized that the receiving lawyer has certain duties when he or she receives metadata. The opinion divided the receiving lawyer's duties into two distinct situations. The first was whether a lawyer "may review metadata," the second being what a receiving lawyer "must do when he or she receives metadata that appear to contain [c]onfidential [i]nformation."³²⁸

In terms of whether a lawyer may review metadata, the Colorado opinion noted the split among jurisdictions. However, rejecting the mining prohibition view, Colorado reasoned that these jurisdictions' ethics opinions fail in two respects: first, they "appear to be based on an implied

<http://www.cobar.org/index.cfm/> ID/386/subID/1811/CETH/Ethics-Opinion-90:-Preservation-of-Client-Confidences-in-View-of-Modern-Communications-Technology,-11, (last visited Nov. 11, 2010) [hereinafter Colo. Op. 90]. Colo. Op. 90 concluded that "[a] lawyer must exercise reasonable care when selecting and using communication devices in order to protect the client's confidences or secrets from unintended disclosure." Colo. Op. 90, *supra*.

³²¹ Colo. Op. 119, *supra* note 314.

³²² *Id.*

³²³ *Id.*

³²⁴ *Id.* (emphasis added).

³²⁵ See Ariz. Op. 07-03, *supra* note 12.

³²⁶ Colo. Op. 119, *supra* note 12.

³²⁷ See Ariz. Op. 07-03, *supra* note 12 (emphasis added).

³²⁸ Colo. Op. 119, *supra* note 12.

premise that searching for metadata is surreptitious or otherwise involves procedures that are difficult or complicated"; ³²⁹ second, these opinions not only "seem to assume that metadata generally contain [c]onfidential [i]nformation," but also that "any metadata transmitted to a third party must, therefore, have been transmitted inadvertently." ³³⁰

Colorado squarely rejected both of these assumptions in three logical steps. First, the opinion noted that "there is nothing inherently deceitful or surreptitious about searching for metadata." ³³¹ Indeed, some metadata can be revealed by simply "passing a computer cursor over a document." ³³² As such, the opinion noted that "[r]eferring to searching for metadata as 'mining' or 'surreptitiously 'get[ting] behind'" a document is misleading. ³³³ Second, not all metadata contains confidential information. In fact, some metadata may be intended by the sending lawyer to be reviewed by the receiving lawyer. An "absolute ethical ban" on [*231] reviewing metadata "ignores" this simple fact. ³³⁴ In other words, Colorado argued that it is not the act of reviewing metadata in and of itself that is objectionable. Rather, it is the viewing of confidential material that may result from such an act that is prohibited by the rules. Finally, and further supporting the notion that the mere act of reviewing metadata is not per se objectionable, the Colorado Ethics Committee noted that "metadata [is] often of no import." ³³⁵ Once one accepts these truisms, and "discards the notions that it is dishonest or deceitful to search for or to look at metadata or that metadata typically contain significant [c]onfidential [i]nformation," ³³⁶ the rational and logic of Colorado Ethics Opinion 119's conclusion is obvious. Because there "is no Rule in the Colorado Rules of Professional Conduct that contains any prohibition on a lawyer generally reviewing or using information received from opposing counsel or other third party . . . a [r]eceiving [l]awyer generally may search for and review any metadata included in an electronic document or file." ³³⁷

While there are no rules that prohibit a Colorado lawyer from reviewing metadata, once a lawyer discovers material that appears to contain confidential information, the Colorado Ethics Committee made clear that Colorado Rule 4.4 governs his or her conduct. Colorado Rule 4.4-Respect for Rights of Third Persons, is more specific than the equivalent rule in the other jurisdictions that have issued opinions pertaining to metadata. Colorado Rule 4.4 includes the same prohibition on embarrassing third persons or obtaining evidence in ways that violate the rights of third persons as do these other jurisdictions and the Model Rule version in paragraph

³²⁹ Id. Colorado based this conclusion upon other ethics opinions' "use of such language as 'mining.'" Id.

³³⁰ Id. (emphasis added).

³³¹ Id.

³³² Id.

³³³ Id.

³³⁴ Colo. Op. 119, supra note 12.

³³⁵ Id.

³³⁶ Id.

³³⁷ Id.

(a).³³⁸ Similarly, subsection (b) tracks the Model Rule language mandating notification (only) when the receiving lawyer "knows or should know" that the document was "inadvertently sent."

³³⁹ Unlike the Model Rule, and unlike the equivalent rule in all of the jurisdictions that have issued metadata ethics opinions, Colorado Rule 4.4 also prohibits an attorney who has received notice from the sender that "the document was inadvertently sent" from examining the document and mandates that he abide by the sender's instructions.³⁴⁰

In applying the plain language of Rule 4.4 to documents that contain metadata, the Colorado Ethics Committee noted that because a sending lawyer is presumed to comply with his or her Rule 1.1 competence and Rule 1.6 confidence duties, and [*232] would thus not intentionally transmit confidential information to an opposing party or to a third party, "a [r]eceiving [l]awyer reasonably should believe that any [c]onfidential [i]nformation contained in metadata received from [a] [s]ending [l]awyer was transmitted inadvertently."³⁴¹ As such, Rule 4.4(b) mandates that the receiving lawyer notify the sending lawyer. While the receiving lawyer and sending lawyer may at that point, "as a matter of professionalism," discuss what the appropriate next step should be,³⁴² absent notice of inadvertent transmittal prior to reviewing the metadata, the receiving lawyer is not ethically prohibited "from continuing to review the electronic document or file and its associated metadata."³⁴³

The Colorado Ethics Committee acknowledged, but specifically disagreed with, the District of Columbia's reliance upon Rule 8.4(c) in finding that a receiving lawyer must stop reviewing documents when he or she has "actual knowledge that the [s]ending [l]awyer did not intend to disclose [c]onfidential [i]nformation in the metadata."³⁴⁴ Noting that Rules 4.4(b) and 4.4(c) "are the more specific rules," they "trump the more general requirements of Rule 8.4(c)."³⁴⁵ However, and logically following the literal reading of the applicable rules, when a Colorado lawyer receives notice from the sending lawyer, prior to reviewing received metadata, that

³³⁸ Colorado Rule 4.4(a) provides: "In representing a client, a lawyer shall not use means that have no substantial purpose other than to embarrass, delay, or burden a third person, or use methods of obtaining evidence that violate the legal rights of such a person." Colo. Rules of Prof'l Conduct R. 4.4(a).

³³⁹ Colorado Rule 4.4(b) provides: "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." Colo. Rules of Prof'l Conduct R. 4.4(b).

³⁴⁰ Colorado Rule 4.4(c) provides: 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. Colo. Rules of Prof'l Conduct R. 4.4(c).

³⁴¹ Colo. Op. 119, *supra* note 12.

³⁴² *Id.* (noting that the parties might discuss whether a waiver of privilege or confidentiality had occurred, seek to agree on how to handle the matter, and/or seek a court determination).

³⁴³ *Id.* (emphasis added).

³⁴⁴ *Id.* Colorado Rule 8.4(c) holds that it is professional misconduct for a lawyer to "engage in conduct involving dishonesty, fraud, deceit or misrepresentation." Colo. Rules of Prof'l Conduct R. 8.4. Colorado Rule 8.4(c) is identical to the District of Columbia Rule 8.4(c) and the Model Rule 8.4(c). Compare *id.*, with D.C. Rules of Prof'l Conduct R. 8.4(c), and Model Rules of Prof'l Conduct R. 8.4(c).

³⁴⁵ Colo. Op. 119, *supra* note 12.

metadata contains confidential information, pursuant to Rule 4.4(c), "the [r]eceiving [l]awyer must not examine the metadata and must abide by the [s]ending [l]awyer's instructions regarding the disposition of the metadata." ³⁴⁶

Colorado, like all jurisdictions that permit mining, would not be opposed to attorneys forming a bilateral agreement to refrain from mining each other's metadata. Just as the sending lawyer and receiving lawyer are not required, but may "as a matter of professionalism," discuss whether a waiver of privileged or confidential material has occurred after a receiving lawyer notifies the sending lawyer of his discovery of confidential material during his review of metadata, so may both attorneys, as a matter of professionalism, agree amongst themselves that mining will not take place. In other words, in Colorado, as in all jurisdictions, attorneys are always free to abide by a "higher" professional path than the minimum ethical conduct prescribed by the ethical rules. Thus, there is nothing prohibiting attorneys from agreeing to refrain from mining each other's electronic documents. And, as in other jurisdictions, the breach of such an agreement would constitute "conduct involving dishonesty, fraud, deceit or misrepresentation" as [*233] well as possibly "conduct that is prejudicial to the administration of justice." ³⁴⁷ In this regard, Colorado is similar to all jurisdictions that permit mining.

Colorado, however, differs from the other jurisdictions in that Colorado Rule 4.4(c) permits one attorney to unilaterally prohibit other attorneys from mining electronic documents. As noted above, Colorado Rule 4.4(c) mandates that "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." ³⁴⁸ As such, a Colorado attorney who electronically transmits a document to another attorney could attach a notice to the effect that the document has been scrubbed of metadata, and that any metadata that may remain "was inadvertently sent." Under Colorado Rule 4.4(c), the receiving attorney would then be required to refrain from examining the document (in this context refrain from mining the metadata) and abide by the sending attorney's instructions. Colorado, in other words, explained that mining of metadata is generally permitted, but also provided a ready made mechanism through its rules that enables any one attorney to prevent another attorney from mining metadata. All that is required is a unilateral notice informing the receiving lawyer that any metadata was inadvertently transmitted.

J. Maine: Mining Prohibited

Maine became the latest jurisdiction to issue a metadata ethics opinion in 2008, ³⁴⁹ and is one of three jurisdictions that have adopted new ethical rules subsequent to issuing ethics opinions pertaining to the mining of metadata. Like Alabama, but unlike New York, the abrogation of the

³⁴⁶ Id.

³⁴⁷ Colorado Rule 8.4, sections (c) and (d) are identical to the Model Rule versions. Compare Colo. Rules of Prof'l Conduct R. 8.4(c)-(d), with Model Rules of Prof'l Conduct R. 8.4(c)-(d). Colorado Rule 8.4(d) provides that it is misconduct for a lawyer to "engage in conduct that is prejudicial to the administration of justice." Colo. Rules of Prof'l Conduct R. 8.4(d).

³⁴⁸ Colo. Rules of Prof'l Conduct R. 4.4(c).

³⁴⁹ Me. Op. 196, *supra* note 12.

old ethical rules and the adoption of the Maine Rules of Professional Conduct (effective August 1, 2009) ³⁵⁰ did not change Maine's view on the mining of metadata: the mining of metadata was prohibited under the now abrogated Maine Code of Professional Responsibility and remains prohibited under the Maine Rules of Professional Conduct.

In late 2008, the Professional Ethics Commission of the Board of Overseers of the Maine Bar (Maine Ethics Commission), in an opinion that carefully examined the rationale and reasoning of the nine jurisdictions that had previously issued metadata ethics opinions, looked to prior Maine ethics opinions, interpreted the Maine Code of Professional Responsibility, and drew guidance from a 1999 opinion by the Maine Supreme Judicial Court, ³⁵¹ concluded that absent court authorization, "it is ethically impermissible for an attorney to seek to uncover [*234] metadata embedded in an electronic document received from counsel for another party, in an effort to detect confidential information that should be reasonably known not to have been intentionally communicated." ³⁵² In doing so, Maine rejected the jurisdictions that permit the mining of metadata, and "believ[ing] that the better view is that generally expressed by New York and the jurisdictions that have followed it," ³⁵³ strongly prohibited the mining of metadata in Maine. In terms of the sending attorney's duties, Maine followed the general consensus and concluded that "the sending attorney has an ethical duty to use reasonable care when transmitting an electronic document to prevent the disclosure of metadata containing confidential information." ³⁵⁴

Addressing the sending attorney's duties, Maine noted that there is a "relative unanimity" among the jurisdictions that have examined the issue. ³⁵⁵ As such, the Maine Ethics Commission found that the sending attorney is "ethically required to take reasonable measures to avoid the communication of confidential information, regardless of the mode of transmission." ³⁵⁶ For an attorney transmitting electronic documents, this duty includes taking measures to "prevent the disclosure of metadata containing confidential information." ³⁵⁷ Some measures that the Commission suggested a sending attorney could take included converting the document to

³⁵⁰ The Maine Rules of Professional Responsibility were replaced by the Maine Rules of Professional Conduct, effective as of August 1, 2009. See generally Me. Rules of Professional Conduct, available at <http://www.mebareoverseers.org/attorney-regulation/professional-conduct/> (last visited Nov. 11, 2010).

³⁵¹ [Corey v. Norman, Hanson & Detroy, 1999 ME 196, 742 A.2d 933.](#)

³⁵² Me. Op. 196, *supra* note 12.

³⁵³ *Id.* Interestingly, and tellingly as to how different ethics committees examining similar, if not identical, rules use similar justifications and rationales in reaching inapposite conclusions, Maine termed the mining-prohibited jurisdictions "the better view," while Colorado called the mining-permitted jurisdictions "better reasoned." See *id.*; Colo. Op. 119, *supra* note 12. Pennsylvania in 2007 also recognized this anomaly, politely noting that "various opinions reach different conclusions, although each offers a persuasive rationale." See Pa. Op. 2007-500, *supra* note 12, at 9.

³⁵⁴ Me. Op. 196, *supra* note 12.

³⁵⁵ *Id.*

³⁵⁶ *Id.* (emphasis added).

³⁵⁷ *Id.*

generic files, such as PDF, or resorting to paper copies.³⁵⁸ Although a sending attorney's ethical duties may not dictate that he or she retain a computer expert, the Commission noted that it "d[id] not believe it reasonable for an attorney today to be ignorant of the standard features and capabilities of word processing and other software" used in the legal profession.³⁵⁹

While Maine's rationale with regard to the sending attorney's duties brought forth some practical suggestions, it is Maine's reasoning with regard to the receiving attorney's duties that is most telling in the overall context of permitting or prohibiting the mining of metadata. In reaching its conclusion that the mining of metadata was ethically impermissible, the Maine Ethics Commission reviewed the New York, Florida, and Alabama metadata opinions that prohibited mining, and the ABA, Maryland, and Colorado opinions that permitted it, as well as Pa. Op. 2007-500 (terming it a "default" result) and the District of Columbia opinion (noting the District's actual knowledge threshold).³⁶⁰

Recognizing that none of the Maine Rules of Professional Responsibility specifically addressed the metadata situation, the Maine Ethics Commission looked **[*235]** to the general proscriptions against conduct deemed dishonest and against the administration of justice. Under the Maine Code of Professional Responsibility Rules, these proscriptions were found in Bar Rule 3.2(f)(3) and (4).³⁶¹ Recognizing the generality of these wide proscriptions, the Commission noted that it was "appropriately cautious in its specific application of the general proscription in Bar Rule 3.2(f)(3) and (4)."³⁶² Having noted this disclaimer of sort, the Commission then, like the New York Ethics Committee in 2001, phrased the issue in such a way as to foreshadow the outcome: Maine Ethics Opinion 196 declared that:

[A]n attorney who purposefully seeks to unearth confidential information embedded in metadata attached to a document provided by counsel for another party, when the attorney knows or should know that the information involved was not intended to be disclosed, has acted outside of these broad ethical requirements [i.e., Maine Bar Rule 3.2(f)(3) and (4)].³⁶³

Just as the New York State Bar Committee on Professional Ethics would have been hard pressed to have found that a New York attorney could "surreptitiously" examine electronic

³⁵⁸ Id.

³⁵⁹ Id.

³⁶⁰ Me. Op. 196, *supra* note 12.

³⁶¹ Id. Rules 3.2(f)(3) of the old Maine Code of Professional Responsibility made it unethical for a Maine lawyer to "engage in conduct involving dishonesty, fraud, deceit, or misrepresentation," while 3.2(f)(4) made it unethical to "engage in conduct that is prejudicial to the administration of justice." Me. Code of Prof'l Responsibility R. 3.2(f)(3)-(4) (2008) (abrogated Aug. 1, 2009). The equivalent rules in the Maine Rules of Professional Conduct, Rule 8.4(c) and (d), contain identical language. Compare Me. Code of Prof'l Responsibility R. 3.2(f)(3)-(4), with Me. Rules of Prof'l Conduct R. 8.4(c)-(d). Maine Rule 8.4(c) and (d) are identical to the Model Rule 8.4(c) and (d). See Me. Rules of Prof'l Conduct R. 8.4(c)-(d); Model Rules of Prof'l Conduct R. 8.4(c)-(d).

³⁶² Me. Op. 196, *supra* note 12.

³⁶³ Id. (emphasis added) (citing Me. Code of Prof'l Responsibility R. 3.2(f)(3)-(4)).

documents in order to "get behind' what is visible on the computer screen," ³⁶⁴ so it would have been equally difficult for the Maine Ethics Commission to have found that a Maine attorney could, under any circumstances, "purposefully seek[] to unearth confidential information." ³⁶⁵ In fact, after defining the issue as one of purposefully seeking to unearth what the attorney knows (or should know) to be confidential information, the Commission noted that Bar Rule 3.2(f)(3) and (4) would be meaningless if not applied in this situation and that such "conduct strikes at the foundational principles that protect attorney-client confidences, and in doing so it clearly prejudices the administration of justice." ³⁶⁶

While the Maine Ethics Commission noted its concern in applying the general proscriptions of Bar Rule 3.2(f)(3) and (f)(4) too widely, the Commission found that the Maine Supreme Judicial Court had provided guidance with regard to the use of inadvertently disclosed confidential information in an earlier opinion entitled *Corey v. Norman*, ³⁶⁷ and reasoned that because the Commission had adopted the *Corey* rationale in Ethics Opinion 172, ³⁶⁸ issued eight years earlier, precedent [*236] existed for concluding that mining of metadata did constitute conduct falling within those general proscriptions.

In *Corey*, an attorney had inadvertently been provided, along with other documents, a document clearly marked "confidential and legally privileged." ³⁶⁹ When the sending attorney requested that the documents be returned, the receiving attorney declined, arguing that he did not have an obligation to do so. ³⁷⁰ The trial court disagreed and ordered the documents returned. ³⁷¹ The Maine Supreme Judicial Court, sitting as the Law Court, upheld the lower court's ruling. ³⁷² Three months after *Corey* was decided, the Maine Ethics Commission, in Ethics Opinion 172, concluded that in light of the Law Court's holding in *Corey* "an obligation exists to protect against the consequences of the unwitting failure of opposing counsel to preserve the lawyer-client privilege," ³⁷³ there now existed "a solid basis for defining at least one aspect of conduct

³⁶⁴ N.Y. Op. 749, *supra* note 12, at 1 (emphasis added).

³⁶⁵ Me. Op. 196, *supra* note 12 (emphasis added).

³⁶⁶ *Id.*

³⁶⁷ [Corey, 1999 ME 196, 742 A.2d 933.](#)

³⁶⁸ Me. Prof. Ethics Comm'n, Op. No. 172 (March 7, 2000), available at <http://www.maine.gov/tools/whatsnew/index.php?topic=ebar> oversees ethics opinions&i d=89501&v=article (last visited Nov. 11, 2010) [hereinafter Me. Op. 172].

³⁶⁹ [Corey, 1999 ME 196, P 15, 742 A.2d at 940.](#) In fact, the document was marked in capital letters ("CONFIDENTIAL AND LEGALLY PRIVILEGED"), making it abundantly clear to the receiving attorney what type of information the document contained. *Id.* Transferring such a scenario to the metadata context, under these facts, even the strongest mining-permitted jurisdiction would hold that a receiving attorney who may initially have been ethically permitted to mine the metadata, once faced with such clearly confidential and privileged matter, has to stop and notify the sending attorney. The exception would be Maryland which does not follow the notification rule. See Md. Op. 2007-09, *supra* note 12, at 2.

³⁷⁰ [Corey, 1999 ME 196, P 15, 742 A.2d at 940.](#)

³⁷¹ *Id.*

³⁷² *Id.* P 22, 742 A.2d at 942.

³⁷³ Me. Op. 172, *supra* note 368.

that is prejudicial to the administration of justice." ³⁷⁴ Accordingly, the Commission withdrew Maine Ethics Opinion 146, ³⁷⁵ which held that it was not an ethical violation to "fail to return to opposing counsel an obviously privileged document inadvertently made available to him by opposing counsel." ³⁷⁶

Maine, like all mining-prohibited jurisdictions, prohibited the mining of metadata, finding that such conduct falls within the general proscriptions against dishonesty and conduct prejudicial to the administration envisioned in Model Rules 8.4(c) and (d), and (the then in existence) Maine Bar Rule 3.2(f)(3) and (4). Unlike other mining-prohibited jurisdictions, however, Maine acknowledged that the Commission was not free to "add ethical limitations not expressed by the Bar Rules" ³⁷⁷ no matter how "theoretically appealing" the conclusion. ³⁷⁸ This aversion **[*237]** to legislating on the part of the Maine Ethics Commission should, presumably and ideally, hold true for all jurisdictions' ethics commissions. Unlike other mining-prohibited jurisdictions, however, Maine, while acknowledging this limitation on the scope of its ethics commission's reach, also had a basis beyond the Commission's views—an opinion by the Law Court—to support a finding that the mining of metadata fell under the dishonest and prejudicial to the administration of justice category, thus making such conduct ethically impermissible. Maine, in 2008, while laboring under its Professional Responsibility Code, adhered to a literal reading of the rules, only expanding upon the literal language in the face of clear guidance from the State's highest court.

Although Maine adopted the Maine Rules of Professional Conduct approximately ten months after issuing Opinion 196, there is no reason to believe that the mining of metadata is now ethically permissible. This conclusion is supported by three factors. First, the finding that the mining of metadata was ethically impermissible under the old Code rules was based to a large extent on the Maine Ethics Commission's conclusion that Bar Rules 3.2(f)(3) and (f)(4) clearly prohibited such conduct. Because the language of the rules that replaced Bar Rules 3.3(f)(3) and (f)(4), i.e., Maine Rules of Professional Conduct Rules 8.4(c) and 8.4(d) are identical, there

³⁷⁴ Id.

³⁷⁵ Me. Prof. Ethics Comm'n, Op. No. 146 (December 9, 1994), available at <http://www.maine.gov/tools/whatsnew/index.php?topic=ebar> oversees ethics opinions&i d=89776&v=article (last visited Nov. 11, 2010) [hereinafter Me. Op. 146]. Interestingly, the Maine Commission in 1994 had disagreed with ABA Op. 92-328, see id., which had mandated the ABA's pre-Rule 4.4(b) refraining from viewing, notifying the sending attorney, and abiding by the sending attorney's instructions in instances of inadvertently received confidential material. See ABA Op. 92-368, supra note 99. The Maine Commission, in Me. Op. 146, referring to the Maine Code of Professional Responsibility, strongly emphasized that their charge as a Commission was not to "read into those Rules limitations on conduct that have not been stated expressly." See Me. Op. 146, supra.

³⁷⁶ Me. Op. 172, supra note 368.

³⁷⁷ Me. Op. 146, supra note 375. Me. Op. 146 was withdrawn by Me. Op. 172 in 2000. See Me. Op. 172, supra note 368. However, the Maine Professional Ethics Commission still adheres to the general belief expressed in Me. Op. 146, that in interpreting ethical rules, violations of which may lead to professional sanctions, the Maine Professional Ethics Commission "is not free to add ethical limitations not expressed by the Bar Rules." See Me. Op. 146, supra note 375. See also Me. Op. 172, supra note 368 ("the Commission has eschewed finding conduct to be a violation, which is merely implicit from the text of the Code . . ."); Me. Op. 196, supra note 12 ("The Commission is appropriately cautious in its specific application of the general proscription in Bar Rule 3.2(f)(3) and (4).").

³⁷⁸ Me. Op. 146, supra note 375.

is no reason to believe that mining would now fall outside of these general proscriptions on attorney conduct.

Second, the version of Rule 4.4(b), ³⁷⁹ adopted by the Maine Supreme Judicial Court in 2009, both lowers the standard for when a receiving lawyer knows a document was inadvertently disclosed to her, and specifically prohibits that lawyer from reading such a document. ³⁸⁰ Maine Rule 4.4(b), exemplifying a well-thought out approach to the problem of inadvertently disclosed material, mandates that a [*238] lawyer who receives a writing and "has reasonable cause to believe" the writing was inadvertently sent and may contain privileged material, may not read the material, must notify the sender, and must promptly "return, destroy or sequester" the material. ³⁸¹ The rule also prohibits the receiving attorney from using or disclosing the material until the matter has been resolved either informally or formally by a tribunal. ³⁸²

The various requirements imposed on the receiving attorney, however, only become applicable when she realizes the material may have been inadvertently disclosed and that it contains confidential material. In terms of this "knowledge" issue, the Model Rule, and the majority of states that have adopted a Model Rule-based version of Rule 4.4(b), and use the "knows or reasonably should know" ³⁸³ standard, with "knows" denoting actual knowledge and "reasonably should know" denoting "that a lawyer of reasonable prudence and competence would ascertain the matter in question." ³⁸⁴ Although the District of Columbia adopted the higher "actual knowledge" standard, thereby permitting the mining of metadata absent actual knowledge on the part of the receiving attorney of an inadvertent transmittal, ³⁸⁵ Maine took the opposite approach and adopted a lower knowing standard of "reasonable cause to believe." ³⁸⁶ Considering that Maine defines "reasonably" as the conduct of a "reasonably prudent and

³⁷⁹ Me. Rules of Prof'l Conduct R. 4.4(b) provides: A lawyer who receives a writing and has a reasonable cause to believe the writing may have been inadvertently disclosed and contain confidential information or be the subject of privilege or of protection as trial preparation material: (1) shall not read the writing or, if he or she has begun to do so, shall stop reading the writing; (2) shall notify the sender of the receipt of the writing; and (3) shall promptly return, destroy or sequester the specified information and any copies. The recipient may not use or disclose the information in the writing until the claim is resolved, formally or informally. The sending or receiving lawyer may promptly present the writing to a tribunal under seal for a determination of the claim. *Id.*

³⁸⁰ The Maine Task Force on Ethics charged with recommending the new rules, looked towards four different possible versions and approaches to inadvertently disclosed documents. Me. Rules of Prof'l Conduct R. 4.4, reporter's note. There four models were: (1) Model Rule; (2) the pre-existing rule in Maine; (3) a version of the rule adopted in New Jersey; and (4) a rule tracking the approach of the proposed ***Federal Rule of Civil Procedure 26(b)(5)(B)*** (Dec. 1, 2006). See *id.*

³⁸¹ Me. Rules of Prof'l Conduct R. 4.4(b).

³⁸² *Id.*

³⁸³ See Model Rules of Prof'l Conduct R. 4.4(b) ("A lawyer who receives a document relating to the representation of the lawyer's client and knows or reasonably should know that the document was inadvertently sent shall promptly notify the sender.").

³⁸⁴ Model Rules of Prof'l Conduct R. 1.0(f), (j).

³⁸⁵ See D.C. Op. 341, *supra* note 12.

³⁸⁶ Me. Rules of Prof'l Conduct R. 4.4(b). Interestingly, while the language of the Rule itself adopts the "reasonable cause to believe" standard, the comments to the Rule references the "knows or reasonably should know" standard. See *id.* at cmt. 2. In a conflict between the rules and the comments, however, the rule language must prevail.

competent lawyer," ³⁸⁷ and maintains that "[a] person's belief may be inferred from circumstances," ³⁸⁸ it would be difficult for a Maine attorney to argue that, absent an indication to the contrary from the sending attorney, any confidential or privileged material contained in the metadata was inadvertently disclosed. This is especially true in light of the comments to Rule 4.4(b) specifically noting that "[t]he fact a writing contains metadata does not necessarily mean the sending lawyer intended the metadata be disclosed, notwithstanding the fact the ostensible writing may have been disclosed intentionally." ³⁸⁹ Add to this that any "reasonably prudent and competent" Maine lawyer would know that the Maine Ethics Commission has held that under the higher "knows or reasonably should know" standard a lawyer who mines metadata was deemed to be engaging in conduct that is "dishonest or prejudicial to the administration of justice." ³⁹⁰

The final indication that the mining of metadata remains ethically prohibited in Maine, subsequent to the adoption of the Maine Rules of Professional Conduct, is **[*239]** simply that the Maine Ethics Commission has not seen fit to revise or withdraw Ethics Opinion 196. Given that that opinion was based to a large extent upon the interpretation of former Bar Rules 3.2(f)(3) and (f)(4), the language of which was fully adopted in Rules 8.4(c) and (d), and that the language of new Rule 4.4(b) supports the holding of Corey, which provided support for Opinion 196, (and arguably goes further) ³⁹¹ there is no reason for the Commission to do so. The act of mining metadata in Maine remains ethically impermissible.

Maine did not include a reference to attorney agreements as a way to preemptively seek to resolve any inadvertent disclosures of documents and material. ³⁹² Maine Rule 4.4(b) does, however, include in its prohibition on the recipient using or disclosing the inadvertently disclosed information, a reference to the claim being resolved both "formally or informally." ³⁹³ The Reporter's Notes explained in this regard that "[t]he inclusion of an informal means of resolving the issue of a claim of protection is an acknowledgment that in certain situations, it may not be feasible, financially or otherwise, to involve a tribunal." ³⁹⁴ If the Rule envisions the attorneys resolving issues arising from the disclosure of inadvertently disclosed material on their own subsequent to disclosure, then it seems certain they should also be able to do so prior to any disclosure through mutual agreements establishing how inadvertent disclosures should be resolved. Similarly, if the parties agree that both sides may review the metadata included in exchanged documents, such conduct would be neither dishonest nor prejudicial to the administration of justice, and would thus not be ethically prohibited.

³⁸⁷ Me. Rules of Prof'l Conduct R. 1.0(h).

³⁸⁸ Me. Rules of Prof'l Conduct R. 1.0(a).

³⁸⁹ Me. Rules of Prof'l Conduct R. 4.4, cmt. 4.

³⁹⁰ Me. Op. 196, *supra* note 12.

³⁹¹ While Corey and Me. Op. 172 mandated the return of inadvertently provided confidential material, Rule 4.4(b) includes a prohibition on reading such material, in addition to mandating the receiving attorney notify the sender, and the return, destruction, or sequestering of the material. See discussion *supra* pp. 74- 76.

³⁹² See N.Y. Rules of Prof'l Conduct R. 4.4 cmt. 2.

³⁹³ Me. Rules of Prof'l Conduct R. 4.4(b).

³⁹⁴ Me. Rules of Prof'l Conduct R. 4.4, reporter's notes.

K. New Hampshire: Mining Prohibited-Clear Wording of Rule

The New Hampshire Bar Association Ethics Committee (New Hampshire Ethics Committee) issued the first metadata ethics opinion of 2009.³⁹⁵ In an opinion entitled *Disclosure, Review and Use of Metadata in Electronic Materials*, the New Hampshire Ethics Committee squarely adopted the consensus with regard to the sending lawyer's duties and the original New York model with regard to the receiving lawyer's prohibition on the mining of metadata. What differentiated New Hampshire from all other jurisdictions that have issued ethics opinions on metadata was that New Hampshire's Rule 4.4(b) contains a specific prohibition upon an attorney who receives inadvertently received information from examining such materials.³⁹⁶ Due to the unique wording of that rule, it is not surprising that New [*240] Hampshire adopted both the mining-prohibited view that all metadata is to be considered inadvertently transmitted and, pursuant to a literal reading of its Rule 4.4.(b), found that reviewing or using metadata is prohibited in New Hampshire.

The New Hampshire Ethics Committee accepted, as a basis for its opinion, that lawyers "routinely" exchange electronic documents via e-mail and other means, that such electronic documents "inevitably" contain metadata,³⁹⁷ and that metadata, if mined, "may . . . reveal client confidences, litigation and negotiation strategy, legal theories, attorney work product and other legally privileged and confidential information that was never intended to be communicated by the sender."³⁹⁸ Having stated this, the Committee set out to provide guidance to New Hampshire lawyers as to their ethical obligations regarding the transmission and receipt of metadata under the New Hampshire Rules of Professional Conduct.

Noting that both the sending and the receiving lawyers "share ethical obligations to preserve confidential information,"³⁹⁹ the New Hampshire Ethics Committee followed the "general consensus" in terms of the sending lawyer's duties to "use reasonable care to guard against disclosure of metadata that might contain confidential information."⁴⁰⁰ The Committee looked to the duty of confidentiality under Rule 1.6,⁴⁰¹ describing the "[p]rotection of client confidences"

³⁹⁵ N.H. Op. 2008-2009/4, *supra* note 12.

³⁹⁶ New Hampshire Rule 4.4(b) provides: "A lawyer who receives materials relating to the representation of the lawyer's client and knows that the material was inadvertently sent shall promptly notify the sender and shall not examine the materials. The receiving lawyer shall abide by the sender's instructions or seek determination by a tribunal." N.H. Rules of Prof'l Conduct R. 4.4(b) (2008), available at <http://www.courts.state.nh.us/rules/pcon/index.htm> (last visited Nov. 11, 2010) (emphasis added).

³⁹⁷ N.H. Op. 2008-2009/4, *supra* note 12, at 1.

³⁹⁸ *Id.* at 2.

³⁹⁹ *Id.*

⁴⁰⁰ *Id.* at 3. N.H. Op. 2008-2009/4 cited to ABA Op. 06-442, Fla. Op. 06-02, and N.Y. Op. 782 as examples of the general consensus with regard to the sending lawyer's duties. *Id.*

⁴⁰¹ New Hampshire Rule 1.6(a) provides: "A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation, or the disclosure is permitted by paragraph (b)." N.H. Rules of Prof'l Conduct R. 1.6(a). While New Hampshire sub-section (b) to Rule 1.6 differs from the Model Rule, sub-section (a) is identical to the Model Rule language, with the exception of New Hampshire adding a comma to set off the final clause. Compare N.H. Rules of Prof'l Conduct R. 1.6(a)-(b), with Model Rules of Prof'l Conduct R. 1.6(a)-(b).

as "one of the most significant obligations imposed upon lawyers," ⁴⁰² the duty to provide competent representation pursuant to Rule 1.1, ⁴⁰³ as well as the general requirements under Rules 5.1 and 5.2 to ensure lawyers and non-lawyers within firms conform to these rules. ⁴⁰⁴ In terms of competent representation, the Committee noted that lawyers should stay abreast of technological advances and potential risks of transmission through appropriate training and education. ⁴⁰⁵ In addition, the Committee suggested that New Hampshire lawyers, in order to fulfill their duty of competent representation, at a minimum obtain a basic understanding [*241] of the existence of metadata in their electronic documents, the features of the software they use to produce such documents, and any "practical" means to "limit the likelihood of transmitting metadata or to purge the documents of sensitive information." ⁴⁰⁶ In this regard, the Committee noted that lawyers could avoid the creation of confidential material in documents when initially creating them, as well as by simply sending hard copy, scanned or faxed versions of the documents. ⁴⁰⁷ New Hampshire, relying upon rules that are the same or substantially similar to those in other states that have examined the issue and the Model Rules, joined the consensus among ethics commissions that an attorney transmitting an electronic document must "take reasonable care to avoid improper disclosure of confidential information contained in metadata." ⁴⁰⁸ What constitutes "reasonable care" will depend upon the facts and circumstances of each situation. Factors the Committee suggested a sending attorney should consider in this regard include: the subject matter of the document; the number of drafts and commenting parties; and whether the client has contributed comments to the document. ⁴⁰⁹

While the New Hampshire Ethics Committee also adopted the mining-prohibited jurisdictions' rationale in prohibiting the mining of metadata, New Hampshire Rule 4.4(b) differs in four

⁴⁰² N.H. Op. 2008-2009/4, *supra* note 12, at 2.

⁴⁰³ New Hampshire Rule 1.1(a) reads simply that "[a] lawyer shall provide competent representation to a client." N.H. Rules of Prof'l Conduct R. 1.1. See also *infra* text accompanying note 406.

⁴⁰⁴ New Hampshire's Rule 5.1 is identical to the Model Rule 5.1, with the exception of the substitution of "each" instead of "a" in sub-sections (a) and (b). Compare N.H. Rules of Prof'l Conduct R. 5.1, with Model Rules of Prof'l Conduct R. 5.1. The change was "intended to emphasize that the obligations created by the rule are shared by all of the managers of a law firm and cannot be delegated to one manager by the others." N.H. Rules of Prof'l Conduct R. 5.1, cmt. New Hampshire Rule 5.2 is identical to Model Rule 5.2. See N.H. Rules of Prof'l Conduct R. 5.2; Model Rules of Prof'l Conduct R. 5.2.

⁴⁰⁵ N.H. Op. 2008-2009/4, *supra* note 12, at 3.

⁴⁰⁶ *Id.* The fact that the Committee decided to provide specific suggestions pertaining to fulfilling the competent representation duty may be a reflection of New Hampshire having rejected the Model Rule's one sentence admonition of "knowledge, skill, thoroughness and preparation" as being "too general." N.H. Rules of Prof'l Conduct R. 1.1, cmt. New Hampshire's Rule 1.1(b), in contrast to the Model Rule, specifies: Legal competence requires at a minimum: (1) specific knowledge about the fields of law in which the lawyer practices; (2) performance of the techniques of practice with skill; (3) identification of areas beyond the lawyer's competence and bringing those areas to the client's attention; (4) proper preparation; and (5) attention to details and schedules necessary to assure that the matters undertaken is completed with no avoidable harm to the client's interest. N.H. Rules of Prof'l Conduct R. 1.1(b). At a very minimum, sub-section (2)- "performance of the techniques of practice with skill"-speaks directly to a lawyer's duty to become familiar with the potential trap-falls of electronic transmission of documents.

⁴⁰⁷ N.H. Op. 2008-2009/4, *supra* note 12, at 3.

⁴⁰⁸ *Id.* at 1.

⁴⁰⁹ *Id.* at 3.

respects from the Model Rule,⁴¹⁰ as well as from the equivalent rules of the other jurisdictions that have examined the metadata ethics issue. The first two differences are semantic, yet also significant: New Hampshire Rule 4.4(b) substitutes "materials" for the Model Rules "document" in order to "make clear that electronic information is covered"⁴¹¹ and replaces the "reasonably should know" standard of the Model Rule with the objective "knows" standard.⁴¹²

[*242]

The remaining two differences are substantive and speak directly to a receiving attorney's duties, and, as opposed to the Model Rules and most mining-permitted jurisdictions, provide an express ethical prohibition against the mining of metadata. The first substantive difference is that in addition to notifying the sending lawyer in instances of known inadvertently transmitted documents, New Hampshire Rule 4.4(b) also mandates that the receiving lawyer "shall not examine the materials."⁴¹³ In this regard, the New Hampshire Ethics Committee concluded that "all circumstances, with the exception of express waiver and mutual agreement on review of metadata, lead to a necessary conclusion that metadata is 'inadvertently sent' as that term is used in Rule 4.4(b)."⁴¹⁴ Because no lawyer would intentionally send confidential material, the receiving lawyer "necessarily 'knows'" such material was inadvertently transmitted.⁴¹⁵ As such, New Hampshire's unique Rule 4.4(b) "imposes an obligation on the receiving lawyer to refrain from reviewing the metadata."⁴¹⁶ The final difference between New Hampshire's Rule 4.4(b) and the Model Rules' 4.4(b) is that New Hampshire adds one final sentence, mandating that the receiving lawyer either abide by the sender's instructions or seek a determination from a tribunal.⁴¹⁷ In this respect, New Hampshire has in essence followed the old ABA approach of refraining from viewing, notifying, and abiding by the sending attorney's request.⁴¹⁸

While New Hampshire is the only jurisdiction out of those that have issued opinions pertaining to the view and or use of metadata that has an express ban on examining inadvertently sent

⁴¹⁰ Interestingly, the comments to New Hampshire Rule 4.4 note that paragraph (b) differs from the ABA Model Rule in only three respects: (1) the use of "materials" instead of "documents;" (2) the use of the objective "knowledge" standard instead of the "reasonably should know;" and (3) the addition of the final sentence. N.H. Rules of Prof'l Conduct R. 4.4, cmt. The comments left out the most important difference from the Model Rule language in terms of inadvertent disclosure of material; the addition of affirmative "shall not examine" prohibition." Compare N.H. Rules of Prof'l Conduct R. 4.4(b), with Model Rules of Prof'l Conduct R. 4.4(b).

⁴¹¹ N.H. Op. 2008-2009/4, *supra* note 12, at 4.

⁴¹² *Id.*

⁴¹³ *Id.* (quoting N.H. Rules of Prof'l Conduct R. 4.4(b)).

⁴¹⁴ *Id.* (quoting N.H. Rules of Prof'l Conduct R. 4.4(b)).

⁴¹⁵ *Id.*

⁴¹⁶ *Id.*

⁴¹⁷ N.H. Rules of Prof'l Conduct R. 4.4(b).

⁴¹⁸ As noted above, this was the approach taken by the ABA prior to the adoption of Model Rule 4.4(b) in 2002, and specifically rejected by the withdrawing of ABA Formal Opinion 92-368 (Nov. 10, 1992) by ABA Formal Opinion 05-437 (Oct. 1, 2005). The only difference between the former ABA approach and the New Hampshire approach is that New Hampshire also included the alternative option of the receiving attorney abiding by the sending attorney's instructions, or seeking a determination by a tribunal.

materials in the language of Rule 4.4(b), the New Hampshire Ethics Committee nevertheless saw the need to express its disagreement with "the view that the lack of an express prohibition in the Rules defines the extent of a receiving lawyer's obligations." ⁴¹⁹ In this regard, the Committee equated "purposefully seeking to unearth confidential information embedded in metadata attached to a document" ⁴²⁰ with a lawyer "peeking at opposing counsel's notes during a deposition or purposefully eavesdropping on a conversation between counsel and client." ⁴²¹ Either instance would implicate the broad principles underlying the Rules, "including the strong public policy in favor of maintaining client confidentiality," ⁴²² and would be contrary to the "general expectation of honesty, integrity, mutual courtesy and professionalism in the New Hampshire [*243] Bar." ⁴²³ As a result, it is abundantly clear to receiving attorneys in New Hampshire that they are specifically prohibited from reviewing inadvertently transmitted metadata by the clear, and unique, language of their State's Rule 4.4(b), and by the equally strong admonition in the language of New Hampshire Ethics Opinion 2008-2009/4.

While the New Hampshire Ethics Committee's language rejecting "the view that an express prohibition in the Rules defines the extent of a receiving lawyer's obligation" ⁴²⁴ was a not so subtle reference to ABA Formal Opinion 06- 442, ⁴²⁵ the Committee specifically and overtly rejected the ABA's suggestion that confidentiality agreements could serve as a means to minimize the resulting harm of inadvertently transmitted metadata. ⁴²⁶ The Committee was concerned that once confidential information has been divulged and learned, "especially if it involves the subject matter of the negotiations," there is "no way to effectively retract that information." ⁴²⁷ While this may be the case in such situations, the bilateral or unilateral agreements suggested by the Author are different in nature and design. Within New Hampshire, or amongst New Hampshire attorneys practicing outside of New Hampshire, absent any agreement of any sort, it is abundantly clear that viewing inadvertently transmitted metadata is prohibited. No unilateral notice to the contrary, i.e., a declaration by the receiving attorney that he will review the sender's e-mails for metadata, can abrogate this ethical ban. However, a mutually negotiated bilateral agreement between two New Hampshire attorneys that any metadata contained in an electronically transmitted document exchanged between them was not inadvertently sent removes such a document from the Rule 4.4(b) context and prohibition

⁴¹⁹ N.H. Op. 2008-2009/4, *supra* note 12, at 5.

⁴²⁰ *Id.*

⁴²¹ *Id.* at 6.

⁴²² *Id.* at 5.

⁴²³ *Id.* at 6.

⁴²⁴ *Id.* at 5.

⁴²⁵ See *supra* text accompanying note 99.

⁴²⁶ See N.H. Op. 2008-2009/4, *supra* note 12, at 6; ABA Op. 06-442, *supra* note 20.

⁴²⁷ N.H. Op. 2008-2009/4, *supra* note 12, at 6.

because the material would no longer be considered to have been inadvertently sent, and the receiving lawyer would thereby have clear knowledge of that fact.⁴²⁸

Additionally, a bilateral agreement, or a unilateral notification, could also play a role when a New Hampshire lawyer is engaged in a transactional intercourse with a lawyer from a mining-permitted jurisdiction. In this scenario, the lawyer from the mining-permitted jurisdiction would be ethically permitted to mine the documents sent by the New Hampshire lawyer, while the New Hampshire lawyer would be ethically prohibited from mining the documents received from the other lawyer. In order to equalize the playing field, the New Hampshire lawyer could ask the other lawyer to agree that neither side would mine each other's documents for metadata. If the opposing counsel refused to agree to such a non-mining agreement, the New Hampshire lawyer could then include a unilateral notice with the electronic transmission, putting the receiving lawyer in the otherwise mining- [*244] permitted jurisdiction on notice that he has taken all reasonable precautions to remove any and all confidential and privileged metadata from the document, but that any metadata that may remain is to be considered confidential and privileged and that the mining of the document for metadata is ethically prohibited as a result. The notice could also include a request that if any metadata is inadvertently discovered, the receiving attorney must cease reviewing the document and immediately notify the sending attorney. Even an attorney subject to the most liberal mining-permitted ethics opinion would, under such a scenario, be prohibited from mining that document for metadata. Thus, while the New Hampshire Ethics Committee may be correct that negotiated confidentiality agreements (outside of the formal discovery context) that address how to approach the possible disclosure of confidential information subsequent to discovery may be ineffective to the extent that the confidential or privileged information is then already disclosed, bilateral agreements between and amongst attorneys, or unilateral notices issued in jurisdictions with different or no ethical guidelines as to the mining of metadata at the outset of, and especially before, any exchange of electronic documents, are if not necessary, highly desirable.

L. West Virginia: Mining Ambiguously Prohibited-Actual Knowledge

West Virginia became the second state to issue an ethics opinion pertaining to metadata in 2009 when the West Virginia Lawyer Disciplinary Board (West Virginia Board) issued Legal Ethics Opinion 2009-01 in June of 2009.⁴²⁹ In a relatively short opinion (four pages) marked with qualifying language,⁴³⁰ the Board seemed to be adopting the District of Columbia's "actual knowledge" standard. However, while the District approached the issue from a positive view, holding that the mining of metadata is permitted absent any actual knowledge on the part of the

⁴²⁸ In fact, the New Hampshire Ethics Committee acknowledged precisely this, albeit stating the proposition in the negative, when, as noted above, it stated that "[t]he Committee believes that all circumstances, with the exception of express waiver and mutual agreement on review of metadata, lead to a necessary conclusion that metadata is 'inadvertently sent.'" N.H. Op. 2008-2009/4, *supra* note 12, at 5 (emphasis added).

⁴²⁹ W. Va. Op. 2009-01, *supra* note 12.

⁴³⁰ The opinion interestingly notes that it "could" be a violation to of Rule 8.4(c) if a lawyer reviews privileged material in metadata if he knows such material was inadvertently sent. *Id.* at 3. See also W. Va. Rules of Prof'l Conduct R. 8.4(c) (2009), available at <http://www.wvdc.org/ropc.htm> (last visited Nov. 11, 2010).

receiving attorney that the material had been inadvertently transmitted, West Virginia phrased the issue in a negative way, noting that if a lawyer has actual knowledge that the metadata was inadvertently transmitted, she may not review or use any accompanying metadata. Although the West Virginia opinion is somewhat ambiguous, the end result seems clear: a West Virginia lawyer may not review or use metadata if she has actual knowledge that it was inadvertently transmitted. Conversely, whether the West Virginia Board also intended the opposite to hold true, it seems clear that if a West Virginia attorney does not have actual knowledge, she is free to view and use the metadata. However, (and further clouding the clarity of the advice of the opinion) prior to doing so, a West Virginia attorney should consult with the sending attorney.

The West Virginia opinion, after defining metadata as "data behind the data," and noting that "metadata reveals information about electronic documents beyond the printable text,"⁴³¹ referenced ABA Opinion 06-442's conclusion that the Rules **[*245]** of Professional Conduct do not contain a specific prohibition against viewing or using metadata.⁴³² Other rules, however, such as Rule 1.1- Competence⁴³³ and Rule 1.6-Confidentiality of Information,⁴³⁴ create an obligation for an attorney to "take reasonable steps to maintain the confidentiality of documents in their possession."⁴³⁵ Reasonable steps include avoiding providing electronic documents with "accessible information that is either confidential or privileged," and "employ[ing] reasonable means to remove such metadata before sending the document."⁴³⁶ Considering this, West Virginia lawyers "must either acquire sufficient understanding of the software they use," or they must ensure that their office "employs safeguards to minimize the risk of inadvertent disclosures."⁴³⁷ The West Virginia Board affirmatively held that the sending attorney has a duty to "protect sensitive metadata," and that this duty could easily be fulfilled by sending hard copies, scanned PDF images, or simply faxing the document, or by using software that removes metadata.⁴³⁸

The West Virginia Board followed the consensus in terms of the duty of the sending lawyer. The Board's discussion pertaining to the duty of the receiving lawyer, a mere two sentences long, however, seemed to adopt the District of Columbia's "actual knowledge" approach. The first sentence espoused that "it could be" a violation of Rule 8.4(c) for a receiving lawyer to review

⁴³¹ W. Va. Op. 2009-01, supra note 12, at 1.

⁴³² Id. at 2.

⁴³³ West Virginia's Rule 1.1 provides: "A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation." W. Va. Rules of Prof'l Conduct R. 1.1.

⁴³⁴ West Virginia's Rule 1.6 is substantially different from the Model Rule 1.6 version with regard to the exceptions to the general duty to maintain confidentiality listed in sub-section (b) of the rule, however, the variations in the wording of sub-section (a) are semantic in nature and do not change the import of either rule. Compare W. Va. Rules of Prof'l Conduct R. 1.6, with Model Rules of Prof'l Conduct R. 1.6.

⁴³⁵ W. Va. Op. 2009-01, supra note 12, at 2.

⁴³⁶ Id.

⁴³⁷ Id.

⁴³⁸ Id. at 3 ("It is the duty of the lawyer sending electronic documents to protect sensitive metadata, and protecting metadata is easy.") (emphasis added).

privileged information inadvertently sent without first consulting with the sending lawyer.⁴³⁹ Accordingly, the second sentence concluded, if the receiving lawyer "has actual knowledge that metadata was inadvertently sent," the lawyer "should not" review the metadata before consulting with the sending lawyer "to determine whether the metadata includes work-product or confidences."⁴⁴⁰ While the West Virginia opinion did not reference or cite to the D.C. Op. 341, nor engage in a more thorough and logical discussion of that opinion, the end result of the lengthy discussion in D.C. Op. 341 and the substantially shorter treatment in W.Va. 2009-01 seemingly remain the same: a West Virginia lawyer with actual knowledge that metadata was inadvertently transmitted "should not" review such metadata without [*246] first consulting with the sending lawyer.⁴⁴¹ Because the prohibition of viewing metadata, as phrased by the Board, only extends to circumstances of "actual knowledge," West Virginia lawyers would presumably be allowed to review metadata absent such "actual knowledge." However, the final conclusion of the West Virginia opinion somewhat retracts the permission to review metadata absent "actual knowledge." The Board, in the conclusion of the opinion, affirmatively stated that "there is a burden on a lawyer receiving inadvertently provided metadata to consult with the sender and abide by the sender's instructions before reviewing such metadata."⁴⁴²

Whether the Board deliberately intended to leave out the "actual knowledge" litmus test is unclear. The end result is that West Virginia attorneys are left with a somewhat cryptic and confusing opinion. The language of the opinion clearly implies that absent "actual knowledge" of the inadvertence of the transmission of metadata, an attorney may review such material. However, the actual and final holding of the opinion admonishes West Virginia attorneys to not review inadvertently transmitted metadata without first consulting with the sending attorney.⁴⁴³ By not referencing the "actual knowledge" standard in the conclusion, the final outcome of the opinion seems to be that before a West Virginia attorney mines metadata, he needs to consult with the sending attorney. Considering that no attorney would, absent special circumstances, wish for opposing counsel to mine his metadata, the end result will effectively be that while West Virginia attorneys without actual knowledge of the inadvertence of transmission of metadata may ethically mine metadata, realistically, such mining will never take place: the sending attorney will likely advise the receiving attorney in such a "consultation" not to mine the metadata.

M. Vermont: Mining Permitted-ABA and Pennsylvania Resurrected

The final metadata ethics opinion to be issued in 2009 was issued by the Vermont Bar Association's Professional Responsibility Section (Vermont Section) in September of that year.

⁴³⁹ Id. West Virginia's Rule 8.4(c), providing that it is professional misconduct to "engage in conduct involving dishonesty, fraud, deceit or misrepresentation," is identical to the Model Rule's 8.4(c) and the District of Columbia's Rule 8.4(c). See W. Va. Rules of Prof'l Conduct R. 8.4(c); Model rules of Prof'l Conduct R. 8.4(c); D.C. Rules of Prof'l Conduct R. 8.4(c).

⁴⁴⁰ W. Va. Op. 2009-01, *supra* note 12, at 3 (emphasis added).

⁴⁴¹ Id. (citing N.Y. Op. 749, *supra* note 12).

⁴⁴² Id. at 4.

⁴⁴³ Id.

⁴⁴⁴ In arguably one of the most thorough and logical metadata ethics opinions to date, Vermont fully adopted both the ABA notion that absent a prohibition on mining in the rules, an ethics committee such as the Vermont Section, is not free to find that such a prohibition exists, and the Pennsylvania view that adopting such a prohibition would negatively impact the ability and duty of the receiving lawyer to diligently represent her client. Mining metadata is thus not ethically prohibited in Vermont. In terms of the sending attorney's duties, Vermont agreed with the consensus view that an attorney transmitting electronic documents must take reasonable precautions to protect confidential and privileged material.

The Vermont opinion was issued in response to a series of questions, broken [*247] down into the non-discovery⁴⁴⁵ and the discovery realm,⁴⁴⁶ posed by the Vermont Bar Association Board of Managers to the Professional Responsibility Section pertaining to metadata. These questions were combined by the Vermont Section into three standard metadata ethics inquiries: (1) what are the duties of an attorney sending electronic documents; (2) may a receiving attorney search⁴⁴⁷ documents for metadata; and (3) what steps should be taken by an attorney who becomes aware of inadvertently disclosed confidential information?⁴⁴⁸ Having posed the issue, the Vermont Section noted that "no provisions of the Vermont Rules of Professional Conduct (VRPC) speak directly to the questions presented."⁴⁴⁹ However, the potentially applicable provisions identified were: Rule 1.1-Competence;⁴⁵⁰ Rule 1.3- Diligence;⁴⁵¹ Rule

⁴⁴⁴ Vt. Op. 2009-1, supra note 7.

⁴⁴⁵ Id. at 1. The first batch of questions posed to the Professional Responsibility Section that pertained to metadata in the non-discovery context were: (a) Can the receiving lawyer use tools in the program that created the file to mine for metadata?; (b) Can the receiving lawyer use more specialized tools to mine for metadata?; (c) Can the receiving lawyer engage the 'track changes' function to review the history of edits made to the document[?]; (d) Is the receiving lawyer's responsibility different if the sending lawyer has inadvertently left the 'track changes' function engaged, so that the entire history of changes to the document are exposed without any action being taken by the receiving lawyer[?] Id.

⁴⁴⁶ Id. The second batch of questions asked by the Vermont Association Board of Managers pertained to the disclosure and searching of metadata during discovery in the litigation context: [W]hether (a) in the absence of a court order addressing discovery issues relating to metadata, lawyers or parties can mine for metadata in documents received from the opposing party during discovery; and (b) whether it is permissible for a party to remove metadata from documents before disclosing them during discovery. Id.

⁴⁴⁷ The Vermont Professional Responsibility Section, possibly foreshadowing their neutral and logical opinion, deliberately chose to use the term "search" instead of "mine." Id. The Section noted that "the term 'mine' appears to be a pejorative characterization of the use of electronic tools to analyze electronic documents." Id. Thus, the Section decided to use the phrase "search" instead of the phrase "mine," "because it characterizes the search embedded in a more neutral manner." Id. at 1 n.1.

⁴⁴⁸ Id. at 2.

⁴⁴⁹ Id. Vt. Op. 2009-1 was issued in September of 2000 and applied the Vermont Rules of Professional Conduct adopted by the Vermont Court Order 08, Vt. S. Ct., June 17, 2009, and effective September 1, 2009. See Vt. Rules of Prof'l Conduct (2 0 1 0), a v a i l a b l e a t <http://www.vermontjudiciary.org/LC/Statutes%20and%20Rules/PROMULGATED-JUN1709-VRPC.pdf> (last visited Nov. 11, 2010). In this regard, the Committee did note that Rule 4.4(b), which became effective September 1, 2009, did address the obligation of a lawyer who receives inadvertently disclosed documents. See Vt. Op. 2009-1, supra note 7, at 6.

⁴⁵⁰ Vermont Rule 1.1 provides: "A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation." Vt. Rules of Prof'l Conduct R. 1.1. Vermont Rule 1.1 is identical to the Model Rule 1.1. See id.; Model Rules of Prof'l Conduct R. 1.1.

1.6(a)-Confidentiality of Information;⁴⁵² Rule 3.4- **[*248]** Fairness to Opposing Party and Counsel;⁴⁵³ Rule 4.4-Respect for Rights of Third Persons;⁴⁵⁴ and Rule 8.4-Misconduct.⁴⁵⁵

Having listed the applicable rules, the Vermont Section answered the first of the general questions posited: "[D]oes a lawyer who sends electronic documents to opposing counsel have a duty to exercise reasonable care to avoid disclosing confidential metadata?"⁴⁵⁶ Here the Vermont Section joined the virtual unanimous **[*249]** view of all bar associations that have examined this issue, and concluded that "lawyers who send documents in electronic form to opposing counsel have a duty to exercise reasonable care to ensure that metadata containing

⁴⁵¹ Vermont Rule 1.3 provides: "A lawyer shall act with reasonable diligence and promptness in representing a client." Vt. Rules of Prof'l Conduct R. 1.3. Vermont Rule 1.3 is identical to the Model Rule 1.3. See id.; Model Rules of Prof'l Conduct R. 1.3.

⁴⁵² Vermont Rule 1.6(a) provides: "A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation, or the disclosure is required by paragraph (b) or permitted by paragraph (c)." Vt. Rules of Prof'l Conduct R. 1.6(a). Vermont Rule 1.6 is identical to the Model Rule 1.6. See id.; Model Rules of Prof'l Conduct R. 1.6. The exceptions to the duty of confidentiality listed in paragraphs (b) and (c) were not addressed by the Section per se, and are usually deemed not applicable in the context of metadata outside of the formal discovery arena. However, note that it can be argued that the language of Rule 1.6(b) requiring a lawyer to "reveal information relating to the representation of a client when required by other provisions of these rules or to the extent the lawyer believes necessary[]" is applicable in this context. See Vt. Rules of Prof'l Conduct R. 1.6(b). While Rule 1.6(b) is generally perceived to pertain to the prevention of criminal acts likely to cause death or substantial bodily harm (1.6(b)(1)), or the client committing a crime or fraud (1.6(b)(2)), reading the first clause of the disjunctive language of 1.6(b), i.e., authorizing disclosure "when required by other provisions of these rules," separately, it becomes clear Rule 1.6(b) dovetails with the disclosure of metadata in the formal discovery litigation context as per Rule 3.4. See generally Vt. Rules of Prof'l Conduct R. 1.6, 3.4.

⁴⁵³ The Vermont opinion reproduces several provisions of Rule 3.4 in the section dealing with potentially applicable Rules of Professional Conduct, and referencing the Rule in its discussion of the duty of the receiving lawyer. See Vt. Op. 2009-1, *supra* note 7, at 2, 5. The sections of Rule 3.4 reproduced are: A lawyer shall not: (a) unlawfully obstruct another party's access to evidence or unlawfully alter, destroy, or conceal a document or other material having potential evidentiary value. A lawyer shall not counsel or assist another person to do any such act; (b) falsify evidence, counsel or assist a witness to testify falsely, or offer an inducement to a witness that is prohibited under law; (c) knowingly disobey an obligation under the rules of a tribunal, except for an open refusal based on an assertion that no valid obligation exists; (d) in pretrial procedure, make a frivolous discovery request or fail to make reasonably diligent effort to comply with a legally proper discovery request by an opposing party; or (f) request a person other than a client to refrain from voluntarily giving relevant information to another party unless: (1) the person is a relative or an employee or other agent of a client; and (2) the lawyer reasonably believes that the person's interest will not be adversely affected by refraining from giving such information. See id. at 2; Vt. Rules of Prof'l Conduct R. 3.4.

⁴⁵⁴ The Vermont opinion reproduces both sections (a) and (b) of Rule 4.4; (b) is the section most pertinent in the metadata context. Vt. Op. 2009-1, *supra* note 7, at 2-3. Vermont Rule 4.4(b) provides: "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." Vt. Rules of Prof'l Conduct R. 4.4(b). Vermont Rule 4.4(b) is identical to the Model Rule 4.4(b). See id.; Model Rules of Prof'l Conduct R. 4.4(b).

⁴⁵⁵ The Vermont opinion reproduces sections (a) through (d) of Vermont Rule 8.4. Vt. Op. 2009-1, *supra* note 7, at 3. Those provisions provide: It is professional misconduct for a lawyer to: (a) violate or attempt to violate the Rules of Professional Conduct, knowingly assist or induce another to do so, or do so through the acts of another; (b) engage in 'serious crime,' defined as illegal conduct involving any felony or involving any lesser crime a necessary element of which is interference with the administration of justice, false swearing, intentional misrepresentation, fraud, deceit, bribery, extortion, misappropriation, theft, or an attempt or conspiracy or solicitation of another to commit a 'serious crime'; (c) engage in conduct involving dishonesty, fraud, deceit or misrepresentation; (d) engage in conduct that is prejudicial to the administration of justice . . . Vt. Rules of Prof'l Conduct R. 8.4(a)-(d).

⁴⁵⁶ Vt. Op. 2009-1, *supra* note 7, at 2.

confidential information protected by the attorney client privilege and the work product doctrine is not disclosed during the transmission process." ⁴⁵⁷ The Vermont Section noted that this duty was rooted in Rule 1.1, 1.3, and 1.6, and that various tools and methods are available to the sending lawyer to enable compliance with this duty. ⁴⁵⁸ These tools and methods include programs to "scrub" metadata from the electronic document before transmission, as well as simply sending PDF or paper documents. Closing its discussion on the duty of the sending attorney, the Vermont opinion again joined the general consensus that the specific steps a sending attorney should engage in depend upon the circumstances of the case. ⁴⁵⁹

In terms of the second question as to whether "a lawyer who receives electronic documents from opposing counsel [can] search those documents for metadata," ⁴⁶⁰ the Vermont Section noted the two diverging views: those jurisdictions that conclude that searching for metadata is dishonest, deceitful, and prejudicial to the administration of justice, and those that conclude that the Rules neither prohibit the searching of metadata nor support the characterization of such as being deceitful, dishonest or prejudicial to the administration of justice. ⁴⁶¹ Having explained the two points of view on the issue, the Vermont Section joined the searching-permitted jurisdictions, finding that nothing in the Vermont rules "compel[s] the conclusion that a lawyer who receives an electronic file from opposing counsel would be ethically prohibited from reviewing that file using any available tools to expose the file's content, including metadata," ⁴⁶² and that any rule prohibiting such a search would "represent a limit on the ability of a lawyer diligently and thoroughly to analyze material received from opposing counsel." ⁴⁶³

Not only are there no Vermont rules that "state or imply" that a receiving lawyer "must refrain from thoroughly reviewing the documents and information received from opposing counsel, regardless of the medium in which the document is transmitted," the rule where such an obligation would most likely appear, Rule 3.4, is "wholly silent on this issue." ⁴⁶⁴ Similarly, the Section noted that neither Rule 4.4 nor Rule 8.4 directly addressed this issue. ⁴⁶⁵ However, the silence and absence of guidance from these rules must be contrasted with the duty of competence and diligence from Rules 1.1 and 1.3, both of which provide "a clear basis for an inference that thorough review of documents received from opposing counsel, including a search for and review of metadata included in electronically **[*250]** transmitted documents," is

⁴⁵⁷ Id. at 3.

⁴⁵⁸ Id. at 4.

⁴⁵⁹ Id.

⁴⁶⁰ Id. at 2.

⁴⁶¹ Id. at 4. Tellingly, the Vermont Section notes that the jurisdictions that conclude that the searching of metadata is prohibited, do so partly "[t]hrough various chains of inference," (in addition to other jurisdictions' Rules of Professional Conduct that have been drafted differently from the Vermont Rules). Id. (emphasis added).

⁴⁶² Vt. Op. 2009-1, supra note 7, at 4-5 (emphasis added).

⁴⁶³ Id. at 5.

⁴⁶⁴ Id. (emphasis added in both instances).

⁴⁶⁵ Id.

required.⁴⁶⁶ Finally, having noted that the rules do not provide a basis for finding a prohibition on the part of a receiving lawyer to search electronically received metadata, and regardless of the fact that the existence of metadata is an "unavoidable aspect of rapidly changing technologies and information data processing tools," the Section affirmatively concluded that it is not within its scope to "insert an obligation into the [VRPC]" mandating such a prohibition.⁴⁶⁷

Whether a Vermont lawyer may search for metadata, however, does not answer the third question posed to the Vermont Section: What steps should a lawyer take upon learning that inadvertently disclosed privileged information has come into his possession?⁴⁶⁸ In this regard, Vermont Rule 4.4(b) is similar to the Model Rule in that it imposes an obligation on Vermont lawyers "to notify opposing counsel if they receive documents that they know or reasonably should know were inadvertently disclosed."⁴⁶⁹ The Section did not provide definite guidance on whether such inadvertent disclosure results in a waiver of the attorney-client privilege or the work-product-privilege, noting instead that this remains an issue of substantive law.⁴⁷⁰

Having addressed the issues of metadata in the non-discovery realm, the Vermont Section turned to the litigation context. The Section first noted that it was beyond the scope of the opinion to address the discovery rights and obligations of parties in litigation. However, the Section observed that the obligations of competence and diligence apply to all attorneys, including those in litigation.⁴⁷¹ As such, "basic rules of competence" require lawyers to be aware that "discoverable information may be included in electronic documents," and that "privileged and confidential information may be embedded in electronic files, including in hidden metadata."⁴⁷² Any standard practices and procedural rules permitting attorneys to withhold documents containing privileged material "apply with equal force to [*251] production of electronic documents."⁴⁷³ However, in terms of metadata specifically, the Section noted that it was not aware of any "authority or support for the proposition that a lawyer can redact,

⁴⁶⁶ Id. (emphasis added).

⁴⁶⁷ Id.

⁴⁶⁸ Vt. Op. 2009-1, supra note 7, at 6. Note that the way the Section phrased the question in the body of the opinion differs somewhat from the way the third question was phrased at the outset of the opinion: the question was initially phrased in terms of what a lawyer who "becomes aware that electronic documents received from opposing counsel contain metadata" should do. Id. at 2. In light of the opinion subsequently concluding that a Vermont lawyer may search such metadata, the obvious follow-up question is the one the Section discussed under the heading "Duty Imposed Upon Lawyer Who Learns of Receipt of Inadvertently Disclosed Privileged Information." Id. at 5 (emphasis added). In other words, it is not learning that metadata may exist that is the crux in the matter, (especially considering the Section's acknowledgment that "[t]he existence of metadata is an unavoidable aspect of rapidly changing technologies and information data processing tools"), but rather the scope of the duty of a receiving lawyer who finds privileged information within the metadata as a result of his search. Id.

⁴⁶⁹ Id. at 6. The opinion noted the history surrounding the adoption of Model Rule 4.4(b), and the subsequent withdrawal of ABA Formal Opinion 92-368. See supra note 99 and accompanying text.

⁴⁷⁰ VT. Op. 2009-1, supra note 7, at 6. The opinion did, however, note that while no Vermont cases had addressed the impact of inadvertent disclosure of privileged documents, numerous other courts had done so. Id. at 4-6. See also *Fed. R. Evid. 502(b)* (mandating that inadvertent disclosure does not waive the privilege if reasonable steps were taken by the holder of the privilege both to prevent and to respond to such disclosure).

⁴⁷¹ VT. Op. 2009-1, supra note 7, at 7.

⁴⁷² Id.

⁴⁷³ Id.

remove, or withhold metadata from electronic client documents . . . disclosed during discovery."⁴⁷⁴ Similarly, the Section was also unaware of "any restriction on the ability of the receiving lawyer or party fully to analyze electronic documents received during discovery, including use of any available tools to search for metadata embedded within those electronic files."⁴⁷⁵

In short, the last metadata ethics opinion issued in 2009 fully embraced the view that an attorney may mine (or in the more neutral words of the Vermont opinion "search") metadata included in documents received in both the non-discovery and the discovery context. However, unlike other mining-permitted jurisdictions, Vermont reached this conclusion by finding that such actions are ethically permitted based on the notion that the rules do not prohibit such actions and by way of a philosophical view that the proper role of a bar association ethics committee does not include promulgating ethical prohibitions where none are found in the State's ethics rules.

As with all jurisdictions that permit mining, Vermont attorneys would also presumably be able to, at the outset of any exchange of documents that may contain metadata, agree that they will not search such metadata. Thus, while the use of attorney agreements stipulating that the mining or searching of metadata is permissible would be superfluous in Vermont, attorney created agreements that provide neither side will search metadata would be acceptable in Vermont. In fact, as in all mining-permitted states, such agreements would fall in the same category as an attorney voluntarily choosing to return an inadvertently received document even though Vermont Rule 4.4(b) only requires notification.⁴⁷⁶ In other words, while an attorney may not act below the minimum ethical lines established by the rules, they can act above and beyond such rules and standards. A mutual agreement between Vermont attorneys to refrain from searching each other's metadata certainly would fall under this category.

N. Minnesota: Notify-No Further Guidance

Minnesota became the first state to issue a metadata ethics opinion in 2010 when the Minnesota Lawyers Professional Responsibility Board (Minnesota Board) issued an opinion entitled *A Lawyer's Ethical Obligations Regarding Metadata* in March of that year.⁴⁷⁷ In a succinct four page opinion, the Board reviewed and emphasized the duties of a sending attorney to act competently in avoiding improper disclosure of confidential and privileged information under Rules 1.1 and [*252] 1.6, and of a receiving lawyer to notify the sending attorney under Rule 4.4(b) in instances of inadvertently transmitted documents.⁴⁷⁸ In terms of the overall body of metadata ethics advice and directives existing through previously issued ethics opinions by other states, Minnesota did not break new ground. The opinion in essence

⁴⁷⁴ Id.

⁴⁷⁵ Id. (emphasis added).

⁴⁷⁶ Comment 3 to Vermont Rule 4.4, and the equivalent Model Rule comment, notes that in the context of a lawyer receiving an inadvertent document "[w]here 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." Vt. Rules of Prof'l Conduct R. 4.4, cmt. 3; Model Rules of Prof'l Conduct R. 4.4, cmt. 3.

⁴⁷⁷ Minn. Op 22, supra note 12.

⁴⁷⁸ Id. at 1.

amounted to a review of the duties associated with Rules 1.1, 1.6, and 4.4(b). If anything, the only unique aspect of Minn. Op. No. 22 was its overt declination to provide guidance as to whether the mining of metadata is ethically permissible in Minnesota, concluding instead that whether a lawyer in Minnesota may search metadata was beyond the scope of the opinion.⁴⁷⁹

The Minnesota Board, following the trend of prior metadata ethics opinions, defined metadata as "data within data," and described it as "information generated and embedded in electronically created documents."⁴⁸⁰ The opinion noted that most metadata is automatically generated, while some is "purposefully created."⁴⁸¹ Metadata can be scrubbed and it can be mined.⁴⁸² Setting up the context of the ethical question addressed in the opinion, the Board provided as examples the names of clients, comments about the strengths and weaknesses of a client's position, and price negotiation stances; all information that may be "embedded in the documents but not apparent in the document's - printed form."⁴⁸³ The Board noted that "a potential exists for the inadvertent disclosure of confidential or privileged information in the form of metadata in both a litigation and non-litigation setting" due in part to the "hidden . . . nature of metadata," and to the "ease with which electronic documents can be transmitted."⁴⁸⁴ It is this context "which in turn could give rise to violations of a lawyer's ethical duties."⁴⁸⁵

Having established the parameters of the issue and identified the potential ethical concern, the opinion looked to the competence requirement of Rule 1.1 that lawyers "provide competent representation."⁴⁸⁶ The Minnesota Board noted that this includes the "use of methods and procedures meeting the standards of competent practitioners."⁴⁸⁷ In terms of metadata, the Board explained this requires that lawyers who use electronic documents "understand that metadata is created in the generation of electronic documents," that the transmission of such documents will "include transmission of metadata," that "recipients of the documents can access metadata," and that "actions can be taken to prevent or minimize the [*253] transmission of metadata."⁴⁸⁸ Coupling this duty with a lawyer's duty of confidentiality pursuant

⁴⁷⁹ Id. at 4.

⁴⁸⁰ Id. at 1.

⁴⁸¹ Id.

⁴⁸² Id. at 1-2.

⁴⁸³ Minn. Op. 22, *supra* note 12, at 2.

⁴⁸⁴ Id.

⁴⁸⁵ Id.

⁴⁸⁶ Id. Rule 1.1 of the Minnesota Rules of Professional Conduct follows the Model Rules language, requiring that "[a] lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness, and preparation reasonably necessary for the representation." See Minn. Rules of Prof'l Conduct R. 1.1 (2010), available at <http://prb.mncourts.gov/rules/Documents/MN%20Rules%20of%20Professional%20Conduct.pdf> (last visited Nov. 11, 2010); Model Rules of Prof'l Conduct R. 1.1.

⁴⁸⁷ Minn. Op. 22, *supra* note 12, at 2 (quoting Minn. Rules of Prof'l Conduct R. 1.1, cmt. 5).

⁴⁸⁸ Id. at 3.

to Rule 1.6,⁴⁸⁹ and noting that this duty "regarding client information extends to and includes metadata in electronic documents,"⁴⁹⁰ the Board concluded that "a lawyer must take reasonable steps to prevent the disclosure of confidential metadata."⁴⁹¹ Moving to the duties of the receiving lawyer, the Minnesota Board succinctly emphasized the notification requirement pursuant to the language of Rule 4.4(b), and noted that the opinion "makes clear that the duty imposed by Rule 4.4(b) regarding documents extends to metadata in electronic documents."⁴⁹²

In terms of explaining the applicable duties of the sending lawyer in the context of inadvertently transmitted documents, and that those duties include and extend to metadata situations, the Minnesota Board fully adopted the general consensus. Similarly, in terms of the receiving lawyer in the same metadata context, the Board fully agreed with the ABA model. The only surprise when viewing the Minnesota opinion in the context of prior metadata ethics opinions is that the Minnesota Board specifically declined to provide any guidance in terms of whether a receiving attorney may ethically mine metadata. In fact, the Board specifically stated that "Opinion No. 22 is not meant to suggest there is an ethical obligation on a receiving lawyer to look or not to look for metadata in an electronic document," maintaining instead that "when a lawyer may be advised to look or not to look for such metadata is a fact specific question beyond the scope of [the] Opinion."⁴⁹³

Minnesota lawyers are thus somewhat left without specific guidance in terms of whether the mining of metadata is permitted. At a minimum, if a receiving attorney discovers confidential or privileged material in metadata, either through an innocuous manner such as by moving the cursor over a document, or as a result of a deliberate search for metadata, the opinion makes it clear that the notice requirement of Rule 4.4(b) comes into play. Similarly, the opinion also makes it abundantly clear that the competence and confidentiality duties of a sending attorney apply equally in the metadata context of electronic documents as with more traditional documents. However, beyond that, Minnesota attorneys, at least in comparison to attorneys in the twelve jurisdictions that have weighed in on this [*254] subject matter, are in essence left to their own accord in terms of whether the mining of metadata is ethically permissible. As such, Minnesota attorneys may benefit more from pre-exchange attorney-agreements specifying whether the parties will or will not mine each other's documents than other attorneys. In other

⁴⁸⁹ Rule 1.6 of the Minnesota Rules of Professional Conduct differs in format from the Model Rule language, but adheres to the general principle that a lawyer shall not knowingly "reveal information relating to the representation of a client." Compare Minn. Rules of Prof'l Conduct R. 1.6, with Model Rules of Prof'l Conduct R. 1.6. Both the Minnesota and the Model Rules comments specify that "[w]hen transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients." See Minn. Rules of Prof'l Conduct R. 1.6, cmt. 16; Model Rules of Prof'l Conduct R. 1.6, cmt. 17.

⁴⁹⁰ Minn. Op. 22, *supra* note 12, at 3.

⁴⁹¹ *Id.*

⁴⁹² *Id.* at 4. Minnesota Rule 4.4(b) is identical to the Model Rule 4.4(b), and reads in full 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." See Minn. Rules of Prof'l Conduct R. 4.4(b); Model Rules of Prof'l Conduct R. 4.4(b).

⁴⁹³ Minn. Op. 22, *supra* note 12, at 4.

words, Minnesota attorneys, through the use of attorney-agreements spelling out both whether mining should be permitted and what steps should be taken in the event confidential or privileged information is discovered, can remove the ethical ambiguity left by the non-guidance of Minn. Op. 22, ensuring that attorneys involved in an exchange of documents act in the same agreed upon manner.

III. The Practical Solution

A. Attorney Agreements

The metadata ethics opinions issued thus far have all focused on the duties of attorneys outside of the formal discovery realm. In other words, the opinions have focused on the scope of the ethical duties of a sending attorney and a receiving attorney as they exchange electronic documents in the normal course of their practice before a matter moves into the litigation stage. Documents will also, of course, be exchanged between attorneys and parties after the litigation process has begun. As the District of Columbia noted in its opinion: "When metadata is provided in discovery or pursuant to a subpoena, the rules of professional conduct are not the only rules of which lawyers must be aware."⁴⁹⁴ The District's opinion specifically mentioned the Federal Rules of Civil Procedure provisions addressing electronic discovery.⁴⁹⁵ While the Federal Rules of Civil Procedure do not govern the electronic exchange of documents outside of the formal discovery process,⁴⁹⁶ they do provide a familiar source to which the legal profession can look for guidance in terms of how to improve the handling of metadata contained in electronically exchanged documents in the non-discovery realm.

On December 1, 2006, amendments to the Federal Civil Rules of Procedure went into effect. Three of these rules, Rule 16(b)(3)(B)(iv)-Privilege Assertion Agreements in Pre-trial Scheduling Order, Rule 26(b)(5)(B)-Claiming Privilege or Protecting Trial-Preparation Materials after Information Produced, and Rule 26(f)- Party Pre-discovery Conference, together encourage, and in some instances mandate, that parties involved in a formal discovery process seek to preempt electronic discovery and privilege issues before they arise.⁴⁹⁷ Rule 26(f), for example, mandates that the parties discuss preserving discoverable information and then prepare a discovery plan that includes the parties' views and proposals **[*255]** regarding discovery and disclosure of electronic documents as well as claims of privilege or protection.⁴⁹⁸ The parameters of the parties' discussion in this regard will eventually be compiled into a discovery

⁴⁹⁴ D.C. Op. 341, *supra* note 12. Florida likewise noted this distinction and emphasized that Fla. Op. 06-2 did not "address metadata in the context of documents that are subject to discovery under applicable rules of court." [Fla. Op. 06-2, supra](#) note 12.

⁴⁹⁵ D.C. Op. 341 mentioned rules 16(b), 26(f), 33(d), 34(a) and 37(f). See D.C. Op. 341, *supra* note 12.

⁴⁹⁶ A party may, however, have a duty to preserve evidence through a so- called "litigation hold" when litigation is reasonably anticipated. See Lucia Cucu, Note, The Requirement for Metadata Production Under *Williams v. Sprint/United Management Co.*: An Unnecessary Burden for Litigants Engaged in Electronic Discovery, [93 Cornell L. Rev. 221, 230 \(2007\)](#).

⁴⁹⁷ [Fed. R. Civ. P. 16\(b\)\(3\)\(B\)\(iv\)](#), [26\(b\)\(5\)\(B\)](#), [26\(f\)](#).

⁴⁹⁸ [Fed. R. Civ. P. 26\(f\)](#), (f)(2), (f)(3)(C)-(D).

report,⁴⁹⁹ which in turn will be relied upon by the judge in formulating the court's Rule 16 scheduling order.⁵⁰⁰ Included in that scheduling order may be the parties' agreement as to privilege claims and protection of pre-trial preparation material after the information is produced.⁵⁰¹ Finally, recognizing that regardless of the parties' best intentions mistakes may occur, Rule 26(b)(5)(B) provides a means for the parties and the court to resolve instances where a claim of privilege is made subsequent to the production of material.⁵⁰²

The drafters of the Federal Rules of Civil Procedure, in other words, recognized that privilege issues are bound to arise when parties are engaged in discovery involving electronic documents. In light of this inevitability, the Rules seek to preemptively resolve these issues before they arise by encouraging the parties to address the subject matter at the outset. One of the ways to achieve such a resolution is for the parties to come to an agreement as to how to assert and protect privileged material.⁵⁰³ It is this notion of parties engaged in the formal discovery process preemptively entering into agreements pertaining to the handling and resolution of the potential disclosure of privileged material that can, and should, be adopted into the non-discovery electronic exchange realm. In other words, just as lawyers who are engaged in the exchange of electronic documents in a formal discovery setting seek to alleviate and regulate the possible disclosure of confidential or privileged material through preemptive bilateral agreements, so should lawyers concerned about similar disclosures in the non-discovery realm. The practicality of this proposal can be seen in that the issues are similar in the discovery and non-discovery realms, and in that an agreement addressing the handling of confidential or privileged material contained in voluntarily exchanged documents will be substantially similar, if not identical, in those same realms. Additionally, in most instances, the same attorneys will also handle the matter in the pre-formal discovery stage and the formal discovery stage. The only difference being that in the non-discovery realm the agreement will specifically address metadata, while in the discovery realm, although metadata may be discussed, it will not be the sole issue addressed.

[*256]

B. Bilateral Agreements and Unilateral Notices

1. Bilateral Agreements

Option A - Bilateral Agreement Permitting Mining

⁴⁹⁹ ***Fed. R. Civ. P. 26(f)(4)(B)***.

⁵⁰⁰ [Fed. R. Civ. P. 16\(b\)](#).

⁵⁰¹ [Fed. R. Civ. P. 16\(b\)\(3\)\(B\)\(iv\)](#).

⁵⁰² ***Fed. R. Civ. P. 26(b)(5)(B)***. The Committee Note to Rule 26 defines a "quick peek" arrangement as one where the responding party to a discovery request provides the requested material for an initial examination without waiving a privilege or protection. ***Fed. R. Civ. P. 26***, advisory committee's note. The requesting party then designates the documents he or she wants to be produced. *Id.* Once this designation has been made, the responding party then screens only the designated documents for privilege claims. *Id.* A claw back arrangement, on the other hand, envisions an agreement wherein the parties agree that production may begin without constituting a waiver of privilege, permitting the responding party to identify mistakenly produced documents and ensuring the return of such documents. *Id.* Significantly, the Committee Note concludes by observing that "[o]ther voluntary agreements may be appropriate depending upon the circumstances of a given litigation." *Id.*

⁵⁰³ [Fed. R. Civ. P. 16\(b\)\(3\)\(B\)\(iv\)](#).

Both parties to this agreement agree that either side may view and search any and all metadata included in electronically exchanged documents. Both parties have removed all confidential and attorney client privileged material in such metadata. [Additional sentences as to how to deal with inadvertently included and subsequently discovered confidential or privileged material should be added here.]

Option B - Bilateral Agreement Prohibiting Mining

Both parties to this agreement agree that neither side will view or search any non-visible parts, including metadata, of electronically exchanged documents. Both parties have sought to remove all confidential and client privileged material from any metadata that may exist in exchanged documents. Both parties agree that any confidential or privileged material which may remain, is inadvertently transmitted and not intended for opposing party. [Additional sentences as to how to deal with inadvertently included and subsequently discovered confidential or privileged material should be added here.]

All jurisdictions, regardless of their view as to whether the mining of metadata is permitted, presumably agree with the comments to Model Rule 1.6 that "[a] fundamental principle in the client-lawyer relationship is that, in the absence of the client's informed consent, the lawyer must not reveal information relating to the representation."⁵⁰⁴ As such, in most instances, the attorneys will be focused on not revealing confidential or privileged information inadvertently contained in metadata as opposed to sharing such information. Therefore, agreements pertaining to metadata will most often take the form of seeking to prohibit mining by the opposing party as opposed to permitting mining. In the jurisdictions where mining is permitted, this would constitute a voluntary opting out of an otherwise ethically permissible act. In jurisdictions where mining is not permitted, agreements of this kind would serve to buttress the ethical ban upon mining, and to specify means to resolve occurrences where confidential material is disclosed regardless of such a ban.⁵⁰⁵ In jurisdictions such as Pennsylvania where the decision whether or not to mine is left to the "sensitive and moral judgment"⁵⁰⁶ of the attorneys, an agreement would serve as the vehicle through which this judgment could be formalized.

There will, however, also be instances where mining of metadata is desired by both parties. In jurisdictions where mining is ethically permitted, an agreement **[*257]** between the parties that they may mine metadata in electronically exchanged documents will serve to formalize the intent of the parties. In jurisdictions where mining is banned, however, an agreement between parties formalizing the parties' intent and agreement to mine metadata would serve to remove the reasons underlying the jurisdiction's ethical ban on such conduct. All ethics opinions that conclude mining of metadata is unethical do so based upon the assumption that such conduct

⁵⁰⁴ Model Rules of Prof'l Conduct R. 1.6, cmt. 2.

⁵⁰⁵ As noted by Arizona, a jurisdiction that bans the mining of metadata as unethical, "some metadata embedded within an electronic document may be discovered by the recipient through inadvertent or relatively innocent means, such as right-clicking a mouse or by holding the cursor over certain text in the document." Ariz. Op. 07-03, *supra* note 12.

⁵⁰⁶ See Pa. Op. 2007-500, *supra* note 12, at 1 (quoting Pa. Rules of Prof'l conduct, pmbi., 9).

is surreptitious or contrary to the parties' understanding and intent.⁵⁰⁷ An agreement between parties affirmatively approving and envisioning the mining of metadata thus vitiates the basis for finding mining to be unethical.

Additionally, and possibly most significantly, an agreement entered into between attorneys in multi-jurisdictional cases will ensure that all parties act according to the same norms. It is in this situation where these agreements will be most beneficial. The agreements will enable attorneys to fully comply with their Rule 1.6 duty to preserve confidentiality and their Rule 1.3 duty to zealously represent their clients. For example, in a case where an attorney in Colorado is negotiating with an attorney in Arizona, both parties will know what rules will govern their conduct as they exchange electronic documents. The Arizona attorney, who is otherwise prohibited from mining metadata, will know whether the Colorado attorney will or will not mine. The Colorado attorney, who is otherwise permitted to mine electronic documents, will likewise know exactly what the Arizona attorney will do, as well as what he himself may or may not do. The attorneys will have resolved the multi-jurisdictional ethical dilemma otherwise inherent with the exchange of electronic documents by entering into a mutually agreed upon course of conduct.

Just as important, considering that the majority of lawyers in the nation are governed by one of the thirty-eight jurisdictions that have yet to pass judgment on whether mining metadata is ethically permissible, bilateral agreements would enable attorneys to arrive at a mutually agreeable standard of conduct regarding metadata. The alternative is for attorneys to guess as to whether mining may or may not be permitted in their jurisdiction; not an easy task considering the overwhelming lack of unanimity of the states that have actually addressed the issue. In light of the range of views on this topic, the overall desirability of attorney crafted agreements is plain.

Regardless in what jurisdiction the attorneys may be licensed, these bi or multilateral agreements would simply put forth whether the mining of metadata is permitted by either side, as well as how the parties will proceed in the event confidential or privileged material is discovered as a result of either conscious mining of metadata or inadvertent discovery of the same. The key is that both sides would be involved in fashioning the governing parameters of their conduct and that this occurs at the outset of any exchange of electronic documents. A violation of such an agreement would in and of itself constitute unethical behavior.

As is seen from the above review of ethics opinions, the five jurisdictions that fall into the clear mining-prohibited camp—Florida, Alabama, Arizona, Maine, and New Hampshire—all contain language in their respective opinions supporting the [*258] conclusion that parties can "opt out" of the prohibition on mining metadata. Thus, for example, Alabama's reliance on the surreptitious nature of the act of mining as a basis for concluding mining is impermissible disappears once both parties agree that mining is permitted. In such a circumstance, there is nothing surreptitious or deceitful involved in the act of mining the metadata. On the contrary, an instance where the parties enter into a bilateral agreement specifying that both parties are permitted to look beyond

⁵⁰⁷ The exception would arguably be New Hampshire in light of the direct prohibition included in the New Hampshire version of Rule 4.4(b). See N.H. Rules of Prof'l Conduct R. 4.4(b).

the "visible" document would be the exact scenario envisioned by the original New York opinion wherein the receiving attorney had received "a direction to the contrary," i.e., indicating that the sending lawyer indeed "intend[ed] the lawyer to receive the 'hidden' material or information."⁵⁰⁸ Similarly, a bilateral agreement wherein the parties affirmatively state that the mining of metadata is permitted would vitiate the "inadvertent" or "unintentional" transmission arguments that jurisdictions such as Florida rely upon to find mining to be unethical. In fact, Arizona, a jurisdiction that relied to an extent on the "inadvertently sent" language of its version of Rule 4.4(b) to support a ban on mining, did specifically note that "[a] lawyer who receives an electronic communication may attempt to discover the metadata that is embedded therein if he or she has the consent of the sender."⁵⁰⁹

The conclusion that mining would not be barred as unethical when both attorneys enter into bilateral agreements specifically permitting mining also holds true in the "actual knowledge" jurisdiction of the District of Columbia and in the "independent professional judgment" jurisdiction of Pennsylvania. In the District of Columbia, a bilateral agreement permitting mining would automatically vitiate any possible actual knowledge on the part of the receiving attorney that the metadata was inadvertently transmitted. In fact, the very opposite would be the case: there would be a clear affirmation that the metadata was intentionally transmitted. Similarly, Pennsylvania's reliance upon its attorneys' "judgment" and "common sense, reciprocity, and professional courtesy,"⁵¹⁰ is tailor-made for parties to craft bilateral agreements to coordinate and formalize exactly what professional courtesy will entail in a particular case. A subsequent violation of such an agreement would constitute misconduct in violation of Rule 8.4(c).⁵¹¹

The fact a bilateral agreement permitting mining vitiates a jurisdiction's reasons underlying its ethical ban in mining metadata does not, however, absolve a receiving attorney's ethical duties when he uncovers confidential or privileged material in the course of such an agreed upon and approved mining expedition any more than it absolves the sending attorney of his competence and confidentiality [*259] duties. As Colorado, a jurisdiction that permits a receiving lawyer to "search for and review any metadata included in an electronic document or file,"⁵¹² noted, once a lawyer discovers confidential material contained therein, the lawyer's Rule 4.4(b) duties engage. At a minimum, the receiving lawyer must abide by his jurisdiction's Rule 4.4(b) requirement, whether it is notification, as in Colorado, or notification and abiding by the sender's request, as in New Hampshire. While a bi or multilateral agreement overtly permitting mining between the attorneys would act to remove the "surreptitious" and "deceitful" practice of the act

⁵⁰⁸ N.Y. Op. 749, *supra* note 12, at 3. The opinion put the issue in the negative, stating that "[i]n the present inquiry, although counsel for the other party intends the lawyer to receive the 'visible' document, absent an explicit direction to the contrary counsel plainly does not intend the lawyer to receive the 'hidden' material or information about the authors of revisions to the document." *Id.* (emphasis added). An instance where the parties entered into a bilateral agreement to permit mining would fall squarely in this "absent an explicit direction" category.

⁵⁰⁹ Ariz. Op. 07-03, *supra* note 12 (emphasis added).

⁵¹⁰ Pa. Op. 2007-500, *supra* note 12, at 1-2.

⁵¹¹ Model Rule 8.4(c) holds that it is professional misconduct for a lawyer to "engage in conduct involving dishonesty, fraud, deceit or misrepresentation." Model Rules of Prof'l Conduct R. 8.4(c). Breaching an agreement entered into with opposing counsel constitutes such misconduct. See *id.* at cmt. 2.

⁵¹² Colo. Op. 119, *supra* note 12.

of mining itself, and thus the mining itself as being an ethically prohibited act, the same does not hold true for the ethical duties imposed upon an attorney who inadvertently discovers privileged material through the act of mutually agreed upon mining. An attorney must still follow the minimum requirements established by his jurisdiction in this regard. What these agreements would provide, however, is an opportunity for the parties, prior to the inadvertent disclosure of the privileged material, to agree upon and establish what actions, above and beyond the minimum established by the Rules, should be followed upon such disclosure. In other words, what the Federal Rules of Civil Procedure have acknowledged as the better practice in the litigation context would likewise be the better practice in the non- or pre-litigation context. Thus, any bilateral agreement that permitted the review of metadata should also include provisions specifying the exact procedure to follow once and if confidential material is discovered. Although the attorneys would be free to fashion their own remedies in this regard, they would likely choose to be guided by the quick peek and claw back provisions suggested by the Federal Rules of Civil Procedure.⁵¹³

2. Unilateral Notices

Metadata Search and Review Prohibited Notice:

Undersigned counsel has sought to remove any and all confidential and client privileged material from the metadata of the attached electronic document through all reasonable means available to him. The only portion counsel intends to transmit to opposing counsel is the visible portion of this document. The recipient of this electronic document is hereby informed, notified and provided actual knowledge that any confidential and privileged material that may remain in the metadata of the document is inadvertently transmitted. Counsel specifically notifies counsel that viewing and or searching such metadata is prohibited. [Additional sentences pertaining to resolution of confidential or privileged material that may nevertheless be inadvertently included and discovered should be resolved would be inserted here.]

In addition to bilateral agreements regulating attorney conduct with regard to the mining of metadata, one attorney could also seek to regulate an opposing attorney's ability to ethically mine metadata through the use of a unilateral notice. Under this scenario, one party, using a unilateral agreement, could prohibit the [*260] other side from mining metadata regardless of a particular jurisdiction's view on metadata mining. This is so because even jurisdictions that permit the mining of metadata by the receiving attorney generally prohibit such conduct if the receiving attorney has knowledge of the inadvertence of the transmission of the material. A unilateral notice by a sending attorney that he has sought to remove any and all privileged material from the metadata of an electronically transmitted document, and that any information contained in the metadata that remains was unintentionally included and is to be considered inadvertently transmitted, would make it unethical for the receiving attorney to mine such metadata, regardless if that attorney was located in a jurisdiction where the mining of metadata was otherwise ethically permitted. The opposite is, however, not true. In other words, an attorney located in a mining-prohibited jurisdiction can not opt out of his jurisdiction's ban on mining by unilaterally giving notice he will mine the metadata in electronically received documents.

⁵¹³ See *Fed. R. Civ. P. 26*, advisory committee's note to 2006 amendment.

Unlike the scenario where both sides agree to mine, or both sides agree not to mine, one party could thus prevent the other party from mining a received document using a unilateral notice emphasizing the inadvertence of any included metadata. This would hold true regardless of the jurisdiction in which a receiving attorney may be governed. Under this scenario, the sending attorney would include a notice with any electronically transmitted documents affirmatively stating that he has sought to remove all metadata, that any remaining metadata may contain confidential material, and that any such confidential material within the metadata was inadvertently transmitted. Unlike the standard e-mail privacy disclaimers used by attorneys presently that have no legal effect,⁵¹⁴ such a unilateral notice would have the clear effect of ethically prohibiting the receiving lawyer from mining a transmitted document for metadata. It would constitute a clear and unequivocal affirmation of the inadvertence of the transmission of such material, and a clear and unequivocal notice and actual knowledge on the part of the receiving lawyer of such inadvertence. Colorado, for example, specifically noted that if the receiving lawyer, "before examining metadata in an electronic document . . . receives notice from the sender that [c]onfidential [i]nformation was inadvertently included in the metadata," he or she may not examine the metadata and must abide by the sender's instructions.⁵¹⁵ Although the ABA opinion does not affirmatively state the same, it would be difficult to imagine reaching a different conclusion under the Model Rules, especially when the ABA has acknowledged that agreements may be employed as a means of reducing the risk of dissemination of confidential material through the transmission of metadata.

While there are several scenarios wherein unilateral notices could be used, only one would have the true intended effect: a unilateral notification by a sending attorney to a receiving attorney in a mining-permitted jurisdiction not to mine the metadata in electronic documents received from the sending attorney would preclude the receiving attorney from being able to ethically mine the document. **[*261]** Unilateral notices by a receiving attorney that he will mine documents received, would not serve to change what that attorney could already ethically do or not do as per his jurisdiction's view on metadata. A party located in a mining-permitted jurisdiction providing a notice to an opposing party that he will mine any received documents would merely be giving notice that he will be doing something that is already ethically permissible. This remains the same regardless if the sending attorney from whom he is receiving the documents is governed by a mining-permitted or mining-prohibited jurisdiction. As long as the receiving attorney is located in, or governed by, a mining-permitted jurisdiction, he may mine, regardless of whether he has given notice that he will do so or not. The opposite is, however, not true: a lawyer located in or governed by a mining-prohibited jurisdiction could not unilaterally remove himself from his jurisdiction's ban on mining. While his conduct is arguably no longer surreptitious in that it is known, the act of mining still remains, in the eyes of the mining-prohibited jurisdiction, deceitful and an attempt to obtain what he was not intended to have. A unilateral notice announcing an intent to mine would be superfluous and ineffectual. A unilateral notice to opposing counsel instructing the receiving attorney not to mine, however, would have the intended effect where such attorney was governed by a mining-permitted

⁵¹⁴ See, e.g., Joshua L. Colburn, Note, "Don't Read This if It's Not for You": The Legal Inadequacies of Modern Approaches to E-Mail Privacy, [91 Minn. L. Rev. 241 \(2006\)](#).

⁵¹⁵ Colo. Op. 119, *supra* note 12 (emphasis added). The certainty of the outcome in Colorado is, of course, in part due to Colorado Rule 4.4(c). See Colo. Rules of Prof'l Conduct R. 4.4(c).

jurisdiction. In such a scenario, regardless of where the notifying attorney may be located, an opposing party who otherwise could ethically mine electronic documents, upon receiving a notice from the sending attorney along the lines of the Metadata Search and Review Prohibited Notice suggested above, could not ethically mine the metadata. He would have actual knowledge of the inadvertent transmission of such material.

Finally, using such a unilateral notice (or for that matter a bi or multilateral agreement) seeking to prohibit opposing counsel from mining metadata would not in any way absolve the sending attorney of his competence and confidentiality duties. The sending attorney must still ensure he knows the parameters surrounding the creation, removal, and transmission of metadata. What a unilateral notice not to mine would achieve, however, would be both an ethical impediment upon an opposing attorney who otherwise could (if in a mining-permitted jurisdiction) or might (if in a jurisdiction that had yet to resolve the issue) mine the metadata, and serve as one additional step the sending attorney could take to ensure all reasonable actions have been taken to protect his client's confidences.

III. Conclusion

The exchange of electronic documents is ubiquitous and necessary in today's legal profession. An inevitable result of this transmission of information in electronic format is that non-visible metadata relating to the visible data may be included in such documents. How to regulate the potential review and use of this metadata is proving difficult for the legal profession. Fourteen ethics opinions have been issued to date in an attempt to guide lawyers on this issue. Tellingly, they do not reach a consensus as to whether the mining of metadata is permitted. This divergence of opinion is particularly troubling considering that a great deal of these electronic exchanges will take place between attorneys located in different jurisdictions. The situation will thus arise where one attorney's jurisdiction permits [*262] the mining of a second attorney's electronically transmitted document, while the jurisdiction of the second attorney bars her from mining documents received from the first attorney. Such a divergence of ethical guidance is undesirable. Based upon past ethics opinions, there is no reason to believe that a consensus on this issue will emerge through future ethics opinions. The solution may lie in attorneys using bilateral agreements to either permit or to ban the mining of metadata contained in documents exchanged between them. In instances where one side wishes to ensure that the other side cannot mine documents, a unilateral notice could also be employed. The adoption of these bilateral agreements or unilateral notices seems inevitable. Efficiency in the modern practice of law demands it; uniformity in the realm of legal ethics requires it.

Maine Law Review

Copyright (c) 2010 University of Maine School of Law

Maine Law Review