Comment,
WHY INVISIBLE ELECTRONIC DATA IS RELEVANT IN TODAY'S LEGAL ARENA

I. Introduction

While sitting at your office computer, you begin drafting a settlement proposal for a client going through a divorce utilizing your standard word processor. You type up a rough draft and send it to your client asking for any comments or questions she may have. Your client makes a few comments regarding your proposed split of the marital assets suggesting that she likes the proposal, but really just wants the process to end as quickly and painlessly as possible. Your client makes a comment within the document stating she would be willing to settle for a smaller percentage of the marital property if the process becomes too time consuming and litigious. Your client saves these comments in the word processor and sends the document back to you. You make any relevant changes to the proposal in the word processor, delete your client's comment, review the document, save it, and email it to the opposing counsel. Right after the document is sent, you start feeling a little anxious. All of a sudden you remember overhearing another attorney discussing a type of data that is automatically stored within the word processor that allows a user to track any changes or edits and view prior versions of the electronic document. Can the opposing counsel somehow uncover the comment your client made regarding the proposal? Should you have been more careful in sending the electronic document? Was there something you should have done differently before you emailed the electronic document to opposing counsel? Is it possible you violated attorney-client confidentiality without even realizing it?

Numerous situations occur such as this one, in which an attorney submits documents containing metadata to clients, coworkers, or even opposing counsel that can raise such questions. For the most part, the metadata contained in these documents does not provide any usable information to anyone looking at the

data, or reveal any confidential information.[1] However, the metadata contained in some documents can reveal very sensitive and confidential information, the disclosure of which may be detrimental or embarrassing to the client or lawyer.[2] Metadata may reveal information protected by the attorney-client privilege or work product doctrine which can give a party an advantage in contract drafting, negotiations, or other practice settings.[3] Receiving attorneys with the know-how have the ability to search within a document they receive electronically and reveal its metadata.[4] The transfer of metadata contained within attorney created files raises some ethical concerns: what duty does an attorney owe his client when sending documents containing metadata through electronic means; may the recipient ethically review the metadata; and must the recipient notify the sender if metadata is found?[5]

Outside the scope of confidentiality, metadata can be very helpful, especially in formal discovery during litigation. For example, it can reveal when a document was created and by whom, authenticating the document, or it can facilitate more effective and efficient searching and retrieval of electronic information.[6] However, regardless of metadata's foundation, it may not always be admitted as evidence,[7] thus wasting its usefulness. It is important in today's technological era for attorneys to understand how to request the production of metadata, how to determine what forms electronic information are most usable, and how courts have generally handled requests for the production of metadata.

---

1 N.Y. State Bar Ass'n Comm. on Professional Ethics, Formal Op. 782, Dec. 8, 2004.

2 *Id*.

3 Philip J. Favro, *A New Frontier in Electronic Discovery: Preserving and Obtaining Metadata*, 13 B.U. J. SCI. & TECH. L. 1, 12 (2007).

4 *See infra* pp. 5-7; *see also* Favro, *supra* note 3, at 7-10.

5 *See* Elizabeth W. King, *The Ethics of Mining for Metadata Outside of Formal Discovery*, 113 PENN ST. L. REV. 801, 816-828 (2009); AMERICAN BAR ASSOCIATION, LEGAL TECHNOLOGY RESOURCE CENTER, METADATA ETHICS OPINIONS AROUND THE U.S., *available at* http://www.abanet.org/tech/ltrc/fyidocs/metadatachart.html. The ABA created a well-organized table summarizing the ABA's ethical opinion on metadata and a summary of each state that has issued an opinion on metadata focusing on the three major issues discussed in this article surrounding the ethical treatment of the transmission of metadata.

6 *See infra* pp. 6-7.

7 *See infra* p. 15 and notes 85-87.

First, this Note will define metadata and describe the different types that affect the legal field. Next, the Note will briefly summarize the ethical issues that arise regarding the transmission of metadata. Finally, this Note addresses the discoverability of metadata focusing on its evidentiary value, the process of requesting metadata, and how courts have handled production requests in the past. Given the developing significance of metadata, it is imperative for attorneys to understand what metadata is and how it can affect one's work as a lawyer.

II. What Is Metadata?

Metadata is defined generally as "data hidden in documents that is generated during the course of creating and editing such documents. It may include fragments of data from files that were previously deleted, overwritten or worked on simultaneously."[8] Because metadata describes the "history, tracking, or management of an electronic document,"[9] it is often called "data about data."[10] Aside from technical definitions, what metadata actually does is record information about the document or file automatically to assist in storing and retrieving the document or file at a later date.[11] Basically, it is the information you or your computer records when you edit, open, or create an electronic document to

---

8 NYSBA, Formal Op. 782.

9 Williams v. Sprint/United Mgmt. Co., 230 F.R.D. 640, 646 (D. Kan. 2005).

10 *Id.*; *see The Sedona Principles-Second Edition: Best Practices Recommendations and Principles for Addressing Electronic Document Production* Cmt. 12a (Sedona Conference Working Group Series 2007), *available at* http://www.thesedonaconference.org/content/miscFiles/TSC_PRINCP_2nd_ed_607.pdf [hereinafter *Sedona Principles 2d*]. "The Sedona Conference [is] a nonprofit legal policy research and education organization[. It is] comprised of judges, attorneys, and electronic discovery experts [who focus on] resolving electronic document [ ]issues." Aguilar v. Immigration & Customs Enforcement Div of U.S. Dep't of Homeland Sec., 255 F.R.D. 350, 355 (S.D.N.Y. 2008). The Conference has published numerous documents, including the Sedona Principles, which focus on the production of electronically stored information as evidence. Many courts have held the Sedona Principles to be persuasive authority with respect to electronic discovery. *See, e.g.*, *Id.*; Kentucky Speedway, LLC v. Nat'l Ass'n of Stock Car Auto Racing, Inc. et al., No. 05-138-WOB, 2006 WL 5097354 (E.D. Ky. 2006).

11 *Sedona Principles 2d*, *supra* note 10, at 3.

help the computer understand what the document is and process the information more efficient.

Metadata is created in two principal ways. First, the software being used by the originator of the file creates it automatically.[12] Second, the attorneys working on documents create metadata as they develop, edit, and manipulate the electronic documents.[13] Both types of metadata can be very relevant to a case.

The more interactive the application, such as a database like Microsoft Access, the more important metadata is for the computer or user to understand the information recorded by the application.[14] Thus, metadata is often considered critical for a user or computer to understand a database application, although it adds little benefit to understanding a word processing document.[15] A spreadsheet application, depending on the complexity of the information stored in it, probably falls somewhere in the middle of a word processor and database regarding the necessity of metadata to understand the application.[16]

Aguilar v. Immigration[17] explained that documents contain three basic types of metadata: substantive (or application) metadata, system metadata, and embedded metadata.[18] Substantive metadata is often the type that gives attorneys the most anxiety. When attorneys imagine sending a document through email and mistakenly revealing confidential information within the stored metadata, they are thinking about substantive metadata. Substantive metadata records and reflects any changes to a document made by the user or creator of a document.[19] Though it includes a lot of irrelevant information, substantive metadata can reveal important and confidential information, such as any prior edits made by the creator-attorney.[20] Substantive metadata is

12 King, *supra* note 5, at 805.

13 *Id*.

14 *Williams*, 230 F.R.D. at 647.

15 *Id*.

16 *Aguilar*, 255 F.R.D. at 354.

17 *Id*. at 354-355.

18 *See also*, *Sedona Principles 2d*, *supra* note 10, at 4.

19 *Id*.

20 *Id*.

automatically linked with the document and travels with it anytime it is sent electronically.[21]

The most commonly found substantive metadata in word processing documents includes the date the document was created by the user, any revisions, the dates when the revisions occurred, the text that was revised, and any tracked changes or comments made within the document.[22] The "track changes" function is often considered the most relevant information stored by metadata.[23] The "track changes" function, as many attorneys are aware, shows any alterations made to previous drafts of a document and the identities of the users who made the changes.[24] This feature is valuable in that it allows attorneys and their clients to "view and understand the evolution of a document."[25] Though the "tracked changes" are deleted on the viewable surface of a document, the "tracked changes" are often still stored within the substantive metadata. This information can be transmitted electronically with the document if it is not removed and reveal secret information to other parties—thus possibly violating attorney-client confidentiality.

The second type of metadata, system metadata, contains the information that explains a file or document to the user's operating system created automatically by that operating system or the application.[26] Some examples include "the author, date and time of creation, and the date a document was modified."[27] Many courts have held that "most system [ ] metadata lacks evidentiary value because it is [simply] not relevant."[28] However, courts

---

21 *Id*.

22 Favro, *supra* note 3, at 7; *see also*, *Sedona Principles 2d*, *supra* note 10, at 3; NYSBA, Formal Op. 782.

23 Favro, *supra* note 3, at 7.

24 *Id*.

25 *Id*.

26 *Sedona Principles 2d*, *supra* note 10, at 60; *see also Aguilar*, 255 F.R.D. at 354.

27 *Aguilar*, 255 F.R.D. at 354 (*quoting* United States District Court for the District of Maryland, *Suggested Protocol for Discovery of Electronically Stored Information* 25-28, *available at* http://www.mdd.uscourts.gov/news/news/ESI Protocol.pdf).

28 *Aguilar*, 255 F.R.D. at 354, (*citing* Mich. First Credit Union v. Cumis Ins. Soc'y, Inc., No. 05-74423, 2007 WL 4098213, at *2 (E.D. Mich. Nov.16, 2007)); *see Kentucy Speedway*, 2006 WL 5097354, at *8; Wyeth v. Impax Labs., Inc., 248 F.R.D. 169, 170 (D. Del. 2006)).

have determined that "[s]ystem metadata is relevant[ ] if the authenticity of a document is questioned[,] or if establishing who received"[29] a document and when is important to a claim brought in court.[30] System metadata helps authentication because the information regarding the identity of the author and the date and time of creation, etc., is created automatically by the user's application or operating system, which is hard to manipulate manually. Thus, system metadata can potentially provide an objective means of authenticating many electronic documents.

Embedded metadata consists of formulas, linked files, or hyperlinks, etc., that are generally stored in database programs or spreadsheets.[31] The user creates embedded metadata by inputting formulas within spreadsheets or creating queries within databases, or many times the application fills in formulas automatically creating embedded metadata. Spreadsheet and database output often contain calculations, query formulas, or hidden columns that are not visible in printed versions and can only be accessed within the "native"[32] applications.[33] Because of this, embedded metadata is often essential to understand certain electronic documents. For example, spreadsheet output may be difficult to understand without the ability to view the formulas underlying the printed output.[34] Also, hidden embedded metadata may be required to search very large databases in an efficient manner. Embedded metadata is often the subject of formal discovery to better understand complex spreadsheets or databases that are relevant to a claim.

---

29 *Aguilar*, 255 F.R.D. at 354.

30 *See id.* Hagenbuch v. 3B6 Sistemi Elettronici Industriali S.R.L., No. 04 C 3109, 2006 WL 665005, at *3 (N.D. Ill. Mar. 8, 2006).

31 *Aguilar*, 255 F.R.D. at 355.

32 "Native" format files are files unchanged and read using the software that used to create them. *What Does That Mean? A Supplemental Glossary of Modern Tech Terms*, 25 No. 2 LAW. PC 5 (Oct. 15, 2007). Certain spreadsheet or database rendered files are practically unusable when produced in a printed version, making the production of files in their "native" format a necessity to understand the information in many circumstances. H. Christopher Boehning & Daniel J. Toal, *Ruling Gives Guidance on Native Production*, NEW L.J. (Dec. 23, 2009), *available at* http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202437219532.

33 *Sedona Principles 2d*, *supra* note 10, at 4.

34 *Aguilar*, 255 F.R.D. at 355.

The next section of this article will focus on attorney created metadata (most often substantive metadata) and the ethical issues that can arise when confidential information contained in the metadata is viewable to those not privileged by the attorney-client relationship.

III. Metadata's Effects on Attorney-Client Confidentiality

Three common issues arise when attorneys transmit documents or files containing attorney created metadata electronically: the sender's duty when transmitting metadata; whether the recipient may review the metadata; and whether the recipient must notify the sender if metadata is found. A handful of states[35] and the ABA have issued ethical opinions regarding these issues.[36]

A. *What Is the Sender's Duty When Transmitting Metadata?*

The ABA Standing Committee on Ethics and Professional Responsibility opined that there is no explicit duty an attorney must follow when electronically transmitting documents contain-

---

35 Ala. State Bar Office of Gen. Counsel, Formal Op. 2007-02, Mar. 14, 2007, *available at* http://www.alabar.org/ogc/PDF/2007-02.pdf; Az. State Bar of Az. Ethics Comm., Ethics Op. 07-03, Nov. 2007, *available at* http://www.myazbar.org/Ethics/opinionview.cfm?id=695; Colo. Bar Ass'n Ethics Comm., Ethics Op. 119, May 17, 2008, *available at* http://www.cobar.org/index.cfm/ID/386/subID/23789/CETH//; Professional Ethics of the Fl. Bar, Op. 06-2, Sept. 15, 2006, *available at* http://www.floridabar.org/tfb/tfbetopin.nsf/SearchView/ETHICS,+OPINION+06-2?opendocument; Me. Bd. of Overseers of the Bar Prof'l Ethics Comm'n, Op. 196, Oct. 21, 2008, *available at* http://www.maine.gov/tools/whatsnew/index.php?topic=mebar_overseers_ethics_opinions&id=63337&v=article; Md. State Bar Ass'n Comm. on Ethics, Ethics Docket No. 2007-09; N.H. Bar Ass'n Ethics Comm., Op. 2008-2009/4, *available at* http://www.nhbar.org/uploads/pdf/EthicsOpinion2008-9-4.pdf; NYSBA, Formal Op. 782; Pa. Bar Ass'n – Comm. on Legal Ethics and Prof'l Responsibility, Formal Op. 2009-100; Vt. Bar Ass'n Prof'l Responsibility Section, Ethics Op. 2009-1, *available at* http://69.39.146.6/Upload%20Files/WebPages/Attorney%20Resources/aeopinions/Advisory%20Ethics%20Opinions/Electronic%20Documents/09-01.pdf; D.C. Bar – Legal Ethics Comm., D.C. Op. 341, Sept. 2007, *available at* http://www.dcbar.org/for_lawyers/ethics/legal_ethics/opinions/opinion341.cfm; W.V. Bar Ass'n, Lawyer Disciplinary Bd., L.E.O. 2009-01; *available at* http://www.wvodc.org/pdf/lei/LEI%2009-01.pdf.

36 *See* METADATA ETHICS OPINIONS AROUND THE U.S., *supra* note 5.

ing metadata. The ABA has merely suggested a number of ways to eliminate metadata for those who are "concerned about the possibility of sending, producing, or providing to opposing counsel a document that contains or might contain metadata."[37]

Every state that has issued a formal opinion on this issue has held that the sender has a duty of reasonable care.[38] The sender has "an ethical duty to use reasonable care when transmitting electronic documents to ensure that he or she does not disclose his or her client's secrets and confidences."[39] Although not all of the opinions formally state that attorneys are charged with a duty to understand the foreseeable consequences of transmitting metadata, this conclusion can be inferred from most of the opinions.[40] Not only is the attorney charged with the duty of reasonable care and knowledge, but some state opinions actually hold the attorney to a duty to understand and employ means to remove metadata from the documents or files that are sent electronically.[41] The implied, yet key duty seems to be knowledge. Because of this, all attorneys should take the time to understand metadata and the potentially confidential information electronic documents can disclose if not handled properly. This would arm an attorney with the knowledge to take the reasonable steps necessary to avoid implicating any ethical issues.

B. *May the Recipient of the Document Ethically Review What the Metadata Discloses?*

The ABA held that the receiving attorney may review the metadata; however, the state opinions are somewhat split. The ABA focused on MRP Rule 4.4(b) holding that the attorney's sole requirement is to notify the sender that he or she received

---

37 *Id*. (*quoting* ABA Standing Comm. on Ethics and Prof'l Responsibility, Formal Op. 06-442 The ABA suggests scrubbing, negotiating a confidentiality agreement, or sending the file in different formats that don't transmit metadata.)

38 *Id*.

39 Ala., Formal Op. 2007-02.

40 *See* Ala., Formal Op. 2007-02; Colo., Ethics Op. 119; Me., Op. 196; N.H., Op. 2008-2009/4; NYSBA, Formal Op. 782, Dec. 8, 2004; Pa., Formal Op. 2009-100; D.C., Op. 341, Sept. 2007; W.V., L.E.O. 2009-01.

41 Me., Op. 196; Pa., Formal Op. 2009-100; D.C., Op. 341; W.V., L.E.O. 2009-01.

information inadvertently.[42] The ABA determined that there were no further restrictions upon the receiving attorney's conduct.[43]

Eight states[44] have determined that the receiving attorney has an ethical duty *not* to review the information. They stated that a strong public policy exists against an attorney engaging in conduct that would amount to an unjustified intrusion into the opposing counsel's attorney-client relationship.[45] Additionally, Alabama stated that the discovery and review 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."[46] Washington D.C. and West Virginia added a caveat to this general rule. Their opinions state that this rule would hold only if the recipient had actual knowledge that the metadata was sent inadvertently.[47]

Colorado, Maryland, and Vermont have determined that recipients could review the metadata unless the sender notified the recipient of the inadvertent transmission before the document was opened and reviewed.[48] As long as the recipients were not notified of an inadvertent transmission, they would not violate an ethical duty if they reviewed and used the metadata contained in the document or file.[49] According to Pennsylvania's opinion, each instance must be decided on a case-by-case basis, giving deference to the attorney's discretion based on their duties to their client. A receiving lawyer in Pennsylvania "(a) must [ ] determine whether he or she may use the data received as a matter of substantive law; (b) must consider the potential effect on the client's matter[ ]; and (c) should advise and consult with the client

---

42 ABA Standing Comm. on Ethics and Prof'l Responsibility, Formal Op. 05-437.

43 *Id.*

44 Alabama, Arizona, Florida, Maine, New Hampshire, New York, Washington D.C., and West Virginia.

45 *See* METADATA ETHICS OPINIONS AROUND THE U.S., *supra* note 5.

46 Ala., Formal Op. 2007-02.

47 D.C., Op. 341; W.V., L.E.O. 2009-01.

48 Colo., Ethics Op. 119; Md., Ethics Docket No. 2007-09; Vt., Ethics Op. 2009-1.

49 *Id.*

about the appropriate course of action under the circumstances."[50]

C. *Must the Recipient Notify the Sender if Metadata Is Found?*

The ABA opinion says that if lawyers know or reasonably should know that the transmission was inadvertent, they must notify the sender.[51] Of the ten states that addressed this question in their formal opinions, all but Maryland stated that the recipient must notify the sender of an inadvertent transmission.[52] If a recipient "discovers metadata by any means, and knows or reasonably should know that the sender did not intend to transmit the information, the recipient has a duty to [promptly notify the sender]."[53] West Virginia determined that it is always safest to notify the sender before searching an electronic document whether or not the recipient has actual knowledge of inadvertently sent metadata.[54] Maryland never adopted Rule 4.4(b); therefore, in that state there is no actual duty to notify.[55] However, Maryland observed that it would be wise to communicate the pros and cons with his or her client and work together to decide how best to act under the circumstances.[56]

Given the developing significance of metadata in today's legal arena, a substantial need exists for attorneys to understand what metadata is and know how it can affect their client's interests.[57] Though not every lawyer can be an expert on all aspects of metadata, the duty of reasonableness under the circumstances is appropriate to protect attorney-client confidentiality. A lawyer should be charged with an active duty to stay current on technological advances in document transmission to best understand the potential risks and best methods of transmitting information to opposing parties. Initiating a set of standard protocol, such as always copying and pasting documents into plain text editors, us-

50 Pa., Formal Op. 2009-100; *see also* King, *supra* note 5, at 825-28.

51 ABA, Formal Op. 05-437. Based on MRP Rule 4.4(b), as stated above.

52 *See* METADATA ETHICS OPINIONS AROUND THE U.S., *supra* note 5.

53 Az., Ethics Op. 07-03. Thus, following RPC 4.4(b) procedures.

54 W.V., L.E.O. 2009-01.

55 Md., Ethics Docket No. 2007-09; *see also* METADATA ETHICS OPINIONS AROUND THE U.S., *supra* note 5; King, *supra* note 5, at 822.

56 Md., Ethics Docket No. 2007-09; *see also* METADATA ETHICS OPINIONS AROUND THE U.S.

57 Favro, *supra* note 3, at 6.

ing manufacturers' add-in metadata removal procedures, or utilizing third party software that removes metadata, to be followed each time information is transmitted electronically to opposing counsel would significantly reduce the possibility of either side from crossing any ethical boundaries.

IV. The Discovery of Metadata in Formal Litigation

A. *Court Admission of Metadata as Evidence*

Courts are generally "skeptical about admitting metadata as evidence."[58] This is probably due to the fact that the courts are unfamiliar with metadata and how they should deal with it. Despite this judicial skepticism, metadata may have significant evidentiary value. "Sometimes [it] is needed to authenticate a disputed document [(often using system metadata),] or to establish facts material to a dispute."[59] If used properly in litigation, metadata can provide a substantial benefit by "facilitating more effective and efficient searching and retrieval of electronically stored information."[60] Furthermore, the 2006 amendments to Rule 34 of the Federal Rules of Civil Procedure have included express changes regarding electronically stored information (ESI), which includes metadata.[61] "Rule 34 was expressly drafted to recognize that electronic data is subject to discovery."[62] Commentators have argued that this reveals an inherent acceptance by the FRCP drafters of metadata's importance in the legal profession.[63]

The discovery of metadata is subject to the balancing test of Federal Rule of Civil Procedure 26(b)(2)(C), which "requires a court to weigh the probative value of proposed discovery against its potential burden."[64] According to Gretchen Harris in her article entitled *Metadata: High-Tech Invisible Ink Legal Considera-*

---

58 Thomas R. McLEan, *EMR Metadata Uses and E-Discovery*, 18 ANNALS HEALTH L. 75, 79 (2009).

59 *Sedona Principles 2d*, *supra* note 10, at 4.

60 *Id*.

61 *See* Favro, *supra* note 3, at 6.

62 *Id*. at 19.

63 *See generally Id*.

64 *Aguilar*, 255 F.R.D. at 355.

tions,[65] courts generally weigh three criteria in favor of ordering metadata discoverable. First, the stronger the possibility the metadata will be admissible or lead to the admissibility of other information, the more likely it will be relevant and found to be discoverable.[66] Next, courts will consider the time and financial burden of producing metadata.[67] If the probative value of the metadata outweighs the time and financial burden placed on the producing party, the more likely it will be discoverable.[68] Finally, the more useful the electronic evidence is in interpreting, searching, or retrieving ESI, the more likely it will be discoverable.[69] This factor is especially relevant when parties are requesting very voluminous amounts of electronic evidence. Without the embedded metadata intact, large electronic files may be practically unsearchable, thus, unusable.[70] Therefore, metadata will be considered discoverable "if it is relevant to the claim or defense of any party,"[71] and its production will not violate attorney-client privilege.[72]

B. *The Process of Requesting Metadata Production Through Discovery*

The Sedona Principles and the Federal Rules of Civil Procedure emphasize that due to the ever-changing nature of electronic discovery, requesting metadata production should optimally be a party-driven process.[73] Federal Rule of Civil Procedure 26(f) requires the parties to meet together and confer to develop a discovery plan prior to their initial conference with the court.[74] During a Rule 26(f) conference, parties should formu-

---

65 Gretchen J. Harris, *Metadata: High-Tech Invisible Ink Legal Considerations*, 78 MISS. L.J. 939 (2009).

66 *Id*. at 954.

67 *Id*.

68 *Id*.

69 *Id*; *see Sedona Principles 2d*, *supra* note 10, at 60. Embedded metadata may be key to interpreting complex spreadsheets or database output if they are deemed relevant to a case.

70 *Harris*, *supra* note 65, at 954.

71 *Aguilar*, 255 F.R.D. at 355.

72 *Id.* (citing FED. R. CIV. P. 26(b)(1)).

73 *Sedona Principles 2d*, *supra* note 10, at 63; FED. R. CIV. P. 34(b); FED. R. CIV. P. 26(f).

74 FED. R. CIV. P. 26(f); Boehning & Toal, *supra* note 32.

late a discovery plan that "states the parties' views and proposals on . . . any issues about [the] disclosure or discovery of electronically stored information, *including the form or forms in which it should be produced*."[75] The commentary to Rule 26(f) notes that the issue of whether metadata should be produced is a topic that should be discussed in a Rule 26(f) conference.[76]

Parties should work together in good faith to identify relevant and discoverable ESI, the scope of the discoverable ESI that should be preserved by the sending party, and the formats of the ESI that would be most efficient to work with.[77] When choosing the form of ESI production, the Sedona Principles recommends that the parties bear in mind two primary considerations: "(1) the need for, or probative value of, both [visible data] and metadata; and (2) the extent to which the production of metadata will enhance the functional utility of the electronic information produced [allowing] the parties to conduct a more cost effective and efficient review."[78] If parties keep the lines of communication open when developing a discovery program during a Rule 26(f) conference and work together constructively to formulate what electronic data is relevant and should be produced, it is likely they will not run in to court denials of ESI production requests during discovery.

After a Rule 26(f) conference, Federal Rule of Civil Procedure 34(b) allows the requesting party to specify the particular form of the electronic document or file to be produced.[79] The responding party must then either produce the ESI in the form specified, or object to the discovery request.[80] If the responding party objects, or the party seeking production did not specify a form of production, the responding party must state the form of

---

75 Boehning & Toal, supra note 32 (citing FED. R. CIV. P. 26(f)(C)(3) (emphasis added)).

76 *See Kentucky Speedway, LLC*, 2006 WL 5097354, at *8; *see generally* Scotts Co. LLC v. Liberty Mut. Ins. Co., No. 2:06-CV-899, 2007 WL 1723509 (S.D. Ohio June 12, 2007).

77 SEVENTH CIRCUIT ELECTRONIC DISCOVERY PILOT PROGRAM, STATEMENT OF PURPOSE AND PREPARATION OF PRINCIPLES, Phase One Oct. 1, 2009 – May 1, 2010, 12 (Oct. 1, 2009).

78 *Sedona Principles 2d*, *supra* note 10, at 62.

79 *Aguilar*, 255 F.R.D. at 355. Metadata can be specifically requested for production under Federal Rule of Civil Procedure 34(b).

80 Favro, *supra* note 3, at 19.

ESI it plans to produce for the requesting party.[81] If, as just stated, the requesting party does not specify a form for production, the responding "party must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms."[82] A "reasonably usable" form depends on the circumstances of the case; something best determined by both parties during a Rule 26(f) conference.[83] If no party agreement or court order exists to define what is "reasonably usable," the producing party should take into account the need to produce metadata that is accessible enough to allow the receiving party to access, search, and display the necessary information based on the needs of the case.[84] Generally, absent a party agreement or court order, the responding party cannot produce metadata in a form that makes the documents difficult to review.[85] After parties complete this process, if the requesting party further objects and seeks an alternative form, the parties "must meet and confer under [FRCP] Rule 37(a)(2)(B) in an effort to resolve the matter before the requesting party can file a motion to compel [production]."[86]

If a party requests the production of metadata in the initial discovery request, courts generally have ordered production as long as the producing party has not yet produced the documents in another form,[87] and the request is relevant and reasonable.[88] However, because this process is rather complicated, and be-

---

81 *Id*; FED. R. CIV. P. 34(b)(2)(D)).

82 FED. R. CIV. P. 34(b)(2)(E)(ii); *see Sedona Principles 2d*, *supra* note 10, at 65.

83 *Sedona Principles 2d*, *supra* note 10, at 65.

84 *Id*.

85 Favro, *supra* note 3, at 19.

86 FED. R. CIV. P. 34(b), Advisory Committee's Note, 2006 Amendment.

87 *See In re Payment Card Interchange Fee & Merch, Disc*., No. MD 05-1720(JG)(JO), 2007 WL 121426, at *4 (E.D.N.Y. Jan. 12, 2007) (ordering the production of metadata for any documents not yet produced); *Hagenbuch*, 2006 WL 665005, at *4 (granting motion to compel the production of requested documents in native form); In re Verisign, Inc. Securities Litigation, No. C 02-02270 JW, 2004 WL 2445243, at *2-3 (N.D. Cal. Mar. 10, 2004) (ordering the production of metadata to sustain searchability of the electronic version).

88 *See Mich. First Credit Union*, No. 05-74423, 2007 WL 4098213, at *2-3 (E.D. Mich. Nov. 16, 2007) (denying production of metadata despite a timely request because it was (1) not relevant and (2) production would be unduly burdensome).

cause metadata is such a new variable that has been thrown into the mix of discovery requests, many requesting parties fail to initially request the production of metadata. If a requesting party does not seek metadata initially, courts tend to deny later requests, especially if the producing party has already produced the documents in an alternative form.[89]

Often parties will refuse to produce documents with discoverable metadata intact based on the valid argument that the information is privileged as part of attorney-client confidentiality. When a party refuses production of otherwise discoverable metadata, Federal Rule of Civil Procedure 26(b)(5) requires a party to describe the nature of data not produced that will enable the other party to assess the applicability of privilege without revealing the privileged information. If a party fails to produce this record of reasons for withholding the otherwise discoverable information, courts will often hold that the party has waived any attorney-client privilege and order the production of metadata.[90]

When the discovery of metadata during formal litigation is at issue, the Sedona Principles suggest the producing party to consider the relevant risks of inadvertent production of confidential, privileged, and work product information associated with the different forms of production, whether the production of data in forms other than their native format will provide sufficient usability and functionality, and the relative costs and burdens associated with the proposed forms of production.[91] The requesting party should take the time to understand the relevant information it is seeking through the production requests.[92] This "will require a thorough understanding of the key issues in the litigation and the degree to which metadata will be useful in exploring

---

89 *See Ky. Speedway*, 2006 WL 5097354, at *8 (denying motion to compel the production of metadata because the request came seven months after the initial request and plaintiff showed no particularized need for the metadata); *Wyeth*, 248 F.R.D. at 171 (deciding parties never agreed on any particular format, therefore documents produced in TIFF format were sufficient); *but see Williams*, 230 F.R.D. at 654 (holding when a party is ordered to produce documents as maintained in the ordinary course of business, the producing party should produce the documents with their metadata intact).

90 *Williams*, 230 F.R.D. at 653-654.

91 *Sedona Principles 2d*, *supra* note 10, at 63.

92 Boehning & Toal, *supra* note 32.

them."[93] By and large, working collaboratively with opposing counsel throughout the discovery process will help ensure that both parties understand what is being requested and how best to supplement the requests. This will help alleviate the many headaches caused by the discovery process. Furthermore, if both parties are on the same page with their formal requests for metadata, courts will be more likely to grant the requests.

V. Conclusion

It is essential for the twenty-first century attorney to understand what metadata is and how it can affect the representation of his or her clients. It would be most advantageous for an attorney to understand the types of metadata, and how they are created. When sending information electronically during the day-to-day representation of a client, attorneys should be charged with the duty to take reasonable steps to ensure confidential information is not inadvertently transmitted to opposing counsel. Additionally, if any confidential information is inadvertently received, the receiving attorney should communicate with his or her client, address any ethical issues raised by the situation, alert the sending attorney, and proceed cautiously so as not to implicate any ethical issues. Finally, attorneys should utilize a standard set of procedures to ensure that electronically transmitted documents are cleaned of confidential metadata, thus avoiding any inadvertent transmission of unwanted information, which would help eliminate any problems before they occur.

Because the electronic discovery of metadata is becoming common in court, both parties should always consider the discovery and production of metadata and its relevance to formal litigation. In some instances, metadata will have significant evidentiary value. It may help interpret, search and retrieve, and authenticate relevant information. Parties should determine whether metadata would be necessary to understand the information they intend to request. The process of requesting the production of metadata may be considered complicated due to the legal profession's lack of knowledge surrounding metadata. Some courts may require formal requests for metadata and some may consider the request implied. It is best practice to confer

93 *Id.*

with opposing counsel prior to submitting to court a formal discovery request.[94] Both parties should work together when forming their discovery requests to ensure they are on the same page with what they are requesting. This will help streamline the discovery process and further protect the transfer of functional and usable electronically stored information.

Though metadata is often considered a complicated and misunderstood facet of the electronic legal arena, its prevalence in understanding electronically stored information should keep metadata at the forefront of many attorneys' ethical and electronic discovery considerations.

Mathew Robertson

[94] *See Kentucky Speedway, LLC*, 2006 WL 5097354, at *8; *Scotts Co. LLC*, 2007 WL 1723509, at *4.