

I. Introduction

Most lawyers routinely create, edit, send and receive electronic documents in the course of everyday business. A recent debate has surfaced about what ethical duty, if any, lawyers have when sending or receiving documents that contain metadata. Metadata is “data about data.”¹ Specifically, metadata is “electronically stored information” within electronic documents that can provide “information about the creation or modification of the document.”² A lawyer that sends a document with metadata to an outside party could reveal confidential client information as well as litigation or negotiation strategy.³ Current ethics rules do not explicitly address the duty of lawyers who send or receive documents with metadata, but bar and lawyer associations have issued varied advisory opinions interpreting their current rules to guide lawyers in their jurisdiction. While all of the bar associations agree that there is a duty on the sending lawyer to prevent disclosure of confidential client information, they are generally divided into two camps concerning the ethical duty of the receiving lawyer to review metadata. One side finds that it is unethical for lawyers to seek out and review metadata in documents that are sent to them and the other side finds the activity to be ethically acceptable.

This paper contends it should not be unethical for a receiving lawyer to view metadata within an electronic document. Although this type of information has been given its own fancy word that may by itself intimidate those lawyers who are not comfortable with computers and technology, most metadata that lawyers may inspect in documents is viewed with a simple click of the mouse and not with special software. The use of electronic documents in the legal profession is ubiquitous and the metadata is just as much a part of those documents as the text produced by the sender. Placing the burden on the sender to remove confidential or other types of information the lawyer does not want the receiving lawyer to view creates a uniform and easily enforced rule that does not allow a sending lawyer to claim technological ignorance when performing his duties of protecting client information. Furthermore, bar associations that find it is ethical for lawyers to view metadata but require the receiving lawyer to notify the lawyer that sends the document when metadata is inadvertently sent, should remove all notification

¹ Marcia Coyle, *Where Do the Footprints of Metadata Lead?*, NAT'L L.J., Feb. 20, 2008, available at <http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1203430076731>.

² *Id.*

³ David Hricik & Chase Edward Scott, *Metadata: The Ghosts Haunting e-Documents*, 13 GA. B.J. 16 (2008).

requirements. Professional rules of conduct should move in the same direction as the law and, for ethical purposes, metadata should not be conceptually removable from the data on the face of the electronic document. If the electronic document as a whole was advertently sent, then the metadata should also be considered advertently sent.

II. Metadata Overview

Microsoft Office documents like Word, Excel and PowerPoint all contain metadata. Basic information about the life of a document is found by clicking on “Properties” located in the “File” menu.⁴ This screen provides information about the document such as the date and time it was created, the name of the hard drive where it is stored, the date it was last accessed and modified, the names of people who edited it and the number of revisions and the total editing time of the document.⁵ This type of information makes it easier for a law firm’s document management system to save, retrieve and organize documents.⁶ It also could reveal unintended information to opposing counsel. For example, a lawyer at Crowles & Thompson in Texas revealed an incident that happened at his firm where the opposing counsel stalled in producing documents.⁷ When they finally turned the documents over, they claimed they had just finished scanning them.⁸ The metadata in “Properties” revealed that the documents had been scanned a year earlier.⁹

Lawyers working on a document within a law firm may use the “Track Changes” or “Comment” feature in Microsoft Word to collaborate on a document.¹⁰ These features apply metadata to the document. Multiple attorneys may make revisions or add comments to the document that reveal confidential client information or the negotiation strategy of the firm.¹¹ A lawyer may forget to turn these features off before sending a document, or may not realize the document contained the information and send the document with the sensitive information embedded within the metadata. The same lawyer at Crowles & Thompson said the first thing he

⁴ *Id.* at 17.

⁵ Dan Pinnington, *Beware the Dangers of Metadata*, LAWPRO MAGAZINE, June 2004 at 36.

⁶ Susan J. Silvernail, *Metadata: What It Is & Why You Should Care* (Aug. 11, 2007) (unpublished article presented at the Alabama Association for Justice Seminar), *available at* <http://www.mrblaw.com/CM/TechnologyAndTheTrialLawyer/Technology-And-The-Trial-Lawyer-What-It-Is.asp>.

⁷ Coyle, *supra* note 1.

⁸ *Id.*

⁹ *Id.*

¹⁰ Hricik & Scott, *supra* note 3, at 18–19.

¹¹ *Id.*

does when receiving a Word or Excel file is “check and see if they had track changes turned on that maybe I can take advantage of.”¹²

There have been some newsworthy incidents where metadata embedded in documents has led to the release of information that the creator of the document did not intend. For example, in 2003 it was discovered that a research paper about Iraq published by the British government was plagiarized from a U.S. researcher.¹³ Since the British government published the article on their website in Microsoft Word format, the names of four people in the government who edited the article were discovered and they were called before Parliament for a hearing.¹⁴ Another incident happened in 2004 when SCO Group, seller of UNIX and Linux, sent a letter to 1,500 companies threatening to sue if they used their product without a license.¹⁵ SCO filed suit against Damien-Chrysler and metadata within a word version of their lawsuit paperwork revealed they had originally focused on suing Bank of America instead.¹⁶

III. Bar and Lawyer Associations Take a Stance

Prompted by an increased awareness and strategic use of metadata to extract information, bar associations have released advisory opinions about the ethical implications of sending and receiving documents that contain metadata outside of formal discovery. The advisory opinions focus on three questions. First, does the lawyer sending the document have a duty to prevent the disclosure of confidential information embedded in the metadata of a document? The general answer to this question is that sending lawyers do have a duty. Second, can the receiving attorney “mine”¹⁷ for metadata in documents? And third, does the receiving lawyer have a duty to inform the sending lawyer when he discovers confidential or inadvertently sent metadata within the document? The bar associations are divided into two general schools of thought concerning questions two and three. One side generally finds it is ethically acceptable to seek out and view metadata and the other side generally finds it is unethical.

¹² Coyle, *supra* note 1.

¹³ Catherine Sanders Reach, *Lemon Juice, Cornstarch, and Microsoft: Invisible Ink and Your Documents*, 27 NEWSLETTER STATE B. WIS. L. PRACTICE SEC. 7 (2004).

¹⁴ *Id.*

¹⁵ *Id.*

¹⁶ *Id.*

¹⁷ “Mining” refers to “the act of deliberately seeking out and viewing metadata embedded in a document.” J. Anthony McLain, *Opinions of the General Counsel: Ethical Propriety of Mining Metadata*, 68 ALA. LAW. 240 (2007). It is assumed in these three points that the sending lawyer has not made clear that he would like the receiving lawyer to look at “Track Changes” or “Comments” within the document. Obviously, if the lawyers are consciously using metadata as a tool and want each other to view the information there is no ethical issue.

A. Does the Sender Have a Duty?

As to the first question, all the bar associations, except for the American Bar Association, have taken the direct position that a lawyer who sends a document has a duty to prevent the disclosure of confidential information through metadata. While the American Bar Association did not specifically address the sending lawyer's duty with respect to metadata, they referenced Model Rule of Professional Conduct 1.6 which outlines a lawyer's duty to safeguard against inadvertent or unauthorized disclosure of client information.¹⁸ The New York State Bar Association found that based on the New York Lawyers Code of Professional Responsibility, a lawyer must use reasonable care to make sure he does not disclose confidential information when sending documents.¹⁹ "What constitutes reasonable care will vary under the circumstances" . . . and "may, in some circumstances, call for the lawyer to stay abreast of technological advances."²⁰ The New York County Lawyers Association echoed the New York State Bar Association stating that a lawyer "has the burden to take due care in appropriately scrubbing documents prior to sending them outside the office or in sending them in a way that ensures that the documents are free of metadata."²¹ The Arizona, Florida, District of Columbia, Colorado and Maryland bar associations also all stated that, under their rules of professional conduct, lawyers that send documents must take reasonable precautions to prevent the release of confidential information through metadata.²²

Since the risk of inadvertently sending metadata has become more well known and various jurisdictions have issued these advisory opinions saying the sender of a document must take reasonable care to prevent the release of confidential information through metadata, lawyers are taking precautions to protect themselves. When using the "Track Changes" or "Comment" feature, lawyers must make sure to delete all the embedded information before sending the

¹⁸ ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 06-442 (2006). In footnote four the ABA quoted Model Rule of Professional Conduct 1.6 which states, "[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." They then went on to say that "Addressing whether the sending or producing lawyer acted competently in any given factual scenario is beyond the scope of this opinion" *Id.*

¹⁹ N.Y. State Bar Association Comm. on Prof'l Ethics, Op. 782 (2004).

²⁰ *Id.*

²¹ N.Y. County Lawyers Association Comm. on Prof'l Ethics, Op. 738 (2008). "Scrubbing means removing metadata such as tracked changes and comments from a document." *Id.*

²² See Ariz. State Bar Comm. on the Rules of Prof'l Conduct, Op. 07-03 (2007); Fla. State Bar Ethics Department, Op. 06-2 (2006); D.C. Bar Legal Ethics Comm., Op. 341 (2007); Colo. Bar Association Ethics Comm., Op. 119 (2008); Md. State Bar Association Comm. on Ethics, Docket No. 2007-09.

document.²³ Microsoft has also released add-ins to help remove metadata from Office files.²⁴ Law firms are also using third party software such as Metadata Assistant by Payne Consulting Group to remove metadata from their documents.²⁵ One law firm in Newark, NJ educates all new employees, no matter what position, on the dangers of metadata. At that firm, all documents sent outside the firm automatically have the metadata removed by third party software.

B. Can the Receiving Lawyer Mine and View Metadata?

There are conflicting conclusions from bar associations about the second issue of whether a lawyer who receives a document can mine for metadata and review it. A group of bar associations generally finds this conduct ethically permissible. The American Bar Association interprets the Model Rules of Professional Conduct to allow lawyers to actively mine electronic documents for metadata and review the information as long as the electronic document was not obtained illegally or fraudulently.²⁶ They believe searching for metadata in a document does not fall “under the rubric of a lawyer’s honesty” as defined by the Model Rules of Professional Conduct.²⁷ The Maryland State Bar Association, influenced by the Model Rules of Professional Conduct and its own rules of conduct, also allows for the mining and reviewing of metadata.²⁸ The D.C. Bar took a slightly stricter approach under the D.C Rules of Professional Conduct finding that a receiving lawyer can review metadata except if he or she has “actual prior knowledge” that the metadata was inadvertently sent.²⁹ Actual knowledge may exist if the sending lawyer tells the receiving lawyer that metadata was inadvertently included or if the receiving lawyer immediately notices that the metadata has been unintentionally included.³⁰ The Colorado Bar’s analysis is similar to the D.C. Bar. They concluded that a receiving lawyer “generally may ethically search for and review metadata embedded in an electronic document,”

²³ Pinnington, *supra* note 5, at 37.

²⁴ *Id.*

²⁵ *Id.*

²⁶ ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 16-442 (2006).

²⁷ *Id.* The ABA opinion says that the closest applicable rule is 4.4(b) which 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 sender.” *Id.* The ABA says even if rule 4.4(b) was triggered, the rule is “silent as to the ethical propriety of a lawyer’s review or use of such information.” *Id.*

²⁸ Md. State Bar Association Comm. on Ethics, Docket No. 2007-09.

²⁹ D.C. Bar Legal Ethics Comm., Op. 341 (2007).

³⁰ *Id.*

but may not when he or she has prior notice from the sender that the metadata was inadvertently sent.³¹

The New York State Bar Association takes an opposite approach and is part of a group of bar associations that generally find it unethical to mine and review metadata. Focusing on the use of software, they found that under the New York Lawyers Code of Professional Responsibility lawyers may not make use of computer software to search for metadata within documents.³² The New York County Lawyers Association more broadly found that “a lawyer who seeks to discover inadvertent disclosures of attorney work product or client confidences or secrets or is likely to find privileged material violates” the New York code.³³ Rejecting the view of the American Bar Association, The New York County Lawyers Association viewed the issue from an ethical standpoint advising that mining for metadata is “deceitful and prejudicial to the administration of justice.”³⁴ The Arizona and Florida Bar Associations came to similar conclusions.³⁵ Even though none of these states’ codes of professional conduct explicitly discuss metadata, they interpreted their existing rules broadly to cover metadata issues. This interpretation is juxtaposed to the American Bar Association who interpreted the Model Rules of Professional conduct narrowly. Since all of these bar associations found it is unethical to mine for metadata, it is not surprising that they also found it unethical to view metadata if stumbled on by accident.

C. Does the Receiving Lawyer Have a Duty to Inform the Sending Lawyer?

The bar associations are also conflicted about the third question concerning the duty of a lawyer who receives a document with confidential or inadvertent metadata to inform the sending attorney of the mistake. The bar associations views fall into the same general groups as the second question, although some of the states that allow receiving lawyers to view metadata find that they must inform the sending attorney in certain circumstances. Although the American Bar Association allows lawyers to review metadata in all circumstances except fraud, they find that Model Rule of Professional Conduct 4.4(b) covers metadata within documents in addition to the

³¹ Colo. Bar Association Ethics Comm., Op. 119 (2008).

³² N.Y. State Bar Association Comm. on Prof’l Ethics, Op. 749 (2001).

³³ N.Y. County Lawyers Association Comm. on Prof’l Ethics, Op. 738 (2008).

³⁴ *Id.*

³⁵ See Ariz. State Bar Comm. on the Rules of Prof’l Conduct, Op. 07-03 (2007); Fla. State Bar Ethics Department, Op. 06-2 (2006).

documents themselves.³⁶ The rule states that a “lawyer who receives a document relating to the representation of the lawyer’s client and knows or should know that the document was inadvertently sent shall promptly notify the sender.”³⁷ The Maryland State Bar Association stated that receiving lawyers do not have to give notice to the sending attorney when they receive inadvertently sent or privileged metadata since the Maryland Rules of Professional Conduct did not adopt Model Rule of Professional Conduct 4.4(b) that the American Bar Association used to formulate its rule.³⁸ The D.C. bar said that, in addition to not allowing a receiving lawyer to view metadata when he has “actual knowledge” it was inadvertently sent, the receiving lawyer must also notify the sending lawyer.³⁹

Not surprisingly, the bar associations that ruled it is unethical to look for and review inadvertently sent or confidential metadata also found that the receiving lawyer has a duty to inform the sending lawyer. The New York County Lawyers Association, finding that it is not ethical to mine and review metadata, found that a lawyer who receives confidential or inadvertently sent metadata should inform the sending attorney.⁴⁰ The Arizona Bar Association said that a lawyer must notify the sender if the lawyer knows or reasonably should know that metadata contains confidential information or was inadvertently sent.⁴¹ The Florida Bar’s statement is similar to the Arizona bar, which stated, “if the recipient lawyer inadvertently obtains information from metadata that the recipient knows or should know was not intended for the recipient, the lawyer must promptly notify the sender.”⁴²

D. Pennsylvania’s Noncommittal Approach

The Pennsylvania Bar Association issued a formal opinion on metadata, but did not take a stance on the ethical implications of sending and receiving metadata.⁴³ The opinion summarizes other jurisdictions opinions and then concludes that under the Pennsylvania Rules of Professional Conduct, “each attorney must determine for himself or herself whether to utilize metadata contained in documents and other electronic files based upon the lawyer’s judgment

³⁶ ABA Comm. on Ethics and Prof’l Responsibility, Formal Op. 16-442 (2006).

³⁷ *Id.*

³⁸ Md. State Bar Association Comm. on Ethics, Docket No. 2007-09.

³⁹ D.C. Bar Legal Ethics Comm., Op. 341 (2007).

⁴⁰ N.Y. County Lawyers Association Comm. on Prof’l Ethics, Op. 738 (2008).

⁴¹ Ariz. State Bar Comm. on the Rules of Prof’l Conduct, Op. 07-03 (2007).

⁴² Fla. State Bar Ethics Department, Op. 06-2 (2006).

⁴³ Pa. Bar Association Comm. on Legal Ethics and Prof’l Responsibility, Formal Op. 2007-500 (2008).

and the particular factual situation.”⁴⁴ Although they conceded that the ultimate rules will be decided by judicial determination, the only concrete advice the opinion provides is that inadvertent transmissions of metadata should not constitute a waiver of attorney-client privilege, “except in the case of extreme carelessness or indifference.”⁴⁵

IV. Analysis

A. Criticism of the ABA’s Position

Just as the bar associations are split on the ethical implications of mining for metadata, legal commentators are divided on which school of thought is correct and best suited for the realities of legal practice. Some commentators, such as professor David Hricik, disagree with the American Bar Association’s view and embrace the position that viewing inadvertent or confidential metadata is unethical under the Model Rules of Professional Conduct.⁴⁶ Hricik argues that Model Rule of Professional Conduct 8.4(c) should apply to a lawyer who views metadata embedded in a received document.⁴⁷ The rule states that it is “professional misconduct” for the lawyer to “engage in conduct involving dishonesty, fraud, deceit or misrepresentation.”⁴⁸ Hricik goes on to say:

The notion that a lawyer should be permitted to look for inadvertently transmitted embedded data and, thereby, intentionally take advantage of the accidental failure of a colleague to understand the inner workings of software is startling. The characterization of the intentional act of taking advantage of those mistakes as anything less than dishonest is disappointing.⁴⁹

B. Addressing the Critics

As seen from the title of his article, *Mining for Embedded Data: Is it Ethical to Take Intentional Advantage of Other People’s Failures?*, the underlying premise to Hricik’s argument is that it is unethical for a lawyer to use a mistake of their opposing counsel to the advantage of their own client. If one starts with this premise, then they will surely reach the conclusion that mining for metadata is unethical. This starting premise is erroneous within the adversarial

⁴⁴ *Id.* The opinion goes on to say that the lawyer’s determination “should be based upon the nature of the information received, how and from whom the information was received, attorney-client privilege and work product rules, and common sense, reciprocity and professional courtesy.” *Id.*

⁴⁵ *Id.*

⁴⁶ See generally David Hricik, *Mining for Embedded Data: Is it Ethical to Take Intentional Advantage of Other People’s Failures?*, 8 N.C. J.L. & TECH. 231 (2007).

⁴⁷ *Id.* at 242.

⁴⁸ *Id.*

⁴⁹ *Id.* at 247.

context of the United States legal system. Consider the following situations: Is it unethical for a lawyer to point out a flaw in an opposing counsel's argument or to advise a client to enforce a provision in a contract because the opposing party's lawyer failed to object to the provision? In both of these cases the answer is that it is not unethical. Just because a receiving lawyer intentionally takes advantage of the sending lawyer's failure to remove metadata, that does not necessarily mean his actions are unethical.

Hricik also argues that the American Bar Association was incorrect in solely applying Model Rule of Professional Conduct 4.4(b) to the situation of viewing metadata. This position is unconvincing based on the reasoning behind the amendment to rule 4.4(b). The sole requirement of 4.4(b) that the receiving lawyer notify the sender when the lawyer knows or reasonably should know that a document was inadvertently sent was a direct response to the ABA Standing Committee on Ethics and Professional Responsibility Formal Opinion 92-368 which states that the receiving lawyer is obligated to refrain from examining inadvertently sent materials.⁵⁰ As the official reporter's explanation of the changes specify, rule 4.4(b) was changed because the 1992 opinion was criticized. Hricik implies that the American Bar Association's decision to rely solely on rule 4.4(b) was arbitrary, but the American Bar Association did so because the rule was changed specifically so the receiving lawyer of inadvertently sent information did not have an ethical obligation to refrain from viewing inadvertently sent material.

Hricik also attempts to distinguish the text of Model Rule of Professional Conduct 4.4(b) from the act of mining for metadata. He contends that while the rule addresses what the receiving lawyer should do when he finds inadvertently sent information, it fails to address whether it is unethical for a lawyer to search for the information in the first place. This argument stems from Hricik's characterization of metadata as "hidden" and his description of mining for metadata as "look[ing] behind" a document.⁵¹ Most of the important metadata in a Microsoft Word document can be found by clicking on "File" and then "Properties." This action only takes two clicks of the mouse, which is the same effort it takes to simply open a Word document. Such information can hardly be considered hidden. Similarly, in a Microsoft Excel document, one can view the formula of how the sender reached a certain number simply by double clicking

⁵⁰ ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 92-368 (1992).

⁵¹ Hricik, *supra*, note 47 at 233-234.

on the number. Critics of Hricik would argue that metadata is not “hidden,” but is part of the document and therefore looking for it would not be deceitful or dishonest.

While knowledge of metadata may not be completely widespread among lawyers, it is safe to assume that it will only increase in the future. Even though there is no current study revealing how many lawyers are aware of metadata, Hricik uses the fact that not all lawyers are aware of the dangers of inadvertently sending metadata as a reason for barring lawyers from searching for and viewing metadata.⁵² Regardless of the current percentage of lawyers who are aware of metadata, it does not make sense to bar something based on lack of knowledge when it is safe to assume that the knowledge will increase. Rules should be made looking forward, not backward, and technological ignorance should not be an excuse for lawyers to reveal confidential information through metadata. Likewise, technological ignorance of the sender is not a reason to make it unethical for the receiving lawyer to view metadata.

C. Support for the ABA’s Position

As compared to Professor Hricik’s paper criticizing the American Bar Association’s position, there are no published papers of equal depth defending the American Bar Association’s position that mining for metadata is not unethical and that it should be allowed. There are lawyers who believe the American Bar Association’s view is correct. One Florida attorney said, “mining for metadata was an invaluable tool for fretting out fraud and unethical individuals.”⁵³ Through metadata, this attorney was able to detect that an individual claiming he used a part manufactured by his client’s company was actually using a false certificate.⁵⁴ Some lawyers also feel that they are not adequately representing their client if they do not look for metadata.⁵⁵ In some circles of lawyers, “a policy of banning metadata mining is thought of as ridiculous.”⁵⁶

A. Metadata Compared to Previous Technological Advancements

The American Bar Association’s opinion that searching for and reviewing metadata within received documents is completely ethical is the correct view. When new technology comes to light in the legal community, there will always be lawyers who are uninformed and also those who are against implementing the technology into the practice of law simply because it is

⁵² See *id.* at 246–247. The latest study performed in 2004 said that 43% of respondents were aware metadata existed. *Id.*

⁵³ Jessica M. Walker, *What’s a Little Metadata Mining Between Colleagues?*, DAILY BUSINESS REVIEW (Apr. 23, 2006).

⁵⁴ *Id.*

⁵⁵ *Id.*

⁵⁶ *Id.*

new. The advent of computers and the widespread use of electronic documents have dramatically changed the way lawyers send and receive information and there will surely be new technology in the future that further alters the dynamic. Searching for metadata within a document is similar to past technological advances such as viewing the “band” of information on a received fax, looking for the IP address of the computer that sent you an email or taking fingerprints off of a letter or document.⁵⁷ In the example of the letter, the intention of the sender was to send the information within the letter, not the information pertaining to who had touched the letter. Yet, searching for fingerprints on a letter is completely ethical and would never be barred by the Model Rules of Professional Conduct. At a certain point in time when fingerprinting technology was introduced, it is logical to believe that many attorneys were not aware of the technology. Just because new technology is invented that changes the way lawyers communicate and there are lawyers that aren’t aware of some of the information that is conveyed in that type of communication, it should not be deemed unethical for the receiving lawyer to search for and view that information under the rubric of zealous advocacy. “Our tools for dealing with information have made a great leap forward, but that does not mean that we should refrain from being responsible for the information we create.”⁵⁸

B. Federal Courts and The Federal Rules of Civil Procedure Accept Metadata

Recent court opinions and amendments to the Federal Rules of Civil Procedure show that the law is accepting metadata as part of a document and not a separate piece that should be viewed and thought of as disconnected. Taken together, these developments demonstrate that awareness of metadata in general is growing and also that the law deems it a useful tool for lawyers to convey information and not an unethical and deceitful intrusion. In 2005, the United States District Court in Kansas decided *Williams v. Sprint/United Mgmt. Co.*⁵⁹ The plaintiffs in the case claimed their employer discriminated against them on the basis of age in terminating their employment.⁶⁰ The issue before the court was whether the employer had to produce Excel spreadsheets that contained information about the lay-offs in a native format with the metadata

⁵⁷ Michael Katz, *Beneath the Surface: Metadata, Transparency and the Ethical Use of Information* (Mar. 6, 2008).

⁵⁸ *Id.*

⁵⁹ *Williams v. Sprint/United Mgmt. Co.*, 230 F.R.D. 640 (D. Kan. 2005).

⁶⁰ *Id.* at 641.

still intact.⁶¹ The court ruled that that the defendant employer had to turn over the Excel spreadsheets with the metadata intact.⁶² The court stated that:

[W]hen a party is ordered to produce electronic documents as they are maintained in the ordinary course of business, the producing party should produce the electronic documents with their metadata intact, unless that party timely objects to production of metadata, the parties agree that the metadata should not be produced, or the producing party requests a protective order.⁶³

In 2006, the Federal Rules of Civil Procedure (“FRCP”) were amended to clarify rules concerning electronic discovery. A comprehensive change to the FRCP was the addition of the term “electronically stored information” to the rules so courts no longer have to construe electronic information as falling under the rubric of “documents” or “things.”⁶⁴ The purpose of the rule amendments was to acknowledge the rising use and importance of “electronically stored information” for discovery and lay out guidelines on how lawyers should perform discovery with electronic information. In terms of metadata, the amendment to rule 34(a) legitimizes metadata as subject to discovery because it is part of the document.⁶⁵ Rule 35(b) lays out the procedure for the lawyers on both sides to negotiate the form in which the electronic documents will be produced.⁶⁶ The lawyer may request that the opposing party produce the electronic documents in native format with the metadata attached. If the lawyers cannot reach a deal, then the court will decide how the electronic documents will be produced.⁶⁷

C. Practical Reasons for Allowing Lawyers to view Metadata

The *Williams* case and the FRCP amendments are representative of the current trend in the law to treat metadata as part of the electronic document which, if it contains information relevant to the case, should be used by a court of law to achieve equity. Since the law is moving towards allowing metadata of electronic documents to be discoverable, this will conflict with state bar associations that have made it unethical to review metadata. It is unclear in those

⁶¹ *Id.*

⁶² *Id.* at 652.

⁶³ *Id.*

⁶⁴ Lee H. Rosenthal, *A Few Thoughts on Electronic Discovery After December 1, 2006*, 116 YALE L.J. POCKET PART 167 (2006), <http://thepocketpart.org/2006/11/30/rosenthal.html>.

⁶⁵ See FED.R.CIV.P. 34; Rosenthal, *supra* note 64. Rule 34(a)(1)(A) states that “any designated documents or electronically stored information — including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations — stored in any medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form” are discoverable. FED.R.CIV.P. 34(a)(1)(A).

⁶⁶ See FED.R.CIV.P. 35.

⁶⁷ *Id.*

jurisdictions how a court in discovery will rule if it finds that the receiving attorney ethically violated his duty not to look at metadata, but also finds that the metadata is relevant to the case. In a non-discovery context, making it unethical to view metadata raises practical enforcement implications. If the receiving attorney is not attempting to bring information from metadata into discovery, there is no way to know whether he reviewed the metadata. If a lawyer inadvertently sends a document that contains metadata within the “Comment” feature that reveals litigation strategy, the receiving lawyer will simply use that information and there will be no way to tell that it was viewed. It is not possible to punish the viewing of this type of inadvertently sent metadata.

In addition to the law clearly accepting metadata as part of the actual electronic document, placing the ethical burden on the sender of a document to prevent the release of confidential information is a more streamlined and sensible approach to dealing with the problem of inadvertently sent metadata. One problem with the bar associations that have deemed it unethical to search for and review metadata is that many of them do not ban it outright, but add layers to their rules that look at the mental state of the receiving attorney. For instance, the D.C. Bar states that a receiving lawyer can review metadata except if he or she has “actual prior knowledge” that the metadata was inadvertently sent.⁶⁸ Actual knowledge may exist if the sending lawyer tells the receiving lawyer that metadata was inadvertently included or if the receiving lawyer immediately notices that the metadata has been unintentionally included.⁶⁹ This rule raises questions such as how soon must a receiving attorney notice inadvertent metadata for it to be immediately noticed. These types of rules will unnecessarily burden the court system with time-consuming inquiries. If all the bar associations place the burden on the sender, then all jurisdictions will have a unified standard which will bring continuity and certainty to exchanges of electronic information between lawyers.

D. Law Firms Current Practices

Within large and medium size law firms, the problem of lawyers inadvertently revealing information through metadata has become a non-issue because of automated software that automatically removes metadata from any documents before an e-mail containing a document is

⁶⁸ D.C. Bar Legal Ethics Comm., Op. 341 (2007).

⁶⁹ *Id.*

sent.⁷⁰ Many large and medium size law firms have been utilizing automated software that automatically removes metadata since 2004. In fact, the current issue for those in charge of technology procedures at law firms is to provide the user more personal customization so certain types of metadata are not automatically removed when the user wants that information to be sent.⁷¹ Since many firms have these automatic systems in place, the situation of an unknowing attorney mistakenly revealing client confidences or strategic thought through metadata is greatly reduced. At many large and medium size firms it will simply never happen and in this situation is it obviously not burdensome to place the burden on the document sender to remove unintended information.

Admittedly, many solo practitioners and small law firms do not have this type of automated software. It may be that they are unaware of metadata completely, aware of metadata but not aware of removal software, or aware of metadata and the removal software but have chosen not to purchase it. Lack of software does make it somewhat more burdensome on the sender to remove metadata since it would have to be done manually, although Microsoft does offer support for this procedure on their website.⁷² Also, solo practitioners and small firms tend to have external IT help that provide basic computer and network support, but do not provide legal specific IT related advice. One solo practitioner I spoke to knew about metadata and manually removed it when he thought necessary.⁷³ Another solo practitioner I spoke to was not aware metadata.⁷⁴ While solo practitioners and small law firms do not have the resources that larger law firms have in terms of money to pay for software or legal specific IT professionals within their office, that does not mean that states should base their professional rules of conduct on such inequity. First, there are many compelling reasons stated within this paper as to why it should not be unethical for lawyers to view metadata in documents they receive and why it is logical to place the burden on the sender to prevent the release of untainted information that apply to both small and large firms. Second, claiming that we should base professional conduct

⁷⁰ Interview with Steven A. Marks, Chief Information Officer, Sills Cummis and Gross P.C., in Newark, N.J. (Mar. 19, 2009); Telephone Interview with Salvatore A. Galluccio, Director of Information Technology, Landman CorsiBallaine & Ford P.C. (Apr. 9, 2009). There are 148 attorneys at Sills Cummis and Gross P.C. and 54 attorneys at Landman Corsi Ballaine & Ford P.C. *Id.*

⁷¹ *Id.* Both firms use metadata removal software from Workshare, <http://www.workshare.com/go/metadata-software.aspx> (last visited Apr. 12, 2009) *Id.*

⁷² <http://office.microsoft.com/en-us/help/HA010776461033.aspx> (last visited Apr. 13, 2009).

⁷³ Interview with Ari Gal, Ari Gal Law Office, in New York, N.Y. (Apr. 1, 2009).

⁷⁴ Interview with Daniel Gershburg, Daniel Gershburg Esq., P.C., in New York, N.Y. (Apr. 1, 2009).

rules on the resource inequity between large and small law firms is not an accepted argument. For example, large law firms have better access to online and print legal research materials, yet we hold all lawyers to the same standard of legal research when accessing competent representation. On the whole, there are no Model Rules of Professional Conduct that specify one permissible course of action for large firm lawyers and another for small firm lawyers based on access to resources. There is one standard for all lawyers. The logic that we should allow lawyers to view metadata in documents they receive because smaller law firms have fewer resources is not followed anywhere within the Model Rules of Professional Conduct. Third, part of being a competent lawyer is understanding the inherent risks in the way lawyers communicate with each other. Technological ignorance should not be an excuse to revealing information through metadata. Additionally, removing metadata from an electronic document manually is not so burdensome that it would be unreasonable to expect the lawyer who sends the document to do it.

E. Other Ways Confidential Information is Protected

Placing a restriction on lawyers searching and reviewing metadata within electronic documents is not the only method to inhibit the release of confidential information. The attorney-client privilege, one of the oldest privileges dealing with confidential communication, protects information between a client and a lawyer.⁷⁵ Another evidentiary privilege is the work product doctrine, which provides for qualified privilege of materials prepared by attorneys for litigation.⁷⁶ If lawyers attempt to bring information into discovery, these two privileges may bar such an act. The main wrinkle with these protections in terms of metadata is that some jurisdictions have held that both of these privileges may be waived in certain circumstances where the lawyer inadvertently releases information.⁷⁷ The law on waiver varies state to state.⁷⁸ In many jurisdictions, these protections are in place to protect certain information that may be released inadvertently. These privileges, combined with placing an ethical burden on the sender of a document to prevent the release of confidential information through metadata, will limit confidentiality breaches in the discovery context without making it unethical for the sender to review metadata.

⁷⁵ See Edward A. Morse, *Technological Entanglements: Evidentiary and Ethical Considerations of Metadata in Interjurisdictional Litigation*, 2 CREIGHTON J. INT'L COM. L. & TECH. 94, 95 (2007).

⁷⁶ *Id.* at 96.

⁷⁷ *Id.*

⁷⁸ *Id.* at 96–97.

F. The ABA Should Take the Next Logical Step

While the ABA makes it completely ethical for lawyers to search for and view metadata in electronic documents in all circumstances except fraud, they conceptually separate the metadata from the information on the face of the electronic document by specifically applying Model Rule of Professional Conduct 4.4(b) to metadata.⁷⁹ The rule says that a “lawyer who receives a document relating to the representation of the lawyer’s client and knows or should know that the document was inadvertently sent shall promptly notify the sender.”⁸⁰ While this rule appears to apply only to the document as a whole, the ABA’s ethical opinion applies the rule specifically to metadata and therefore separates the metadata from the rest of the electronic document so that metadata could be inadvertently sent while the rest of the electronic document was advertently sent.

The ABA has already taken the prudent position of allowing lawyers to view metadata without being accused of dishonest and deceit, but they should go one step further and state that, for ethical purposes, metadata cannot be separated from the rest of the electronic document. Rule 4.4 should apply if the lawyer “knows or should know” that the document as a whole was inadvertently sent. If the document as a whole was advertently sent then the metadata should also be considered advertently sent. Lawyers who send electronic documents should not be able to claim that while they advertently sent the electronic document, they inadvertently sent the metadata and therefore the receiving lawyer should have notified them.

This “no separation” rule is consistent with the law’s current acceptance of metadata as an integral part of the electronic document. Although those in favor of forbidding lawyers from viewing metadata tend to mystify the concept and focus on the word “mining” when referring to looking for metadata, searching for metadata is far similar to picking apples from a tree than digging for coal deep inside a mountain. By allowing the conceptual separation of the metadata from the rest of the document, the ABA is supporting the logic that it rejected in deciding that it was completely ethical for lawyers to view metadata.

V. Conclusion

Based on the foregoing reasons, creating an ethical violation when a receiving attorney searches for or views metadata is not prudent in a legal, technological or practical sense. To

⁷⁹ See *infra* text accompanying notes 36–37.

⁸⁰ ABA Comm. on Ethics and Prof’l Responsibility, Formal Op. 16-442 (2006).

protect the disclosure of unintended information through metadata, the sole burden should be on the lawyer who sends the electronic document. The law has moved towards accepting information found in the metadata of a document as part of the actual documents itself. Metadata can contain very important information that, in many cases, is necessary for a court to reach an equitable determination. Professional conduct rules should not fight this development by trying to ethically separate the metadata from the document itself. In a technological sense, the knowledge of metadata is growing. There will always be new technology that alters the way lawyers send and receive information. Viewing metadata should not be unethical just because some lawyers are not aware of the risk. Practically, the only time a lawyer will reveal that they viewed metadata would be to try and admit it as part of a document for discovery. In this context, it is unclear what a court will do in light of the *Williams* case and the new amendments to the Federal Rules of Civil Procedure. If a lawyer simply views inadvertently sent information or counsel strategy, there is no reason why they would admit it. Therefore making a rule against viewing metadata would be creating an unenforceable ethical violation whereas placing the burden solely on the sender to prevent the release of confidential information through metadata creates a uniform and easily enforceable rule. Additionally, many law firms have automatic metadata removal software in place, which makes it extremely easy to place the sole burden on the sender to refrain from revealing unintended information through metadata. In the future, the ABA should clarify their position so that, for ethical purposes, metadata is not separable from the rest of the electronic document. This will bring the ABA in line with the current trend in the law and the reality of modern legal practice instead of fighting an established technological development in the way lawyers communicate.