The Sedona Conference Journal

Volume 14 2013

The Sedona Conference Commentary on Ethics & Metadata

The Sedona Conference

Recommended Citation:

The Sedona Conference, *Commentary on Ethics & Metadata*, 14 SEDONA CONF. J. 169 (2013).

For this and additional publications see:
https://thesedonaconference.org/publications

THE SEDONA CONFERENCE® COMMENTARY ON ETHICS & METADATA*

A Project of The Sedona Conference® Working Group on Electronic Document Retention & Production (WG1)

Author:
The Sedona Conference®

Senior Editors:
Ronald J. Hedges
Denise J. Talbert

Contributing Editors:
Monica Anderson
H. Gibbs Bauer
Kevin F. Brady
Adam Cohen
Arthur C. Fahlbusch
Jan D. Gibson
William E. Hoffman

WG1 Steering Committee Liaison:
Conor R. Crowley

We thank all of our Working Group Series℠ Sustaining and Annual Sponsors, whose support is essential to our ability to develop Working Group Series℠ publications. For a listing of our sponsors, click on the "Sponsors" navigation bar on the homepage of our website.

The opinions expressed in this publication, unless otherwise attributed, represent consensus views of the members of The Sedona Conference® Working Group 1. They do not necessarily represent the views of any of the individual participants or their employers, clients, or any other organizations to which any of the participants belong, nor do they necessarily represent official positions of The Sedona Conference®.

PREFACE

> "The enhanced possibility of inadvertent production of privileged or work product information, the stakes in the management of privilege reviews, and careless handling of client communications raise serious ethical issues. Similarly, the disparate views on how lawyers should treat metadata (e.g., when to delete, when to send, when to review) create additional risks for lawyers, especially in cases across different jurisdictions."[1]

The Sedona Conference® Commentary on Ethics and Metadata focuses on the ethical considerations[2] surrounding the inclusion and review of metadata in the non-discovery and discovery contexts. This Commentary is intended to provide practical guidance for lawyers in protecting confidential metadata and to assist the judiciary in fashioning appropriate discovery orders.

The *Sedona Principles Second Edition*[3] contains more detailed information about the ability to access and produce metadata. This Commentary does not presume to duplicate that work. Rather, this Commentary explores significant ethical duties of attorneys in handling metadata, which may constitute client confidences to be protected or evidence to be produced, depending on the circumstances.[4]

These duties must be explored within two very different contexts: the non-discovery context and the discovery context. It is critical throughout this Commentary and in understanding a lawyer's ethical obligations with respect to metadata to always *first* consider whether you are operating within the discovery or nondiscovery context.[5]

1. ***The Non-discovery Context:*** when lawyers send or receive information (i.e., "communications") containing metadata.[6]

2. ***The Discovery Context:*** when lawyers send, produce or receive electronically stored information (ESI) containing metadata in response to a discovery request or subpoena.

In general, the ethical duties of a lawyer relating to metadata follow the same principles of the ethical duties relating to any other type of information. An exception is

---

1] *The Sedona Principles, Second Edition: Best Practices Recommendations & Principles for Addressing Electronic Document Production* (2007), https://thesedonaconference.org/download-pub/81. ("Sedona Principles Second Edition") at 41.

2] This is the first Sedona Commentary devoted to ethics and electronic information. It is also the first Commentary to move beyond WG1's previously exclusive focus on aspects of discovery or records management/preservation.

3] The Commentary drafting team uses the definitions of metadata currently found in the *Sedona Principles* (2d Edition) and the *Sedona Glossary* (3d Edition), https://thesedonaconference.org/download-pub/471. There are a number of nuances associated with the various definitions of metadata used in the ethics opinions, in the case law, and by The Sedona Conference , and the definition of metadata is likely to evolve. However, attempting to harmonize these definitions or proposing an alternative definition of "metadata" is beyond the scope of the Commentary.

4] This Commentary addresses a lawyer's ethical duty established by a jurisdiction's rules of professional conduct (and, in some contexts, more broadly to include any duty imposed on a lawyer by any statute, rule, or case law). The duties discussed apply to a lawyer and not to a client, party, or other nonlawyer. For example, discovery is between parties, but lawyers are the responsible gatekeepers. Hence, we often refer to what a lawyer produces or receives.

5] "In assessing the ethical obligations of both the sending and receiving lawyer with respect to metadata, we find it useful to distinguish between electronic documents provided in discovery or pursuant to a subpoena from those electronic documents voluntarily provided by opposing counsel. Although the Florida and Alabama Bars have recognized a similar distinction, *see* Florida Bar Op. 06-2; Alabama State Bar, Office of Gen. Counsel Op. No. R0-2007-02, the distinction has not been universally recognized in other ethics opinions addressing metadata. *See* ABA Formal Op. 06-442; Maryland Bar Ass'n Ethics Docket No. 2007-09." District of Columbia Bar Opinion 341 (Sept. 2007).

6] Metadata outside the context of discovery may include information – often lawyer-created – *about* discovery obligations, such as circulating a draft Case Management Order for comment by the opposing party.

found in a few jurisdictions that make some presumptions about metadata and, essentially, equate *metadata* with *confidential information* and may not recognize the distinctions between the different types of metadata. For the receiving lawyer in the non-discovery context, as discussed below, there is wide disparity among the state bar associations relating to both (a) the review (potentially mislabeled "mining") of metadata and (b) the "notification" to the sending lawyer of receipt of metadata. Resolving the different approaches of such jurisdictions may present difficulties for a lawyer with a multijurisdictional practice and are also addressed.

Otherwise, for each jurisdiction, the action required of a lawyer who receives confidential metadata through inadvertence is the same action required of a lawyer who receives any other confidential information through inadvertence. For example, if a rule prohibits a lawyer from continuing to read a file once he or she has ascertained it is privileged, a lawyer may not continue to read metadata once he or she has ascertained it is privileged.[7]

And it is critical to also note that these *anti-mining* opinions do not generally apply to a lawyer's ethical obligations relating to documents sent or received pursuant to a request for production;[8] but only relate to metadata (and arguably only certain types of metadata) received in the non-discovery context.

The Commentary was first published for public comment in March 2012. In the year following there were several significant developments in the law, most notably the adoption by the American Bar Association House of Delegates in August 2012 of recommendations by the ABA Commission on Ethics 20/20 to extend a lawyer's duty of competence beyond simply competence in the law to competence in technology relevant to advising and representing clients. The editors have also considered and incorporated several dozen comments from members of The Sedona Conference® Working Group 1 on Electronic Document Retention and Production and from the public at large.

We hope our efforts will be of immediate and practical assistance to practicing lawyers, judges, those who advise lawyers on professional responsibility issues, and those who regulate professional conduct. As with all of our WGS℠ publications, we anticipate that developments in the law and technology will necessitate revisions and updates of this Commentary. Your comments and suggestions for future editions are welcome, and we urge you to visit The Sedona Conference® website at www.thesedonaconference.org to offer your comments on the public forum pages. You may also submit feedback by emailing us at info@sedonaconference.org.

Kenneth J. Withers
Director of Judicial Education
The Sedona Conference®
June 2013

7] *See, e.g., Rico v. Mitsubishi Motors Corp.*, 42 Cal. 4th 807, 68 Cal. Rptr. 3d 758 (Dec. 2007): "[A]n attorney who receives privileged documents through inadvertence ... may not read a document any more closely than is necessary to ascertain that it is privileged. Once it becomes apparent that the content is privileged, counsel must immediately notify opposing counsel and try to resolve the situation."

8] *See* n.4 above; *But also see* D.C. Bar Opinion 341 (Sept. 2007) ("[E]ven in the context of discovery or other judicial process, if a receiving lawyer has actual knowledge that metadata containing protected information was inadvertently sent by the sending lawyer, the receiving lawyer, under Rule 8.4(c), should advise the sending lawyer and determine whether such protected information was disclosed inadvertently. *See* D.C. Ethics Op. 256 ('The 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.').

PREFACE 170

I. ETHICS AND METADATA - BASIC CONCEPTS 173

A. What is Metadata? 173

B. A Lawyer's Primary Ethical Duties Regarding Metadata 175

II. A LAWYER'S ETHICAL OBLIGATIONS IN THE NON-DISCOVERY CONTEXT 178

A. Ethical Duties of a Lawyer *Sending* Metadata 178

B. Ethical Duties, *Generally*, of a Lawyer *Receiving* Metadata 178

C. *But see*, Certain Bar Opinions Prohibit *Mining* by a Lawyer *Receiving* Metadata 179

D. A Receiving Lawyer may Have a Good Reason – or Even an Obligation – to Search for Metadata 183

III. A LAWYER'S ETHICAL DUTIES REGARDING METADATA IN THE DISCOVERY CONTEXT 183

A. Discovery is Different – Usually 183

B. Ethical Duties of a Lawyer for a Party Producing Metadata 184

C. Ethical Duties of a Lawyer for a Party Receiving Metadata 185

IV. MULTIJURISDICTIONAL ISSUES 187

A. The Ethical Dilemma in the *Non-litigation Context* 188

B. Are Other Ethical Duties Implicated 188

C. Best Practices 188

V. MITIGATION 189

A. Metadata: Out of Sight, Out of Mind 189

B. Practical Tips 189

VI. CONCLUSION 190

I. ETHICS AND METADATA – BASIC CONCEPTS

A. What is Metadata?

Quite simply, metadata is often described as *data about data*.

Although a generally accurate description of metadata (i.e., *data about data*), the *Sedona Principles Second Edition* goes further and specifically notes the importance, in the discovery context, of distinguishing between the different types of metadata. "An electronic document or file usually includes not only the visible text but also hidden text, formatting codes, formulae, and other information associated with the file. These many types of ancillary information are often lumped together as 'metadata,' although some distinctions between different types of metadata should be recognized."[1]

These multiple types of metadata are identified and defined in the *Sedona Glossary*.[2] The *Sedona Glossary* contains a general definition for the term *metadata*. But the drafters of the *Sedona Glossary* moved well beyond this general definition and further identified seven different types of metadata and also referred to the more thorough discussion of metadata contained in the *Sedona Principles Second Edition* discussed above.[3] Also relying upon the *Sedona Principles Second Edition*, the court in *Aguilar*[4] recognized this idea that not all metadata is created equally in the discovery context and when resolving questions concerning the evidentiary value, relevance, or usefulness of metadata.[5]

The discussion in *Aguilar* begins with a general definition of metadata: "Metadata, frequently referred to as 'data about data,' is electronically-stored evidence that describes the 'history, tracking, or management of an electronic document.'"[6]

---

1 *The Sedona Principles, Second Edition: Best Practices Recommendations & Principles for Addressing Electronic Document Production* (2007), https://thesedonaconference.org/download-pub/81. ("Sedona Principles Second Edition") at 60.

2 *The Sedona Conference Glossary, Third Edition: E-Discovery & Digital Information Management* (2010), https://thesedonaconference.org/download-pub/471. ("*Sedona Glossary*").

3 *Id* at 33 citing the *Sedona Principles Second Edition* at 60 and citing the *Sedona Glossary Third Edition* at 3 17, 19, 22, 34, 52, 53. The *Sedona Glossary* includes, among others, the following types of metadata:
Application Metadata: Data created by the application specific to the ESI being addressed, embedded in the file and moved with the file when copied; copying may alter application metadata.
Document Metadata: Properties about the file stored in the file, as opposed to document content. Often this data is not immediately viewable in the software application used to create/edit the document but often can be accessed via a "Properties" view. Examples include document author and company, and create and revision dates.
Email Metadata: Data stored in the email about the email. Often this data is not even viewable in the email client application used to create the email, e.g., blind copy addresses, received date. The amount of email metadata available for a particular email varies greatly depending on the email system. Contrast with File System Metadata and Document Metadata.
Embedded Metadata: Generally hidden, but an integral part of ESI, such as "track changes" or "comments" in a word processing file or "notes" in a presentation file. While some metadata is routinely extracted during processing and conversion for e-discovery, embedded data may not be. Therefore, it may only be available in the original, native file.
File System Metadata: Metadata generated by the system to track the demographics (name, size, location, usage, etc.) of the ESI and, not embedded within, but stored externally from the ESI.
Metadata: Data typically stored electronically that describes characteristics of ESI, found in different places in different forms. [Metadata] [c]an be supplied by applications, users or the file system. Metadata can describe how, when and by whom ESI was collected, created, accessed, modified and how it is formatted. [Metadata] [c]an be altered intentionally or inadvertently. Certain metadata can be extracted when native files are processed for litigation. Some metadata, such as file dates and sizes, can easily be seen by users; other metadata can be hidden or embedded and unavailable to computer users who are not technically adept. Metadata is generally not reproduced in full form when a document is printed to paper or electronic image. *See also* Application Metadata, Document Metadata, Email Metadata, Embedded Metadata, File System Metadata, User-Added Metadata and Vendor-Added Metadata. For a more thorough discussion, *see* The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age (Second Edition).
User-Added Metadata: Data, possibly work product, created by a user while copying, reviewing, or working with a file, including annotations and subjective coding information.
Vendor-Added Metadata: Data created and maintained by the electronic discovery vendor as a result of processing the document. While some vendor-added metadata has direct value to customers, much of it is used for process reporting, chain of custody, and data accountability. Contract with User-Added Metadata.

4 *Aguilar v. Immigration & Customs Enforcement Div. of U.S. Dep't of Homeland Sec.*, 255 F.R.D. 350 (S.D.N.Y. 2008).

5 *Id* at 354 ("To understand why the importance of metadata varies, it is first necessary to explain what it is and distinguish among its principal forms.")

6 *Aguilar* at 354 citing *Williams v. Sprint/United Mgmt. Co.*, 230 F.R.D. 640, 646 (D.Kan 2005).

However, just as the *Sedona Principles Second Edition* and the *Sedona Glossary Third Edition,* the *Aguilar* court goes on to explain that "[a]lthough metadata often is lumped into one generic category, there are at least several distinct types, including substantive (or application) metadata, system metadata, and embedded metadata."[7]

- **Application Metadata**[8]

  "Substantive metadata, also known as *application metadata*, is 'created as a function of the application software used to create the document or file' and reflects substantive changes made by the user ... and includes data that instructs the computer how to display the fonts and spacing in a document. ... Substantive metadata is embedded in the document it describes and remains with the document when it is moved or copied."[9]

- **System Metadata (File System Metadata)**

  "System metadata 'reflects information created by the user or by the organization's information management system.'[10] ... This data ... can usually be easily retrieved from whatever operating system is in use. ... Examples of system metadata include data concerning 'the author, date and time of creation, and the date a document was modified.'"[11]

- **Embedded Metadata**

  "Embedded metadata consists of 'text, numbers, content, data, or other information that is directly or indirectly inputted into a [n]ative [f]ile by a user and which is not typically visible to the user viewing the output display' of the native file. …'[12] Examples include spreadsheet formulas, hidden columns, externally or internally linked files (such as sound files), hyperlinks, references and fields, and database information."[13]

As noted above and as expected, the discussions and significance of the different types of metadata in *Aguilar* and in the *Sedona Principles Second Edition* concern the production of metadata in the *discovery context*.

The *role* or importance of metadata for a lawyer in the *non-discovery context* is generally limited to the ethical obligations as interpreted by the ethics opinions discussed below. And there is no obvious discussion of the different types of metadata by the state bar

---

7 *Aguilar* at 354 citing *Sedona Principles Second Edition* at 60 and citing as supporting authority United States District Court for the District of Maryland, *Suggested Protocol for Discovery of Electronically Stored Information* 25-28 ("*Maryland Protocol*"). *See also* the *Sedona Glossary* at 3, 17, 19, 22, 34, 52, 53. Although the *Sedona Glossary* identifies seven different types of metadata, the court in *Aguilar* identifies the three primary types of metadata and does seem to collapse some of the seven distinct types defined in the Sedona Glossary into one of its three categories (e.g., what is defined in the *Sedona Glossary* as Email Metadata appears to be subsumed within the definition of substantive (or application) metadata in *Aguilar*).

8 Although the court in *Aguilar* uses the terminology "substantive metadata" (and expressly equates it with "application metadata"), throughout this Commentary, the more commonly used and understood terminology of "application metadata" will be used.

9 *Id* (emphasis added).

10 *Aguilar* at 354 citing *Sedona Principles Second Edition* at 60.

11 *Aguilar* at 354 citing the *Maryland Protocol* at 26.

12 *Aguilar* at 354, 355 citing the *Maryland Protocol* at 27.

13 *Id.*

associations and, specifically, the types of metadata for which *mining* is prohibited.[14] Instead, the general term *metadata* is most often used by the drafters of the *anti-mining* opinions with the unintentional consequences of arguably prohibiting the receiving party of viewing even the author (application metadata) when visible on the face of an email.[15]

A lack of precision in defining or identifying the different types of metadata may result in misunderstandings in both the analysis of a legal question and its resolution. Recognizing these distinctions in types of metadata may assist in understanding (a) the bar associations' ethical opinions in the non-discovery context, (b) how to prevent the inadvertent disclosure of confidential information in both the discovery and nondiscovery contexts, and (c) the parties' obligations to preserve and produce metadata in the discovery context.

B. Lawyer's Primary Ethical Duties Regarding Metadata

A lawyer's primary ethical duties regarding metadata may be said to fall into four subject areas: confidentiality, competence, supervision, and preservation. These duties must be considered in each of the discovery and non-discovery contexts. Of course, these duties apply in more than just the context of metadata, but they are of particular significance in that context.

1. The Duty of Confidentiality

The injunction on a lawyer's disclosure of confidential information[16] draws from the first cases protecting attorney-client communications in 16th century England to the modern right of privacy found in many constitutions,[17] with everything in between from Rule 5.2(a) of the Federal Rules of Civil Procedure ("Fed. R. Civ. P.") to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). The rule may be stated thus:

> A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly

14 Although, the Arizona State Bar in its "anti-mining" opinion states: "Except in the specific circumstances described in this opinion, a lawyer who receives an electronic communication may not examine it for the purpose of discovering the metadata *embedded in it*." Arizona State Bar Opinion 07-03: Confidentiality; Electronic Communications; Inadvertent Disclosure (Nov. 2007). It is unclear if the drafters' use of the term "embedded" is intended as a limitation on "anti-mining" to this *type* of metadata most likely to contain confidential information. Or, more likely, the use of the phrase "metadata embedded in [the electronic communication]" was considered akin to the phrase "metadata associated with [the electronic communication]" and not used as a term of art. *See also* Alabama Ethics Opinion RO-2007-02 at 2 ("The act of deliberately seeking out and viewing metadata embedded in a document is most often referred to as 'mining' the document.").

15 Metadata is generally thought to be hidden information which is not always the case, especially for certain types of metadata (e.g., application metadata for an email including author, recipients, and date), and reinforces the concept of not lumping all metadata into a single generic category. *See* Pennsylvania Bar Ass'n Comm'n on Legal Ethics and Professional Responsibility, Formal Op. 2007-500 at 2 (2007), *reconsidered* Pennsylvania Formal Op. 2009-100 (2009) ("Metadata, which means 'information about data,' is data contained within electronic materials that is not ordinarily visible to those viewing the information."); *see also* North Carolina State Bar, 2009 Formal Ethics Opinion 1, at fn. 1 (Jan. 15, 2009) (adopting Penn. Formal Op. 2007-500 definition); *but see* Barbara J. Rothstein, Ronald J. Hedges, & Elizabeth C. Wiggins, Managing Discovery of Electronic Information: A Pocket Guide for Judges 24-25 (Federal Judicial Center 2007) ("Information about a particular data set or document which describes 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 set or document.") (emphasis added).

16 "Confidential Information" as used here means information subject to a legally recognized or mandated exemption from disclosure or use. Generally, "confidential information" consists of a client confidence or secret or other information that a lawyer generally must not disclose absent authorization from the person possessing the right to withhold the information, including lawyer-client communications and information protected as work product. A lawyer may also possess other, private information from a third party protected from disclosure.

17 *See, e.g.,* California Constitution, Art 1, § 1 "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy."

> authorized in order to carry out the representation or the disclosure is permitted by [certain specific exceptions, e.g., to prevent death or substantial bodily harm].[18]

The basic rules prohibiting the disclosure of confidential information apply equally to confidential information in metadata. A lawyer must exercise reasonable care to prevent the disclosure of confidences and secrets contained in metadata transmitted to another.[19] A lawyer's duty "includes taking care ... to employ reasonably available technical means to remove [confidential] metadata before sending the file."[20]

2. The Duty of Competence

By the very nature of being a member of the bar, a lawyer must act competently in any matter the lawyer undertakes.[21]

"A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."[22] The duty of competence requires a lawyer to avoid disclosure of confidential information in metadata.[23] As Minnesota Lawyers Professional Responsibility Board said, "Competence requires that lawyers understand that:

- metadata is created in the generation of electronic files,
- transmission of electronic files will include transmission of metadata,
- recipients of the files can access metadata, and
- actions can be taken to prevent or minimize the transmission of metadata."[24]

The duty of competence means a lawyer must understand metadata (and the different types of metadata), including having sufficient knowledge for the lawyer to adhere to the lawyer's duties of confidentiality and preservation as applied to metadata.[25]

3. The Duty of Supervision

A lawyer must become knowledgeable about metadata, and a firm must provide for the acquisition of such knowledge. *ABA Model Rules of Prof'l Conduct R. 5.1*

---

18 ABA Model Rules of Prof'l Conduct R. 1.6 *Confidentiality of Information* (2009) (virtually all states have the same or similar rules regarding a lawyer's duty of confidentiality). *See also, e.g.,* California Bus. & Prof. Code § 6068(e)(1) (A lawyer has a duty "To maintain inviolate the confidence, and at every peril to himself or herself to preserve the secrets, of his or her client.")

19 *See, e.g.,* North Carolina State Bar 2009 Formal Ethics Opinion 1 (Jan. 15, 2010) ("[A] lawyer must use reasonable care to prevent the disclosure of confidential client information hidden in metadata when transmitting an electronic communication. ..."); New York State Bar Association Opinion 782 (Dec. 8, 2004) ("Lawyers must exercise reasonable care to prevent the disclosure of confidences and secrets contained in 'metadata' in documents they transmit electronically to opposing counsel or other third parties.").

20 D.C. Bar Opinion 341 (Sept. 2007). Again, appreciating the various types of metadata can aide in preventing the disclosure of confidential information—for instance, a drafter-created file title in a law firm's information management system ("system metadata") can contain confidential information (e.g., "Draft settlement agmt w/ client reqs for para 2") that may need to be "scrubbed" prior to transmission in the non-discovery context.

21 Although set forth as a separate rule by the ABA, the duty of diligence is inherent in competent representation. ABA Model Rules of Prof'l Conduct R. 1.3 Diligence (2009) ("A lawyer shall act with reasonable diligence. ...").

22 ABA Model Rules of Prof'l Conduct R. 1.1 Competence (2009).

23 *See, e.g.,* Minnesota Lawyers Professional Responsibility Board Opinion No. 22 (Mar. 26, 2010) ("[A] lawyer is ethically required to act competently to avoid improper disclosure of confidential and privileged information in metadata in electronic documents.").

24 *Id.*

25 The ABA Commission on Ethics 20/20 is proposing that the comments for the rule on competence be amended to include that "[a] lawyer should keep abreast of changes in the law and its practice, *including the benefits and risks associated with technology*. ..." ABA Commission on Ethics 20/20 Initial Draft Proposals – Technology and Confidentiality (May 2, 2011) at www.abanow.org (emphasis added).

Responsibilities of Partners, Managers, and Supervisory Lawyers (2009) require those with managerial authority to make reasonable efforts to ensure that the firm and its lawyers follow the Rules of Professional Conduct.[26] Also, the duty of supervision as articulated, for example, R. 5.1(a) may require the implementation of a firm-wide application to scrub certain outgoing email to remove metadata.[27] "[L]awyers must either acquire sufficient understanding of the software that they use or ensure that their office employs safeguards to minimize the risk of inadvertent disclosures."[28]

4. The Duty of Preservation

In contrast to the oft-required removal of metadata before transmission to another, the duty of preservation of evidence may include the obligation not to *scrub* certain *transactional* metadata.[29] A lawyer must not unlawfully alter, destroy, or conceal a file or other material having potential evidentiary value.[30] If one reasonably anticipates litigation, one must take care to prevent the routine deletion of certain metadata, especially embedded metadata in potentially relevant ESI. For example, one must not delete metadata such as tracked changes if the changes show the contract negotiations between business people if the contract is the subject of likely litigation. Such deletion may constitute spoliation. Removing metadata from certain evidentiary files may even be illegal.[31]

Preservation obligations and practices outside the context of *reasonably anticipated* litigation, however, differ considerably. "Absent a legal requirement to the contrary, organizations are not required to retain metadata. ..."[32] In fact, an earlier Sedona Commentary reminds us that to maintain the security of certain files mandated for retention, particularly those of certain regulated entities, a party may properly decide to remove some metadata.[33]

---

26 *See also* Rule 5.3(a) Responsibilities Regarding Nonlawyer Assistants: "A lawyer has a duty to supervise a law firm or department's junior members, paralegals, support staff, and any third-parties for whose work the lawyer is responsible."

27 *See also* Professional Ethics of the Florida Bar Opinion 10-2 (Sept. 24, 2010) ("A lawyer who chooses to use [d]evices that contain [s]torage [m]edia such as printers, copiers, scanners, and facsimile machines must take reasonable steps to ensure that client confidentiality is maintained and that the [d]evice is sanitized before disposition, including ... (3) supervision of nonlawyers to obtain adequate assurances that confidentiality will be maintained; and (4) responsibility for sanitization of the [d]evice by requiring meaningful assurances from the vendor at the intake of the [d]evice and confirmation or certification of the sanitization at the disposition of the [d]evice.").

28 D.C. Bar Opinion 341 (Sept. 2007).

29 *See, e.g., The Ad Hoc Committee for Electronic Discovery of the United States District Court for the District Of Delaware, Default Standard for Discovery of Electronic Documents ("E-Discovery")* (revised March 2, 2007) ("[T]he producing party must preserve the integrity of the electronic document's contents, i.e., the original formatting of the document, its metadata and, where applicable, its revision history.").

30 *See, e.g.,* ABA Model Rules of Professional Conduct, Rule 3.4(a), Fairness to Opposing Party and Counsel ("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. ...") "In a discovery or subpoena context ... a lawyer must be careful in situations where electronic documents constitute tangible evidence. Rule 3.4(a) prohibits altering, destroying or concealing material having potential evidentiary value. … [R]emoval of metadata may be prohibited. ..." West Virginia State Bar Ethics Opinion L.E.O. 2009-01 (June 10, 2009).

31 Minnesota Lawyers Professional Responsibility Board Opinion No. 22 (Mar. 26, 2010) ("Removing metadata from evidentiary documents in the context of litigation or in certain other circumstances may be impermissible or illegal.").

32 *The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age* (November 2007) at 28, *available at* https://thesedonaconference.org/download-pub/74. *See also, e.g.,* the *Minnesota Recordkeeping Metadata Standard* as an example of guidelines regarding use and preservation of metadata, including metatags.

33 "Federal law requires a variety of regulated entities to adopt policies and procedures to ensure the security of information, to protect against unauthorized access or use, and to destroy the information through special, secure methods." *The Sedona Conference® Commentary on Preservation, Management and Identification of Sources of Information that are Not Reasonably Accessible* (July 2008) at 19, *available at* https://thesedonaconference.org/download-pub/66. One business practice appropriate to some circumstances may be "[r]emoving some metadata from documents in retaining them as records or when transmitting them to others." *Id.*

II. A LAWYER'S ETHICAL OBLIGATIONS IN THE NON-DISCOVERY CONTEXT

A. Ethical Duties of a Lawyer *Sending* Metadata

A lawyer who sends metadata has the same duties of confidentiality and competence as with the sending of any other information.[34] A lawyer must use reasonable care to prevent disclosure of confidential (including *privileged*) metadata.[35]

Part of the lawyer's duty is to remove others' confidential metadata. Although the typical breach is the lawyer's failure to remove information regarding a client before transmitting it, a file may contain metadata relating to confidential information of a third party. As noted above, a lawyer's duty "includes taking care ... to employ reasonably available technical means to remove [confidential] metadata before sending the [file]. ... Accordingly, lawyers must either acquire sufficient understanding of the software that they use or ensure that their office employs safeguards to minimize the risk of inadvertent disclosures."[36]

Just as with the inadvertent disclosure of any confidential information, if a lawyer discovers he or she has inadvertently sent confidential metadata to another, the lawyer must diligently notify all those who may have received the metadata and obtain its return or destruction. Electronic information may leave the lawyer via a BlackBerry, instant messaging, etc. Due care must be taken in all circumstances.

B. Ethical Duties, Generally, of a Lawyer *Receiving* Metadata

Most jurisdictions require a lawyer who receives a file from another lawyer through inadvertence to notify the sending lawyer. The typical bar association rule mandating such notification derives from ABA Model Rules of Professional Conduct ("MRPC") Rule 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." *A fortiori*, "[i]f a lawyer receives a document which the lawyer knows or

34 To the extent one has access to a public record in electronic form, one should have access to the metadata in that record. By making the file public, the metadata perforce is made public. This was the holding in 2009 by the Arizona Supreme Court. *Lake v. City of Phoenix*, 218 P.3d 1004 (Ariz. 2009) (a "public record" in electronic format, if preserved and requested under the Arizona Public Records Act, includes the metadata). Although the State Bar of Arizona had earlier opined that a recipient may not examine a file for the purpose of discovering the metadata embedded in it. Arizona State Bar Opinion 07-03: Confidentiality; Electronic Communications; Inadvertent Disclosure (Nov. 2007) ("Except in the specific circumstances described in this opinion, a lawyer who receives an electronic communication may not examine it for the purpose of discovering the metadata embedded in it.") Presumably the principle enunciated by the Arizona Supreme Court should apply generally to metadata in public records subject to sunshine laws, the Freedom of Information Act (FOIA), and all other public-records statutes. A lawyer's duty of confidentiality means that if a lawyer submits information in electronic form to a government entity, the lawyer must ensure that any information to be redacted is done correctly and completely, again requiring the lawyer to possess a basic level of competence.

35 *See, e.g.,* North Carolina State Bar 2009 Formal Ethics Opinion 1 (Jan. 15, 2010) ("[A] lawyer must use reasonable care to prevent the disclosure of confidential client information hidden in metadata when transmitting an electronic communication . ..."); New York State Bar Association Opinion 782 (Dec. 8, 2004) ("Lawyers must exercise reasonable care to prevent the disclosure of confidences and secrets contained in 'metadata' in documents they transmit electronically to opposing counsel or other third parties.").

36 D.C. Bar Opinion 341 (Sept. 2007).

reasonably should know inadvertently contains confidential or privileged metadata; the lawyer shall promptly notify the document's sender. ..."[37]

In addition, regardless of a Rule 4.4(b), some jurisdictions require a lawyer who has received confidential materials through inadvertence not to read any more than is essential to ascertain if the materials are protected confidential information. At that point, the lawyer must notify the sending lawyer to resolve the matter.[38]

C. But see, Certain Bar Opinions Prohibit *Mining* by a Lawyer Receiving Metadata

Depending on the jurisdiction governing the receiving lawyer's conduct, different duties may apply to a lawyer who receives a file containing metadata sent by another.[39] Several bar associations' ethics opinions prohibit the receiving lawyer's viewing of any of the file's metadata (referred to as *data mining* in some of these opinions).[40] Such state ethics opinions appear to presume that metadata is *per se* confidential to its lawyer-author.[41]

37 Minnesota Lawyers Professional Responsibility Board Opinion No. 22 (March 2010). The receiving lawyer may also be prohibited from using or further distributing an inadvertently sent document/file until the matter is resolved. *See, e.g.,* ABA Model Rules of Prof'l Conduct R. 4.4(b) (2009): "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." Like Minnesota, most states have a similar rule. But, notably, California, which has been adapting its Rules of Professional conduct to be more like the ABA Model Rules of Prof'l Conduct, specifically rejected 4.4(b): "The Commission also recommends against adoption of paragraph (b) of Model Rule 4.4 and the related comments, in part, because a lawyer's duties concerning inadvertently transmitted writings often are fact-bound inquiries and therefore are difficult to specify in rule that will have disciplinary consequences. In addition, case law may continue to evolve in this area of lawyer conduct in response to variations in factual situations." State Bar Commission for the Revision of the Rules of Professional Conduct at 19 (June 26, 2010).
In its Comment to ABA Model Rule of Prof'l Conduct R. 4.4(b) (2009), the ABA notes, "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. …" ABA Model Rules of Prof'l Conduct Comments to R. 4.4(b) (2009):

> [2] Paragraph (b) recognizes that lawyers sometimes receive documents that were mistakenly sent or produced by opposing parties or their lawyers. If a lawyer knows or reasonably should know that such 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, as is the question of whether the privileged status of a document has been waived. Similarly, this Rule does not address the legal duties of a lawyer who receives a document that the lawyer knows or reasonably should know may have been wrongfully obtained by the sending person. For purposes of this Rule, "document" includes e-mail or other electronic modes of transmission subject to being read or put into readable form.
>
> [3] 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. See R. 1.2 and 1.4. (emphasis added).

If a lawyer is inclined to return a document in these circumstances, the lawyer first must consider if the lawyer's duty of diligent representation would mandate the opposite action.

38 *See, e.g., Rico v. Mitsubishi Motors Corp.,* 42 Cal. 4th 807, 68 Cal. Rptr. 3d 758 (Dec. 12, 2007) ("When a lawyer who receives materials that obviously appear to be subject to an attorney-client privilege or otherwise clearly appear to be confidential and privileged and where it is reasonably apparent that the materials were provided or made available through inadvertence, the lawyer receiving such materials should refrain from examining the materials any more than is essential to ascertain if the materials are privileged, and shall immediately notify the sender that he or she possesses material that appears to be privileged. The parties may then proceed to resolve the situation by agreement or may resort to the court for guidance with the benefit of protective orders and other judicial intervention as may be justified." (quoting *State Comp. Ins. Fund v. WPS, Inc.* (1999) 70 Cal. App. 4th 644, 656-67, 82 Cal. Rptr. 2d 799 (1999))).

39 Some ethics opinions may be binding on members of a state bar (and lawyers who practice in the state) but others are merely advisory. *See, e.g., Arizona State Bar Opinion 07-03: Confidentiality; Electronic Communications; Inadvertent Disclosure* (Nov. 2007) ("Formal opinions of the Committee on the Rules of Professional Conduct are advisory in nature only and are not binding in any disciplinary or other legal proceedings."); Ethics Opinions, State Bar of California ("These advisory opinions regarding the ethical propriety of hypothetical attorney conduct, although not binding, are often cited in the decisions of the Supreme Court, the State Bar Court Review Department and the Court of Appeal.") http://ethics.calbar.ca.gov/Ethics/Opinions.aspx (last visited Jan. 4, 2011).

40 *See, e.g.*, Alabama Ethics Opinion RO-2007-02 at 2 ("The act of deliberately seeking out and viewing metadata embedded in a document is most often referred to as 'mining' the document."). *See also* discussion above concerning the use of phrases similar to "metadata embedded in a document."

41 *See, e.g.,* New York State Bar Association, Committee on Professional Ethics, Opinion 749, *Use of Computer Software to Surreptitiously Examine and Trace E-Mail and Other Electronic Documents* (December 14, 2001) (concluding that, "[a] lawyer may not make use of computer software applications to surreptitiously 'get behind' visible documents or to trace e-mail."). *See also* Alabama State Bar Ethics Opinion RO-2007-02, *Disclosure and Mining of Metadata* (March 14, 2007) ("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."). *Id*. Of course, not all metadata is, in fact, confidential. These presumptions concerning "confidentiality *per se*" may arise from this misunderstanding of the different types of metadata and intend to only prohibit the examination of embedded metadata. The fact that all metadata is not confidential is further supported by The ABA Commission on Ethics 20/20. The Commission is proposing that the rule on inadvertent disclosure be amended to make clear that "[r]eceipt of information containing 'metadata' does not, standing alone, create a duty under this Rule." ABA Commission on Ethics 20/20 Initial Draft Proposals – Technology and Confidentiality (May 2, 2011) at www.abanow.org.

1. Few Reported Decisions

There are few reported decisions discussing whether it is ethical for a lawyer to examine the metadata in a received file. This is likely because courts do not usually deal with rules of professional conduct. (In contrast, in the context of litigation, there is a growing body of case law regarding metadata, although a court usually deals with a lawyer's conduct pursuant to the Fed. R. Civ. P., the Federal Rules of Evidence ["F.R.E."], and the inherent power of the court to govern the proceeding before it.) *In re Jessica L. Cutler, Steinbuch v. Cutler* does explicitly discuss the New York State Bar Association's ethics opinion prohibiting "data mining" of a received file's metadata.[42] *Cutler*, however, a bankruptcy matter, has a set of uncommon facts such that any comments on the New York ethics opinion are *dicta* at best.

2. Bar Associations' Ethics Opinions[43]

a) *Prohibited*

The following jurisdictions generally prohibit a lawyer from examining a received file for metadata:

- Alabama[44]
- Arizona[45]
- Florida[46]
- Maine[47]
- New Hampshire[48]
- New York[49]
- North Carolina[50]

In an early "anti-mining" opinion, the New York State Bar Association held, "A lawyer may not make use of computer software applications to surreptitiously 'get behind' visible documents or to trace e-mail."[51] An awareness of the different types of metadata (e.g., *application metadata* that instructs the computer how to display fonts) may cure this presumption of confidentiality for all metadata and could be limited to metadata more likely to contain confidential information (e.g., *embedded metadata* containing presentation notes).

b) *No Prohibition Unless the Lawyer has Actual Knowledge*

The following jurisdictions generally allow a lawyer to examine a received file for metadata *unless the receiving lawyer has actual*

42 *In re Jessica L. Cutler, Steinbuch v. Cutler*, No. 07-31459, Adv. No. 07-50064, 2009 WL 2370624 (Bankr. N.D.N.Y. June 5, 2009).
43 *See also* the ABA chart Metadata Ethics Opinions Around the U.S., www.abanet.org/tech/ltrc/fyidocs/metadatachart.html (last visited May 3, 2010).
44 Alabama State Bar Ethics Opinion RO-2007-02, *Disclosure and Mining of Metadata* (March 14, 2007).
45 Arizona State Bar Ethics Opinion 07-03, *Confidentiality; Electronic Communications; Inadvertent Disclosure* (November 2007).
46 Florida State Bar Ethics Opinion 06-2 (September 15, 2006).
47 Maine State Bar Ethics Opinion 196 (October 21, 2008).
48 New Hampshire State Bar Association Ethics Opinion 2008-2009/4, *Disclosure, Review, and Use of Metadata in Electronic Materials* (April 16, 2009).
49 New York State Bar Ethics Opinion 782, *E-mailing Documents that May Contain Hidden Data Reflecting Client Confidences and Secrets* (December 8, 2004); New York State Bar Association, Committee on Professional Ethics, Opinion 749, *Use of Computer Software to Surreptitiously Examine and Trace E-Mail and Other Electronic Documents* (December 14, 2001).
50 North Carolina State Bar 2009 Formal Ethics Opinion 1, *Review and Use of Metadata* (January 15, 2010).
51 Conclusion, New York State Bar Association Opinion 749 (Dec. 14, 2001).

knowledge that the file contains confidential metadata and should assume that the information was transmitted inadvertently.

- Colorado[52]
- District of Columbia[53]
- West Virginia[54]

The West Virginia State Bar opinion typifies many of the bar association opinions on metadata in that it appears to set inconsistent guidelines. At one point, it speaks of "actual knowledge" that "metadata was inadvertently sent." Yet, at another point, it seems to require the receiving lawyer to presume that the sending was inadvertent.

"[I]f a lawyer has received electronic documents and *has actual knowledge* that metadata was inadvertently sent, the receiving lawyer should not review the metadata before consulting with the sending lawyer to determine whether the metadata includes work-product or confidences."[55]

But ...

"The Board finds ... 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."[56]

But again ...

The federal court for the Southern District of West Virginia, sitting in diversity, held:

"[N]o West Virginia Rule or Standard of Professional Conduct requires notification to the producing party by the receiving party of the inadvertent disclosure of a privileged document."[57]

c) *No Prohibition*

The following jurisdictions generally have no prohibition on reading metadata received from another:

- Maryland[58]

52 Colorado State Bar Ethics Opinion No. 119, *Disclosure, Review, and Use of Metadata* (May 17, 2008).
53 District of Columbia Bar Ethics Opinion 341, *Review and Use of Metadata in Electronic Documents* (September 2007).
54 West Virginia State Bar Ethics Opinion LEO 200-01, *What is Metadata and Why Should Lawyers Be Cautious?* (June 10, 2009).
55 West Virginia State Bar Ethics Opinion L.E.O. 2009-01 (June 10, 2009) (emphasis added).
56 *Id.*
57 *Mt. Hawley Ins. Co. v. Felman Prod., Inc.*, No. 3:09-CV-00481, 2010 WL 1990555 (S.D. W.Va. May 5, 2010), No. CIV.A. 3:09-0481, 2010 WL 2944777 (S.D. W.Va. July 23, 2010); and *id.* at *7 ("This court has jurisdiction over this case based on diversity of citizenship. [Complaint, # 1, 7, at 2.] Pursuant to Federal Rule of Evidence 501, the privilege 'shall be determined in accordance with State law.'").
58 "Subject to any legal standards or requirements (case law, statutes, rules of procedure, administrative rules, etc.), this Committee believes that there is no ethical violation if the recipient attorney (or those working under the attorney's direction) reviews or makes use of the metadata without first ascertaining whether the sender intended to include such metadata." Maryland State Bar Association - Committee on Ethics, Ethics Docket No. 2007-09.

- Vermont[59]
- Minnesota (but it's a fact-specific question) [60]

This is also the position of the American Bar Association.[61]

d) *Case-by-Case Basis*

According to the following bar association, a lawyer must determine whether to use metadata on a case-by-case basis.

- Pennsylvania[62]

e) *Other Jurisdictions*

Even though other jurisdictions may not have weighed in on the specific question concerning metadata inadvertently sent, one should look for guidance to that jurisdiction's rules regarding a lawyer's duty on receipt of any inadvertently sent ESI. A lawyer should treat those rules as establishing a minimum duty because no jurisdiction has a more lenient rule for confidential metadata than it does for other confidential ESI.

f) *Wrinkles Throughout the Different Bar Association Opinions*

There are wrinkles in all of the opinions. One must carefully read them for the particular application to one's immediate circumstances. Consider the different takes above on what a West Virginia lawyer should do.

As noted, some opinions presume that searching for metadata is, *per se*, searching for confidential information. It is this misunderstanding of the different types of metadata that leads to the blanket prohibition on viewing any metadata, even metadata that would have no claim to confidentiality.

Other opinions appear to share this broad injunction against a lawyer who receives a file from another from searching metadata, yet a closer look at some of them reveals a possibly narrower rule: They may more precisely prohibit the lawyer from *searching for*

59 Vermont Bar Association Professional Responsibility Section Opinion 2009-1 (August 27, 2009). ("[T]here is 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 transmitted documents, is required by [Vermont Rules of Professional Conduct] VRPC 1.1 Competence, and VRPC 1.3 Diligence. ... Vermont lawyers are subject to the obligation to notify opposing counsel if they receive documents that they know or reasonably should know were inadvertently disclosed. Whether inadvertent disclosure results in waiver, ... and whether the receiving lawyer can review and use the inadvertently disclosed information, remain issues of substantive law."). *Id.* at 6.

60 "Opinion 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. Whether and when a lawyer may be advised to look or not to look for such metadata is a fact specific question beyond the scope of this Opinion." Minnesota Lawyers Professional Responsibility Board Opinion No. 22 (Mar. 26, 2010).

61 American Bar Association Formal Ethics Opinion 06-442 (August 5, 2006).

62 Pennsylvania Bar Association Committee on Legal Ethics and Professional Responsibility Formal Opinion 2009-100, *Ethical Obligations on the Transmission and Receipt of Metadata* (June 17, 2009) *superseding* Pennsylvania Bar Association Committee on Legal Ethics and Professional Responsibility Formal Opinion 2007-500, *Mining Metadata* (March 13, 2008) ("The Committee ... determined that the prior opinion provided insufficient guidance to recipients of documents containing metadata and did not provide correlative guidance to attorneys who send such documents.").

confidential information in the metadata. Consider North Carolina: A "lawyer who receives an electronic communication from another party or another party's lawyer *must refrain from searching for* and using *confidential information* found in the metadata embedded in the document."[63]

For most jurisdictions, the minimum rule of thumb is: **A lawyer may not go looking for metadata with a bad intent, i.e., to discover another's confidences.**

D. A Receiving Lawyer may have a Good Reason – or Even an Obligation – to Search for Metadata

At least one bar association has suggested that a lawyer's duties of competence and diligence *require* a search for and review of metadata included in electronically transmitted documents.[64] In addition, among other reasons, a lawyer and a law firm have a duty to protect their electronic information systems from attack by security threats such as a computer virus. By necessity, an anti-virus software application scans the metadata of all incoming (and often outgoing) messages and their attachments. A lawyer may also need to check an email's full header or a file's properties to determine the authenticity of the email or file.

III. A LAWYER'S ETHICAL DUTIES REGARDING METADATA IN THE DISCOVERY CONTEXT

A. Discovery is Different – Usually

For the sending lawyer, just as the situation in the non-discovery context, the lawyer sending/producing files containing metadata must ensure that no confidential information is disclosed to another not entitled to see it. In discovery, however, a lawyer cannot withhold whatever the lawyer chooses. In addition, privileged information withheld – if otherwise responsive – usually must be accounted for on a privilege log.

For the receiving lawyer in the context of discovery, however, the lawyer generally is allowed (and possibly mandated) to search for and examine any produced metadata. This search and examination is conducted without the presumption that such search and examination have a wrongful intent, as held in some jurisdictions' ethics opinions on metadata discussed above in the non-discovery context.

Particularly in litigation, a lawyer may be subject to obligations regarding metadata other than the Rules of Professional Conduct. Certain rules govern a matter before a tribunal regarding the right to withhold confidential information from disclosure and

63 The North Carolina State Bar, 2009 Formal Ethics Opinion 1 (Jan. 15, 2009) (emphasis added). "In summary, a lawyer may not search for and use confidential information embedded in the metadata of an electronic communication sent to him or her by another lawyer or party unless the lawyer is authorized to do so by law, rule, court order or procedure, or the consent of the other lawyer or party. If a lawyer unintentionally views metadata, the lawyer must notify the sender and may not subsequently use the information revealed without the consent of the other lawyer or party." *Id.*

64 Vermont Bar Association Professional Responsibility Section Opinion 2009-1 at 5 (August 27, 2009) ("[T]here is 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 transmitted documents, is required by VRPC 1.1 Competence, and VRPC 1.3 Diligence."). *But see* District of Columbia Bar Ethics Opinion 341, *Review and Use of Metadata in Electronic Documents* (September 2007) at fn. 9 ("In concluding that a lawyer *may* review metadata in documents produced in discovery (that is, unless and until the lawyer has actual knowledge that the metadata contains protected information), we do not intend to suggest that a lawyer *must* undertake such a review. Whether as a matter of courtesy, reciprocity, or efficiency, 'a lawyer may decline to retain or use documents that the lawyer might otherwise be entitled to use, although (depending on the significance of the documents) this might be a matter on which consultation with the client may be necessary.'") (citations omitted).

providing direction regarding a lawyer's duty to protect such information from disclosure. They also direct a lawyer's conduct if such confidential information is subsequently disclosed without authorization from the holder of the right.

B. Ethical Duties of a Lawyer for a Party *Producing* Metadata

The ethical duties of a lawyer for a party producing metadata in response to discovery or a subpoena are generally the same ethical duties of a lawyer for a party producing any other ESI. A party must produce all responsive information not subject to withholding on the basis of privilege or another consideration.[65] This includes metadata. "[M]etadata ... must be produced when requested and not objected to. However, any metadata that is privileged can still be protected and exempt from discovery, upon proper assertion of a privilege."[66] For responsive information in metadata withheld on the basis of privilege, the withholding party must provide a privilege log, i.e., the party must (i) expressly make the claim; and (ii) describe the nature of the information to the extent necessary for another to assess the claim.[67] For practical purposes, other than certain types of *embedded metadata* (e.g., tracked changes, presentation notes, or comments), there will be very little metadata for which a claim of privilege is asserted.

1. A Lawyer Must Review Metadata for Confidential Information

A lawyer has a duty to review metadata for confidential information, including information protected by the attorney-client privilege, in an otherwise nonconfidential responsive file. Whether a diligent review has occurred affects whether confidentiality or privilege claims have been waived on any inadvertently produced information.[68] Again, an understanding of the different types of metadata will assist in identifying the very limited types of metadata that could possibly contain confidential or privileged information and expediting any necessary review.[69]

When conducting this review of files and the appropriate metadata, if, by way of example, responsive yet privileged embedded metadata is part of a file, it must not be removed from the original file; but it must be redacted on a copy of the file. And, as discussed above, the producing lawyer must sufficiently detail the basis for the redaction, such as pursuant to the attorney-client privilege.

---

65 Fed. R. Civ. P. Rule 26(b)(1) Scope in General: "Unless otherwise limited by court order, the scope of discovery is as follows: Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense – including the existence, description, nature, custody, condition, and location of any documents or other tangible things and the identity and location of persons who know of any discoverable matter. For good cause, the court may order discovery of any matter relevant to the subject matter involved in the action. Relevant information need not be admissible at the trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence. All discovery is subject to the limitations imposed by Rule 26(b)(2)(C)."

66 West Virginia State Bar Ethics Opinion L.E.O. 2009-01 (June 10, 2009).

67 Fed. R. Civ. P. Rule 26(b)(5) Claiming Privilege or Protecting Trial-Preparation Materials. (A*) Information Withheld.* When a party withholds information otherwise discoverable by claiming that the information is privileged or subject to protection as trial-preparation material, the party must: (i) expressly make the claim; and (ii) describe the nature of the documents, communications, or tangible things not produced or disclosed – and do so in a manner that, without revealing information itself privileged or protected, will enable other parties to assess the claim.

68 *See, e.g., Mt. Hawley* 2010 WL 1990555 (court found defendant did not take reasonable steps to prevent inadvertent disclosure of an email and thus waived protection for it, applying Federal Rule of Evidence 502(b), considering *Victor Stanley, Inc. v. Creative Pipe, Inc.*, 250 F.R.D. 251 (D. Md. 2008) and similar cases as to reasonableness).

69 The format of production and, specifically, what fields of metadata are produced will obviously impact what metadata is reviewed for confidentiality and privilege.

2. Additional Duties of a Sending Lawyer who has Inadvertently Produced Confidential (including privileged) Metadata

If a lawyer discovers that the lawyer (party) has inadvertently produced privileged or otherwise confidential metadata to another, certain additional duties attach depending on the applicable discovery rules and rules of professional conduct. At a minimum, as part of the lawyer's duty to protect confidential information, the lawyer must request the return or destruction of the inadvertently produced confidential metadata (which usually means the return or destruction of the inadvertently produced file of which the metadata is a part).

For inadvertently produced, privileged information, this information needs to be identified on a privilege log as noted above. For inadvertently produced confidential (not privileged) information, again, depending upon the terms or existence of a protective order, the information may need to be redacted or reproduced with the appropriate legend or other *mark* identifying the information as confidential and restricted in its use.

The burden of retrieving any inadvertently-produced metadata lies squarely on the back of the producing party and its lawyer. Although not a rule of professional conduct, Federal Rule of Civil Procedure 26(b)(5)(B), "clearly places the burden of claiming privilege and notifying other parties on the party who produced the information. This burden is of course consistent with the well-settled rule that the party claiming a privilege or protection has the burden of establishing its entitlement thereto."[70]

C. Ethical Duties of a Lawyer for a Party *Receiving* Metadata

1. General

The ethical duties of a lawyer receiving metadata in response to discovery follow the same principles of the ethical duties of a lawyer who receives any other type of ESI produced in discovery or pursuant to a subpoena.

A lawyer should specify in the discovery request the form(s) in which ESI is to be produced.[71] The request is often for responsive files to be produced in native format with all metadata intact or in a reasonably useable form, which may include specified fields of metadata.[72] Thus, just as the producing party is aware of which metadata fields must be reviewed for possible future production, the receiving party should have an expectation of the types or fields of metadata that will be produced with the responsive files.

---

70 *See Mt. Hawley* 2010 WL 1990555 at *3, *citing United States v. Jones*, 696 F.2d 1069, 1072 (4th Cir. 1982).

71 The Sedona Conference® also recommends the topic, among others, be resolved at a meet and confer between the parties and their attorneys: "The anticipated form or forms of production to be sought, the need for metadata, and the form of preservation of information pending discovery." *The Sedona Conference Commentary on Preservation, Management and Identification of Sources of Information that are Not Reasonably Accessible* (July 2008) at 17, *available at* https://thesedonaconference.org/download-pub/66.

72 In *Covad Commc'n Co. v. Revonet, Inc. 267 F.R.D. 14* (D.D.C. 2010), Judge Facciola held that, because Rule 34(b)(2)(E)(ii) itself also permits production in another, usable format, the Rule contradicted plaintiff's claim that native, electronic format is absolutely obligatory. The court also relied on *The Sedona Conference, Best Practices, Recommendations, & Principles for Addressing Electronic Document Production* (2004) at i, *available at* https://thesedonaconference.org/download-pub/99. ("Unless it is material to resolving the dispute, there is no obligation to preserve and produce metadata absent agreement of the parties or order of the court.") *See also Sedona Principles Second Edition*: "Absent party agreement or court order specifying the form or forms of production, production should be made in the form or forms in which the information is ordinarily maintained or in a reasonably usable form, *taking into account the need to produce reasonably accessible metadata that will enable the receiving party to have the same ability to access, search, and display the information as the producing party* where appropriate or necessary in light of the nature of the information and the needs of the case. ... [T]he Committee Note to Rule 34(b) explicitly states that '[i]f the responding party ordinarily maintains the information it is producing in a way that makes it searchable by electronic means, the information should not be produced in a form that removes or significantly degrades this feature.' Accordingly, a party should produce electronically stored information in 'reasonably usable' forms, though not necessarily 'native format.'" *Sedona Principles Second Edition* at 60 and 63.

A lawyer must not then overlook the review of metadata requested and received in discovery. A lawyer must also have sufficient knowledge and employ the proper diligence to make sure that the received metadata is complete (unless redacted for privilege and subsequently logged) and not altered or deleted from the original in the possession, custody, or control of the producing party.

2. Duties if a Lawyer Discovers or is Notified that Metadata has Been Inadvertently Produced

Unlike a lawyer who receives metadata in the non-discovery context, a lawyer who receives metadata in response to a discovery request or pursuant to a subpoena is generally justified in assuming that the metadata was provided intentionally.

If a lawyer, however, discovers that metadata has been inadvertently produced in discovery, certain duties may attach, particularly if the lawyer is bound by a professional rule of conduct similar to ABA MRPC Rule 4.4(b) (2009), which requires notification to the sending lawyer. Similarly, of those bar associations that have opined on the issue, at least one has held that if a receiving lawyer has *actual knowledge* that metadata containing protected information was *inadvertently* sent by the sending lawyer, the receiving lawyer should advise the sending lawyer.[73] In addition, a jurisdiction may require the cessation of any further examination and notification of the sending lawyer if the received metadata is ascertained to contain confidential information.[74] Typically, rules of procedure do not impose any obligation on the receiving lawyer. For example, the Federal Rules of Civil Procedure "impose[ ] no duty on a party receiving privileged information to do anything unless and until it is notified of the claim."[75] But, "[o]nce notified of an inadvertent production of a privileged document, Rule 26(b)(5)(B) explicitly requires return, sequestration, or destruction of the document and any copies of it. ... The Rule prohibits defendants from using or disclosing the information until the claim is resolved and requires defendants to take reasonable steps to retrieve the information if defendants disclosed it before being notified of the attempted claw-back."[76]

3. Discovery is Different

Unlike metadata received outside the context of discovery, even those jurisdictions that prohibit the examination of metadata ("data mining") do not apply the prohibition generally to metadata produced in discovery. Some of the opinions use overbroad language, but a careful reading suggests the broad injunction against searching for metadata does not apply to metadata received in discovery. For example, compare the broad language of the Alabama State Bar ethics opinion prohibiting all "data mining" with its statement that, in discovery, "the mining of an email may be vital."

---

73 District of Columbia Bar Ethics Opinion 341, *Review and Use of Metadata in Electronic Documents* (September 2007) ("Notwithstanding all this, even in the context of discovery or other judicial process, if a receiving lawyer has actual knowledge that metadata containing protected information was inadvertently sent by the sending lawyer, the receiving lawyer, under Rule 8.4(c) [the analogue to ABA MRPC 4.4(c)], should advise the sending lawyer and determine whether such protected information was disclosed inadvertently. See D.C. Ethics Op. 256 ['the 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'].").

74 *See, e.g.,* [at current footnote 8] *Rico v. Mitsubishi Motors Corp.*, 42 Cal. 4th 807, 68 Cal. Rptr. 3d 758 (Dec. 13, 2007): "[A]n attorney who receives privileged documents through inadvertence ... may not read a document any more closely than is necessary to ascertain that it is privileged. Once it becomes apparent that the content is privileged, counsel must immediately notify opposing counsel and try to resolve the situation."

75 *Mt. Hawley* 2010 WL 1990555 at *3.

76 *Id.*

> "Absent express authorization from a court, it is ethically impermissible for an attorney to mine metadata from an electronic document he or she inadvertently or improperly receives from another party."[77]
>
> *But ...*
>
> One possible exception to the prohibition against the mining of metadata involves electronic discovery. ... [P]arties may be sanctioned for failing to provide metadata along with electronic discovery submissions. ... [T]he mining of an email may be vital in determining the original author, who all received a copy of the email, and when the email was viewed by the recipient. In Enron-type litigation, the mining of metadata may be a valuable tool in tracking the history of accounting decisions and financial transactions.[78]

IV. MULTIJURISDICTIONAL ISSUES

Jurisdictional conflicts have been a significant issue since the founding of these United States. This Commentary addresses only jurisdictional conflicts regarding metadata. Furthermore, those conflicts can be narrowed to those in which a lawyer receives metadata in the *non-discovery context*. As discussed above, this last circumstance is the one in which a conflict may arise because some jurisdictions limit accessing metadata by the receiving lawyer's.

Most jurisdictions' rules of professional conduct have a choice-of-law rule similar to ABA MRPC Rule 8.5:

> b) Choice of Law. In any exercise of the disciplinary authority of this jurisdiction, the rules of professional conduct to be applied shall be as follows:
>
> (1) For conduct in connection with a matter pending before a tribunal, the rules of the jurisdiction in which the tribunal sits, unless the rules of the tribunal provide otherwise; and
>
> (2) For any other conduct, the rules of the jurisdiction in which the lawyer's conduct occurred; or, if the predominant effect of the conduct is in a different jurisdiction, the rules of that jurisdiction shall be applied to the conduct. A lawyer shall not be subject to discipline if the lawyer's conduct conforms to the rules of a jurisdiction in which the lawyer reasonably believes the predominant effect of the lawyer's conduct will occur.

Multijurisdictional practice, and, hence, jurisdictional conflicts, may be more common in the context of litigation. For litigated matters, the choice-of-law rule in most jurisdictions is direct: The applicable rules "for conduct in connection with a matter pending before a tribunal" are the rules of the jurisdiction in which the tribunal sits. Regarding metadata produced and received in the discovery context, even the restrictive bar association opinions generally presume a lawyer may examine all such metadata.[79] Indeed, the applicable rules of professional conduct may mandate such an examination.

77 Alabama State Bar Ethics Opinion RO-2007-02 (March 14, 2007).
78 *Id.*
79 *But also see* n.7 above.

But even for metadata transmitted in the non-discovery context in a matter before a tribunal, determining which jurisdiction's rule applies to a lawyer who is a member of another bar association is simple: the rules of the jurisdiction in which the tribunal sits. To the extent a jurisdiction limits the examination of metadata by the receiving party, the rule that counts is the one in which the tribunal sits. Hence, if Arizona would prohibit such examination and Colorado would otherwise permit it, if the matter is being heard in Phoenix, both Arizona and Colorado lawyers must follow Arizona Ethics Rules in such a matter.

The restrictive *anti-mining* opinions, however, are written primarily with *non-litigation* (i.e., a matter that is not before a tribunal) in mind.

A. The Ethical Dilemma in the *Non-litigation Context*[80]

Lawyers subject to the ethical rules of different jurisdictions may be subject to different ethical obligations concerning the receipt of metadata in the *non-discovery and the non-litigation contexts*. For instance, when a lawyer is admitted to practice law in multiple jurisdictions, his or her ethical obligations may conflict, as they do in Arizona and Colorado. In Arizona, a lawyer is prohibited from examining an electronic communication in the non-discovery context for the purpose of discovering its metadata.[81] In Colorado, a lawyer "generally may ethically search for and review metadata embedded in an electronic document that the receiving lawyer receives from opposing counsel or other third party."[82] If a lawyer is licensed in both Arizona and Colorado, the question arises as to which ethical obligation the lawyer must follow when involved in a matter that is not before a tribunal (i.e., non-litigation context). MRPC Rule 8.5(b) requires the lawyer to follow the ethical rule of the jurisdiction in which the lawyer is conducting business, or the jurisdiction which receives the "predominant effect" of the conduct.

B. Are Other Ethical Duties Implicated?

In instances when it is not particularly clear which jurisdiction receives the "predominant effect" of the conduct, one approach in trying to reconcile this conflict is to follow the ethical requirements of the most restrictive state (that is, the lawyer essentially contracts away his or her "right to mine" in a particular state). In other words, the lawyer is guided by the most restrictive ethics of the two states - e.g., Arizona where mining is prohibited. The lawyer would be assured he or she is not violating state bar ethical requirements concerning "mining" of metadata.

But if there is no prohibition on accessing and reviewing metadata in a jurisdiction in which the lawyer practices, there is a question as to whether the lawyer would be obligated to review metadata to fulfill the lawyer's duty of competency.

C. Best Practices

Best practices suggest that a lawyer anticipate any potential problems or conflicts with jurisdictional rules concerning metadata and resolve them before an issue arises. This can be accomplished by mutual agreements (protective orders or non-waiver agreements) as

---

80 Discussed throughout this Commentary is the distinction between the discovery (information produced in response to a discovery request or subpoena) and non-discovery contexts. This is the only instance in which it is necessary to draw an even further distinction, e.g. (a) in front of a tribunal or (b) in a "non-litigation context."

81 State Bar of Arizona Ethics Committee Opinion, 07-03.

82 Colorado Bar Association Ethics Committee Opinion 119.

to metadata – namely, agree that breach of the agreement (which should be embodied in a court order) would violate MPRC R. 8.4. An agreement on how metadata will be handled reduces the potential for allegations that the way in which a lawyer handled metadata was surreptitious and is less likely to be objectionable on an ethical level. However, in any conflict situation, the court should be notified of the conflict, its nature, and the lawyers' proposed solution.

V. MITIGATION

A. Metadata: Out of Sight, Out of Mind

Too often awareness of metadata follows the old saying: Out of sight, out of mind. And therein lies the risk of malpractice and sanctions.

Certain types of metadata (e.g., embedded metadata) may migrate to new files because of the frequent reuse of prior work-product, potentially carrying with it certain confidential information without any cognizance by the new user. For example; Kate creates a licensing agreement for What-Zit, and Cleo copies it to use as a template for licensing Hot-Now. Embedded in Kate's file are tracked changes containing confidential information, of which Cleo may not be aware when she sends her draft to a different client.[83] Although, as in our example, a lawyer who sends or produces a file may be oblivious to the embedded metadata, the recipient may easily be able to access and view it. It may even appear as the recipient opens the file. Sometimes this is fine, and other times it is unfortunate. In any event, a lawyer should always be aware of all the information he or she sends to another.[84]

B. Practical Tips

Please note that these tips relate only to the sending of information containing metadata in the non-discovery context and are certainly not exhaustive as technology continues to evolve and the quantity of metadata continues to increase.

1. Scrubbing

The easiest way to prevent disclosure of confidential information in metadata is the installation and implementation of metadata scrubbing software.[85] However, scrubbing may constitute spoliation if a legal duty exists to preserve the data that is being scrubbed.[86]

Another practical tip for preventing the disclosure of confidential information in metadata is to scrub the metadata during the conversion to .pdf. A .pdf will have its own metadata, but it is limited to the author who created the .pdf and the date/time the document was converted to .pdf. The .pdf will not contain the original word processing software metadata.

---

83 In addition, the "profile" of the user attached to the "new" document may be that of the creator of the "original." For example, certain metadata fields in Cleo's document may have information from the same metadata fields in Kate's document, for example, Kate may still appear as the author.

84 Businessman Derrick Max, reacting to Democrats' outrage when his e-mailed Congressional testimony revealed input from the Republican Social Security Administration, vented that, "The real scandal here is that after 15 years of using Microsoft Word, I don't know how to turn off 'track changes.'" Zeller, Tom, Jr., *Beware Your Trail of Digital Fingerprints*, N.Y. Times (Nov. 7, 2005).

85 *See also* n.34 above.

86 An alternative is to copy the document to a new file and scrub the new file before transmitting to a third party (which will, most likely, create a new document that also must be preserved).

Scanning a document is another way to avoid inadvertent disclosure of confidential metadata. Scanning a document to .pdf or .tiff eliminates metadata as well unless the metadata is displayed when the document is scanned. However, users often find that converting to .pdf from their desktop is faster and easier, so the safest solution may be some form of scrubbing.[87]

2. Track Changes

If using *Track Changes* in documents, proper acceptance and rejection will eliminate disclosure of confidential metadata, which the recipient could otherwise view. The user should always check to ensure that there are no tracked changes that need to be accepted or rejected.[88]

Another practical tip when using Track Changes is to avoid hiding the *Track Changes* from view by choosing: Review tab from the Ribbon, select the Tracking group; select the pull-down menu that begins with Final: Show Markup; choose Final. (Microsoft Office's Word 2010).

Again, scanning a document to .pdf or .tiff eliminates tracked changes unless tracked changes are displayed when the document is scanned.

3. Electronic Redactions

Also, beware of electronic redactions because electronic redactions may simply be overlays, exposing the *hidden* to search, copy, and paste.

Although some word processing software has electronic redaction tools, it is typically safest to print the document containing the confidential text, black out the confidential text and scan the document before sending it electronically.

4. Agreements and Orders

Other practical tips for avoiding the disclosure of metadata include agreements – confidentiality or non-disclosure agreements, stipulated protective orders, and non-waiver agreements. Such agreements are applicable to document productions in the discovery context and could also be used in the non-discovery context if specified.

VI. CONCLUSION

Electronic communications between lawyers are now standard practice, and the duty of a lawyer to maintain confidences in the transmission of ESI requires consideration of technical and legal questions. What is metadata? What metadata is or should be included in these communications? What are the ethical constraints imposed on the lawyer by the jurisdiction that licensed the lawyer and, for that matter, other jurisdictions where he or she may practice? This Commentary introduces metadata in the context of the duties and obligations lawyers now face on a daily basis and opens the dialogue on ethics and metadata.

87 Some useful scrubbing information is available at http://blogs.adobe.com/acrobat/2010/08/scrubbing-metadata-%E2%80%93-practice-and-policy-2.html and http://www.workshare.com.

88 Documents should also be checked for comments, hidden columns, or other information that the user could embed within the document.