

**Beneath the Surface:
Metadata, Transparency and the Ethical Use of Information**

Table of Contents

- I. Introduction
 - A. Attorneys and Information
 - B. What is Metadata?
 - C. Fact Pattern: How might you be affected?
- II. Interacting Rules, Conflicting Interpretations
 - A. Rule Interaction Creates Confusion
 - B. Overview: Voluntarily Sent v. Required by Discovery
 - C. Overview: Sender v. Recipient
 - D. Different Jurisdictions, Different Rules
 - i. New York: An Early Approach
 - ii. Florida and Alabama
 - iii. Maryland
 - iv. Washington D.C.
 - v. Arizona
 - vi. Pennsylvania
 - E. The ABA Weighs In
- III. A Positive Response To State Opinions
- IV. The ABA Got It Right
 - A. Metadata is Becoming More Integrated Into Daily Life
 - B. State Bar Associations are Asking the Wrong Questions
 - C. Ethics as an Excuse for Remaining Ignorant of Technology
- V. Conclusion

I. INTRODUCTION

A. ATTORNEYS AND INFORMATION

Information. Data. Facts. These are the fundamental building blocks of a lawyer's environment. It is a lawyer's understanding of what must, in fairness, be presented and what must be kept confidential which sets the boundaries of ethical disclosure and privilege or confidentiality in the legal world.¹ With the rapid transition away from paper, or analog form, to digital, electronically created, stored and transferred data, information is now ubiquitous, forming a virtual sea in which modern lawyers live. From software at the heart of patent litigation to emails in an employment case to voicemails and text messages sent after a car accident, digital information is now involved in nearly every case.²

While the gains from the digital revolution are tremendous in terms of increased efficiency, access to information and searchability, the change in information format has caught some off guard. No longer is data limited to what is available on a piece of paper. Where once a letter would be mailed or faxed, today an attorney emails a word processing document or spreadsheet. Yet there is a price to pay for these gains. Where once a letter's recipient could not see anything but what the sender openly presented in the letter, today that email, word processing document and spreadsheet all contain additional information not readily visible on their face. Beneath the surface, packed into the file, exists metadata.

B. WHAT IS METADATA?

Generally speaking, metadata is information about information. As a class of information, metadata is most commonly used to record a file's owner, changes made to that file, the file's relationship to other files, and to label the file with keywords. As a tool, metadata is information

¹ MRPC 1.6.

² Embedded Data PowerPoint Presentation, ABA (2007).

that “describes, explains, locates or otherwise make it easier to retrieve, use, or manage an information resource.”³

Most importantly, the vast majority of a file’s metadata is invisible to someone who simply opens the document. Because it is generally hidden by design, danger arises for lawyers who are unaware that when someone opens a file, they are not seeing all of that file’s contents. While the public generally understands that phone calls and email leave a trail, less well known is the fact that all digital information leaves a digital footprint, and that by default, these footprints travel with their host.

C. FACT PATTERN: HOW MIGHT YOU BE AFFECTED?

So how might metadata effect a lawyer in their everyday practice? Imagine that you are the general counsel of a small software company. You have just been asked to indemnify a business partner, the manufacturer and distributor of the hardware on which your software runs, in a patent infringement suit. The suit levied against your much larger hardware partner targets software contributed by your company. As an action is pending and an indemnity request has been made, you must comply with the Federal Rules of Civil Procedure (“FRCP”). You tell your IT department to do everything reasonable to freeze all digital information and retain all further information,⁴ and hire an outside expert to work with your engineers and evaluate your code to identify possibly infringing code.

Understanding that emails will be open to discovery, everyone is instructed to handle all discussions via phone or face-to-face. Supporting word processing documents and spreadsheets are prepared via master files located on a shared, internal company computer. Different methods

³ *Understanding Metadata*, Niso Press (2004)(<http://www.niso.org/standards/resources/UnderstandingMetadata.pdf>).

⁴ *Zubulake v. UBS Warburg LLC* 220 F.R.D 212 (S.D.N.Y. 2003). *Cache la Poudre Feeds v. Land O’ Lakes*, 244 F.R.D. 614 (D. Colo. 2007)(Discussing when a demand letter makes a suit likely).

for calculating possible damages are experimented with in spreadsheets. Drafts are digitally redlined. Errors are corrected. Trade secrets and confidential information are redacted. Working for a small software company means that you are working on a budget. During discovery you jump at the chance to eliminate storage costs and readily agree to your opposing counsel's suggestion that both sides provide all information and documents electronically via DVD.

Weeks pass and settlement negotiations begin. At your first meeting, your opponent hands out a binder. In it are your company's trade secrets and confidential information. This information was included in early drafts of discovered documents, but you are certain that this information was digitally erased before the documents were sent out. Before you even speak, your opponent attacks your strategy, developed and discussed via digital notes with your outside counsel but, again, removed from documents before transmission to your opponent. When you suggest a settlement amount, your opponent declines and names a higher number. Amazingly, this new amount is the exact amount set by your consultants in an early draft of a spreadsheet valuing and calculating potential damages. You have no idea how your opponent obtained all of this information, but your negotiating position is gone. Did they have a spy? Was someone leaking information? Only after your company agrees to your opponent's draconian terms does your opponent let you in on their secret. You sent the information to them, in the very files you approved for transmission. Their secret weapon was the metadata in those files. Metadata you never even realized you created.

II. INTERACTING RULES, CONFLICTING INTERPRETATIONS

You feel violated. Your opponent used redacted, digitally erased information against your company. "Not all of this information [was] a confidence or secret, but" the revelation still

caused great damage to your company.⁵ You never intended to send over metadata, and your opponent should have known that it was not meant for their eyes.⁶ You feel certain that your opponent committed ethics violations. Unfortunately, you find that not all jurisdictions agree with you.

A. RULE INTERACTION CREATES CONFUSION

Key distinctions arise when states differ in their adoption of existing ABA Ethical Opinions and Model Rules, and in interpreting and deciding when these rules should apply. All agree that recent amendments to the FRCP addressed procedures for dealing generally with electronic documents, and all recognize that “claw back” agreements are recommended.⁷ Not all jurisdictions agree, however, on whether or how metadata is covered by these amendments.

B. OVERVIEW: VOLUNTARILY SENT V. REQUIRED BY DISCOVERY

When setting the ethical duties relating to a lawyer’s protection or use of metadata, jurisdictions “distinguish between electronic documents provided in discovery or pursuant to a subpoena from those electronic documents voluntarily provided by opposing counsel.”⁸ Key here is the requirement that documents sent via a legal request must be frozen per the FRCP.⁹ The sender’s legal ability to scrub metadata is no longer available once the sender should know that the document may be relevant.¹⁰ Accordingly, the sender’s ability to redact information is limited to information which is privileged or confidential.¹¹ In contrast, metadata associated with

⁵ N.Y. State Bar Ass’n Comm. On Prof’l Eth., Op. 782 (2004).

⁶ Model Rules possibly implicated by questions around waiver of privilege and the inadvertent sending of metadata include Rules: (a) 1.6 (Confidentiality of Information); (b) 3.4 (Fairness to Opposing Party and Counsel); (c) 4.4 (Respect for Rights of Third Persons); and (d) 8.4 (Misconduct). DC Bar Opinion 341, *Review and Use of Metadata in Electronic Documents*.

⁷ FRCP Rules 26(f)(3) (Conference of Parties to Discuss ESI), 26(b)(2)(B) (Revised Procedure For Discovery of ESI That Is Not Reasonably Accessible), 37(f) (Safe Harbor Provision For Good-Faith Disposal of ESI) (2006).

⁸ DC Bar Opinion 341, *Review and Use of Metadata in Electronic Documents*. (Florida and Alabama have recognized this distinction. The ABA and Maryland have not.)

⁹ See *Zubulake*.

¹⁰ *Id.*

¹¹ MD State Bar Ass’n. Comm. on Ethics Op. 2007-09 (Oct 16, 2006).

volunteered documents are afforded varying degrees of leeway. For example, some states give deference to the sender, allowing the removal of inadvertently sent metadata contained in volunteered documents. Other states place the burden upon the sending lawyer to thoroughly scrub all voluntarily provided documents prior to sending and allow unrestrained metadata mining.¹²

Recipient duties and authorization to search through received metadata parallel the distinction and reasoning for senders. The recipient is generally free to mine or search metadata of a document supplied via discovery or federal court proceeding. The document, including its metadata, are procedurally frozen and are therefore wholly available to the opposition. The ability to search through metadata is greatly restricted in some jurisdictions. However, where the sender has volunteered the documents at issue, the recipient must refrain from searching through metadata that the recipient should know is privileged or was not intentionally sent.

C. OVERVIEW: SENDER V. RECIPIENT

Ethical rules consistently distinguish between the duties and responsibilities of the sending party and the duties and limitations imposed on the receiving party. The sender theoretically retains complete control of all documents before sending them to the opposition's counsel and must therefore "take reasonable precautions to prevent privileged information from getting to unintended recipients."¹³ States differ in defining which precautions are reasonable, from completely exonerating an attorney who sends metadata to an opponent to imposing a duty upon the sender to remove all metadata that would normally remain confidential or privileged were the document paper and not electronic.¹⁴

¹² *Id.*

¹³ MRPC Rule 1.6, cmt. 17.

¹⁴ "While in some cases scrubbing files for metadata might be necessary to preserve attorney-client privilege, scrubbing data before turning over documents in discovery could actually be unethical, since it destroys evidence

The duty for recipients of electronic documents containing metadata is also subject to varied interpretation. Some states analogize to paper documents and apply the model rules - rules originally designed for analog issues. In those jurisdictions, “[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.”¹⁵ As “[i]t is professional misconduct for a lawyer to . . . engage in conduct involving dishonesty, fraud, deceit or misrepresentation,” these states argue that sifting through any of a document besides what is clear on the document’s face is dishonest.¹⁶ Other states, feeling that the onus is on the sender to control their information, consider the entire document as fair game; all information attached to a document that was intentionally sent is part of that intentional send and is therefore searchable data once in the hands of the recipient.

D. DIFFERENT JURISDICTIONS, DIFFERENT RULES

i. NEW YORK: AN EARLY APPROACH

New York was the first state bar association to issue an opinion on the ethical implications of mining metadata.¹⁷ Their ruling? Protect the sender. The New York lawyer who uses technology to communicate with clients must use reasonable care, which “will vary with the circumstances” and “may . . . call for the lawyer to stay abreast of technological advances.”¹⁸

contained in the page.” In *Williams v. Sprint*, (2005), the “plaintiffs in the case claimed that metadata had been scrubbed from the spreadsheets provided during discovery. The court found that while the emerging standards governing electronic discovery appeared to have a general presumption against producing metadata in discovery, the employer in the case had to turn over the metadata, since it had not claimed the electronic data as privileged information earlier in the case. Although the case law is murky on the issue, some attorneys say sanctions for spoliation of evidence could be possible if documents were scrubbed in production.” Walker, Jessica, *What's a Little Metadata Mining Between Colleagues?*, Daily Business Review (Apr. 21, 2006).

¹⁵ MRPC Rule 4.4(b).

¹⁶ MRPC Rule 8.4(c).

¹⁷ N.Y. State Bar Ass’n Comm. On Prof’l Eth., Op. 749 (2001).

¹⁸ N.Y. State Bar Ass’n Comm. On Prof’l Eth., Op. 709 (1998)(A N.Y. attorney must assess the risks attendant to the use of that technology and determine if the mode of transmission is appropriate under the circumstances). See also Op. 782 (2004)(“Lawyers have a duty . . . to prevent the disclosure of metadata containing client confidences or secrets,” and this duty extends to emails and digital files).

While New York appears to state that attorneys are responsible for unintentionally sent metadata, the rule lacks teeth. The only definitive requirement is to stay aware of the latest relevant technology, and then only when the circumstances require.

Pairing New York's rule for senders with the state's requirements for recipients of metadata shows that the duty and burden in New York is placed squarely on the recipient. Using "technology to access client confidences and secrets revealed in metadata constitutes an impermissible intrusion on the attorney-client relationship. . . ." ¹⁹ The recipient must also notify the sender of the inadvertent disclosure, and abide by the will of the sender in further metadata handling. ²⁰ The rationale for not allowing use of unintentionally sent metadata was to avoid "exploit[ing] an unauthorized communication, because doing so would constitute . . . misrepresentation[,] prejudicial to the administration of justice." ²¹

ii. FLORIDA AND ALABAMA

Florida's Bar looked to Model Rule 4.4 and to its prior opinions regarding the receipt of inadvertently sent paper documents when setting its ethical standard regarding metadata. ²² Florida decided that the sender must take reasonable steps to protect confidential metadata, while it is the recipient's duty to refrain from using metadata if the recipient "knows or should know" the information was not intended for the recipient and "promptly notify the sender". ^{23,24}

¹⁹ N.Y. State Bar Ass'n Comm. On Prof'l Eth., Op. 782 (2004) ("Lawyer-recipients have an obligation not to exploit an inadvertent or unauthorized transmission of client confidences or secrets").

²⁰ *Id.*

²¹ N.Y. State Bar Ass'n Comm. On Prof'l Eth. DR 1-102(A)(4) and DR 1-102(A)(5).

²² Prof. Ethics of the FL Bar Op. 06-2 (Sept. 15, 2006).

(<http://www.floridabar.org/tfb/tfbetopin.nsf/SearchView/ETHICS,+OPINION+06-2?opendocument>) (Last viewed Oct. 21, 2007).

²³ *Id.* citing Ethics Op. 93-3 and Rule 4-4.4(b), FL Rules of Prof. Conduct, effective May 22, 2006. ([R]ecipient lawyer's . . . obligation, upon receiving an electronic communication or document from another lawyer, 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 the recipient. Any such metadata is to be considered . . . as confidential" and unintentionally sent).

²⁴ This is true even "if the recipient lawyer inadvertently obtains information from metadata that the recipient knows or should know was not intended for the recipient," *Id.*

Similarly, Alabama found “that mining metadata (outside the context of discovery) is dishonest.”²⁵

iii. MARYLAND

Like New York, Maryland also sets the duty for lawyers producing electronic materials to a reasonableness standard, with a goal of avoiding the disclosure of confidential metadata.²⁶ Maryland’s Bar, however, was greatly influenced by the recent FRCP amendments relating to electronic documents.²⁷ As such, Maryland lawyers who receive electronic discovery materials are expected to discuss the treatment of metadata beforehand and therefore have no ethical duty to refrain from viewing or using metadata.²⁸

iv. WASHINGTON D.C.

The D.C. Bar also relied in part on the FRCP’s recent amendments requiring parties to “consult at the outset of the case” and allowing for “claw back” agreements.^{29,30} Accordingly, if the recipient has prior knowledge that metadata was sent inadvertently, the recipient must consult with the sender before proceeding.³¹ Distinct in the District of Columbia is that Model Rule 8.4 applies, but only if there is “prior knowledge,” and then only if the document was voluntarily sent.³² Mere uncertainty about whether or not the sender intended to include metadata is not enough to constitute “prior knowledge.” If sent during discovery, the recipient can assume the

²⁵ Hricik, David, *Alabama Bans Metadata Mining*, May 16, 2007. (<http://www.legalethics.com/?p=420>)(Last viewed Oct. 21, 2007).

²⁶ MD State Bar Ass’n. Comm. on Ethics Op. 2007-09 (Oct 16, 2006).

²⁷ See *Preparing for Litigation Under the New Federal Electronic Discovery Rules*, Orrick Client Alert (Dec. 18, 2006).

²⁸ MD State Bar Ass’n. Comm. on Ethics Op. 2007-09 (Oct. 16, 2006).

²⁹ The D.C. Bar looked to MRPC 4.4(b) and found that metadata should be included in document discussion. “Although the purpose of Rule 4.4(b) was to address the inadvertent disclosure of entire documents . . . we see no reason why it would not also apply to [a] . . . portion of a writing that is otherwise intentionally sent.” As such, claw back discussions should include “requested metadata and how to handle the sender’s claim of privilege.” *Id.*

³⁰ Further, the D.C. opinion leaves open the option for the recipient to challenge any sender claim of privilege.

³¹ *Id.*

³² *Id.*

metadata was provided intentionally.³³ Even if the recipient has actual, prior knowledge, the recipient *should* notify the sender, but does not *require* the recipient to do so.³⁴

v. ARIZONA

Arizona recognizes that a sender must “take reasonable measures to prevent the inadvertent disclosure of confidential client information,” yet Arizona’s Bar feels that there is always risk of inadvertent transmission of metadata.³⁵ Therefore, the Bar argues that without protection from an ethics ruling, the sending attorney will likely forego sending relevant documents in order to mitigate this risk and meet their ethical duty to their client.³⁶ So, too, is the recipient of an electronic document precluded from “examin[ing] it for the purpose of discovering the metadata embedded in it.”³⁷ Arizona interprets Rule 4.4 as being applicable to metadata associated with electronic documents.³⁸ As such, a recipient attorney who only “knows or should know that the transmission of metadata was inadvertent has a duty to comply with Rule 4.4.”³⁹ Effectively, then, Arizona has precluded the recipient from searching or using metadata.

vi. PENNSYLVANIA

Pennsylvania’s ruling, limited to “circumstances in which it is clear that the materials were not intended for the receiving lawyer,”⁴⁰ offers little real guidance for its attorneys. After reviewing the prior decisions in all other jurisdictions, Pennsylvania looked not to the near future

³³ *Id.*

³⁴ *Id.*

³⁵ AZ Formal Op. 07-03: *Confidentiality; Electronic Communications; Inadvertent Disclosure* (Nov. 2007) [hereinafter Op. 07-03].

³⁶ *Id.* (“Despite the most reasonable and thorough precautions, and even with the best of intentions, it may not be possible for the sending lawyer to be absolutely certain that all of the potentially harmful metadata has been “scrubbed” from the document before it is transmitted electronically. Under the ABA position, the sending lawyer would be at the mercy of the recipient lawyer. Under such circumstances, the sending lawyer might conclude that the only ethically safe course of action is to forego the use of electronic document transmission entirely. We do not think that is realistic or necessary.”).

³⁷ *Id.*

³⁸ *Id.*

³⁹ *Id.*

⁴⁰ 30-FEB PALAW 46 (2008).

but instead to the current state of rapidly evolving digital technology, along with its own ethical rules, for guidance.

The Opinion first looks at the interaction of Rule 4.4(b) and Rule 1.6 and argues that:

[I]t 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. The absence of a specific rule addressing the inadvertent disclosure of metadata may also be viewed as analogous to the inadvertent disclosure of a document and not an act consciously undertaken by counsel.⁴¹

Next, the Opinion weighs the effectiveness of modern metadata scrubbing technology. Although transmitting attorneys have tools at their “disposal that can minimize the amount of metadata contained in a [transmitted] document,” Pennsylvania determined that “those tools still may not remove all metadata.”⁴² Finally, the American Bar Association’s (“ABA”) recommendation that attorneys protect themselves from the inadvertent disclosure of confidential or privileged information via metadata by applying several techniques including “negotiation of a confidentiality agreement or protective order that allows the transmitting attorney to ‘pull back’ transmitted documents” is considered.⁴³ As Pennsylvania determined that these tools, even taken together, “will not always adequately protect an attorney,” the Opinion opts to not follow the example of the ABA.⁴⁴

Instead, attorneys in Pennsylvania are left to determine for themselves, by weighing several fact-specific factors, “whether to utilize the metadata contained in documents and other electronic files.”⁴⁵ Pennsylvania explicitly states that even with publication of the new Opinion,

⁴¹ *Id.* at 48-49.

⁴² *Id.* at 52.

⁴³ *Id.* at 50.

⁴⁴ *Id.* at 48.

⁴⁵ *Id.* at 52.

“there is still no specific Pennsylvania rule of professional conduct determining the ethical obligations of a lawyer receiving inadvertently transmitted metadata from another lawyer.”⁴⁶

Ultimately, then, the decision is left to “the lawyer's judgment and the particular factual situation.”⁴⁷

E. THE ABA WEIGHS IN⁴⁸

The ABA takes a contrasting approach. In a narrowly written formal opinion, the ABA ruled that the protection of metadata is the responsibility of the sender; if a document is sent intentionally, all information attached to that document is intentionally sent as well.⁴⁹ As such, the recipient is free to search through all received electronic information, using all available tools and techniques.⁵⁰

The Lawyer's Code of Professional Responsibility (the "Code") prohibits lawyers from knowingly revealing a client confidence or secret, DR 4-101(B)(1), except when permitted under one of five exceptions enumerated in DR 4-101(C). DR 4-101(D) states that a lawyer shall exercise *reasonable care* to prevent his or her employees, associates, and others whose services are utilized by the lawyer from disclosing or using confidences or secrets of a client.⁵¹

The ABA set its requirement of “reasonable care” based on the understanding that the sender retains control of the electronic documents—and of the documents’ associated metadata—until the documents are sent to the recipient.⁵² Further, the ABA “disagre[ed] with the proposition that

⁴⁶ *Id.* at 46.

⁴⁷ *Id.*

⁴⁸ As “the Oregon Rule[s] of Professional Responsibility closely follow the ABA Model Rules, and the Model Rules discussed in ABA Op. No. 06-442 are identical to their Oregon counterparts,” Oregon has followed the ABA’s ruling. Stevens, Sylvia E., *Metadata: Guarding Against the Disclosure of Embedded Information* n. 3, Oregon State Bar Bulletin, Apr. 2007, <http://www.osbar.org/publications/bulletin/07apr/barcounsel.html> (last viewed Nov. 27, 2007). *See also* Fucile, Mark J., *Brave New World: Risk Management in the Electronic Era*, Oregon State Bar Bulletin, Oct. 2007, <http://www.osbar.org/publications/bulletin/07oct/practice.html> (last viewed Nov. 27, 2007).

⁴⁹ ABA Formal Op. 06-442 (Aug. 5, 2006) [hereinafter Op. 06-442].

⁵⁰ *Id.*

⁵¹ N.Y. State Bar Ass’n Comm. On Prof’l Eth., Op. 782 (2004). (Emphasis added).

⁵² Op. 06-442 *supra* note 49 at 5.

embedded data is never unintentionally sent.”⁵³ Realizing that there are many tools available to remove metadata, the duty to remove metadata is seen as reasonable and is placed squarely on the sending lawyer.⁵⁴ Accordingly, the ABA set a low bar for the recipient, stating that Rule 4.4(b) “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.”⁵⁵ Lawyers, then, are “free to look for and use information hidden in metadata . . . even if the documents were provided by an opposing lawyer.”⁵⁶

III. A POSITIVE RESPONSE TO STATE OPINIONS

David Hricik argues that the ABA’s rule “permits lawyers to intentionally take advantage of other people’s failures.”⁵⁷ Hricik agrees with the majority of state opinions in viewing metadata mining as dishonest and in violation of ethical rules. Hricik argues that mining metadata results in obtaining clear, thorough, relevant information almost certainly not intended for public consumption.

[I]t is hard to imagine a scenario where a lawyer would *intentionally* include confidential information in the form of embedded information . . . [so] a lawyer at least *should know* that any embedded confidential information was sent inadvertently.⁵⁸

IV. THE ABA GOT IT RIGHT

⁵³ Hricik, David, *Mining for Embedded Data: Is It Ethical to Take Intentional Advantage of Other People’s Failures?*, N.C.J.L. & Tech. Vol. 8, Issue 2 231 at 240 (Spring 2007)(citing *Id.* at 3).

⁵⁴ Op. 06-442 *supra* note 49 at 5.

⁵⁵ ABA Formal Op. 05-437 (Oct. 1, 2005) [hereinafter Op. 05-4437].*Inadvertent Disclosure of Confidential Materials: Withdrawal of Formal Opinion 92-368 November 10, 1992* (2005)

⁵⁶ Slonim, Nancy, *Lawyers Receiving Electronic Documents are Free to Examine 'Hidden' Metadata: ABA Ethics Opinion*, ABA News Release, Nov. 9, 2006, http://www.abanet.org/abanet/media/release/news_release.cfm?releaseid=48 (last viewed Nov. 26, 2007).

⁵⁷ Hricik, David, *Mining for Embedded Data: Is It Ethical to Take Intentional Advantage of Other People’s Failures?*, N.C.J.L. & Tech. Vol. 8, Issue 2 231 at 241-2 (Spring 2007).

⁵⁸ *Id.* at 241.

A. METADATA IS BECOMING MORE INTEGRATED INTO DAILY LIFE

While widespread use of metadata is still in its infancy, awareness of metadata has existed in technology arenas for decades and will only continue to grow in importance, complexity, and integration into all forms of digital information.⁵⁹ The latest iterations of Microsoft's Vista and Apple's OS X operating systems are illustrative, as both greatly increase the default availability, customization and use of metadata.⁶⁰ Both also automatically index all file metadata, allowing computer users to personally modify and search metadata. For example, a salesman who wants to identify difficult customers can label related files with the words "bad customers."⁶¹ The problem arises when that otherwise innocuous file is sent to opposing counsel in litigation involving those very customers. A simple query for the word "bad" or "customers" will list the salesman's file in the recipient's search results—proof that the salesman thought of the plaintiff as a bad customer. Worse, opposing counsel obtained that information from the salesman's own attorney.

As new technology develops, refraining from searching through metadata becomes increasingly difficult. Metadata is being integrated into our daily lives. In the salesman scenario the recipient only stumbled upon the metadata, but this is not much different from actively scanning files to find useful information. Looking through metadata is not much more difficult or time consuming than looking at the face of the presented file. What's more, removing metadata is just as easy, and is becoming easier on a pace that parallels the increased efficacy of metadata

⁵⁹ Karpman, Diane, *Metadata can cause lawyers megaproblems*, CA Bar Journal, Jul. 2007, http://calbar.ca.gov/state/calbar/calbar_cbj.jsp?sCategoryPath=/Home/Attorney%20Resources/California%20Bar%20Journal/July2007&MONTH=July&YEAR=2007&sCatHtmlTitle=Discipline&sJournalCategory=YES&sCatHtmlPath=cbj/2007-07_Discipline_Ethics-Byte.html&sSubCatHtmlTitle=Ethics%20Byte (last viewed Nov. 26, 2007).

⁶⁰ Evers, Joris, *Watch out with metadata in Vista, analysts warn*, Dec. 22, 2005 (http://www.news.com/Watch-out-with-metadata-in-Vista,-analysts-warn/2100-1012_3-6006290.html?tag=item) (Last viewed Oct. 21, 2007).

⁶¹ Reader Poll, Lifestacker.com (<http://lifestacker.com/software/reader-poll/do-you-tag-your-files-offline-313914.php>).

searching.⁶² If searching through metadata is cost-effective for the recipient, scrubbing out metadata is equally cost-effective for the sender.⁶³

B. STATE BAR ASSOCIATIONS ARE ASKING THE WRONG QUESTIONS

Instead of asking about the intent of the sender and applying rationale to determine whether a send was inadvertent, state bar associations should be looking at the volume and scope of metadata and asking how lawyers will work with all information in the future. Searching through metadata is an activity that, at its core, is quite similar to past technological advances such as obtaining phone records attached to a cell phone, IP addresses from emails, fingerprints from a letter, or transaction statements from a bank.⁶⁴ All of these pieces of information are fully discoverable, ethical both to search and to use. Opponents of metadata mining, such as Professor Hricik, argue that the sender could never intend for anyone to see the information if the sender did not even know it was there. Yet the same could be said of those past technological advances as well; at some point in the societal adoption of the then-new technology, the average attorney did not know of the data's existence or intend that opponents find that information, either. 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.⁶⁵

C. ETHICS AS AN EXCUSE FOR REMAINING IGNORANT OF TECHNOLOGY

An advocate must represent their client fully and zealously.⁶⁶ Deciding to not search through metadata with easy-to-use tools should be seen as a missed opportunity to investigate on

⁶² “[R]ates for electronic recovery can run as high as \$500 per hour in a complex case . . . [b]ut some metadata mining is simple, involving basic maneuvers any user can conduct on office software.” Walker, Jessica, *What's a Little Metadata Mining Between Colleagues?*, Daily Business Review (Apr. 21, 2006).

⁶³ The sending attorney has a duty not to violate attorney-client privilege. So I should be scrubbing data.” *Id.*

⁶⁴ “[I]n some circles, a policy of banning metadata mining is thought of as “ridiculous.” “[I]f you sent me a contract, I can have it fingerprinted to see who's handled it.” Searching through “metadata [is] the same thing.” *Id.*

⁶⁵ “As the details of metadata mining ethics are hammered out, many attorneys face a learning curve. They'll discover electronic data can be used for or against them.” *Id.*

⁶⁶ MRPC 1.2.

behalf of a client.⁶⁷ Excusing the transmission of privileged information via metadata now because of ignorance will only perpetuate ignorance and further slow the Bar's adoption of new technology, of new sources of information, and of modern methods of keeping, sending and using information.⁶⁸

By forcing lawyers to be aware of and responsible for metadata, the ABA provides a stick to encourage lawyers to adapt to new technology.⁶⁹ Further, by allowing lawyers to mine metadata, the ABA provides a carrot as incentive and sends a consistent message that all content provided by lawyers is transparent.⁷⁰ Nothing is hidden.⁷¹ Instead of cutting up electronic documents into constituent parts of varying importance and speculating on the sender's intent or the recipient's motives, the ABA argues that whatever is sent is, in its entirety, fair game. This rule is simple, clear and direct, forces the sending attorney to review documents before transmission, and allows for full disclosure to the recipient.

V. CONCLUSION

The current legal landscape for metadata ranges from restricting nearly all recipient use of metadata to placing the burden of responsibility on the sender and allowing full search by the

⁶⁷ "There might have been a prior version before the spin doctors got to it, saying we messed this up. Then they redrafted it to sweeten it up. It's always interesting to see those prior versions." In these cases, lawyers . . . could be giving their client the short shrift by not looking at the metadata." Walker, Jessica, *What's a Little Metadata Mining Between Colleagues?*, Daily Business Review (Apr. 21, 2006).

⁶⁸ "When Florida Bar president-elect Henry Coxe III brought up metadata mining to the Bar's board of governors, some board members conceded they had never heard of the practice. . . . At the board of governors meeting . . . he recounted the first time he became aware of metadata mining and its consequences. The partner at Coxe's firm had sent a[n electronic] brief to a lawyer at another firm. . . . Based on the brief, . . . the other firm was able to reconstruct every change that had been made to the document, including e-mails between Coxe's partner and his client -- a potential violation of attorney client privilege. Alarmed, . . . ,Coxe urged the board to declare unethical the practice of culling through electronic documents to find hidden data about the history of the document. . . . Some of the members had never even heard of metadata before the meeting, and they rushed to vote to condemn it." *Id.*

⁶⁹ "For example, in a case dealing with wage and hour laws, the employer might turn over a spreadsheet that calculated paychecks. The face of the spreadsheet might only show the end amount, but an attorney could mine the document's metadata to find out exactly what formula was used to calculate the paychecks." *Id.*

⁷⁰ Metadata was "an invaluable tool for ferreting out fraud and unethical individuals. . . . He had recently busted an individual that had a false certificate claiming that a part he had was manufactured by Balog's company. The smoking gun, in this case, was metadata contained in the certificate." *Id.*

⁷¹ An "example . . . is a letter blaming a party in a civil suit. . . . [C]ommonly, there are earlier drafts of a letter that may have distributed blame more widely." *Id.*

recipient.⁷² The ABA conducted a thorough analysis of the technological and ethical issues around metadata, resulting in the most ethically consistent, balanced and forward-thinking set of rules. The ABA recommends “claw back” agreements prior to information exchange, places no limit on use of metadata or on mining metadata by the receiving attorney, and puts the burden of protecting privileged or confidential information on the sender.

In setting these rules, the ABA assessed the utility and likely direction of technological development. The ABA also factored in the sender’s control over entire documents, including metadata, and on the impracticality of forcing recipients to decipher the sender’s intent. The ABA structured their ethical rules to reward the lawyer who keeps up with and adapts to the latest information technology and does not allow ignorance of technology as an excuse. By structuring their rules in this way, the ABA ensures that lawyers continue to master the tools central to use of information. Ethics boards in other jurisdictions would be wise to follow the ABA’s lead.

⁷² A modern attorney must be aware of the jurisdiction in which they are working and of changes in technology as it relates to information. All attorneys should work with Information Technology experts to make scrubbing part of the internal document handling procedures in their offices and in the offices of their clients.