Washington University Jurisprudence Review

Volume 7 | Issue 1

2014

Bringing Guns to a Gun Fight: Why the Adversarial System is Best Served by a Policy Compelling Attorneys to Ethically Mine for Metadata

Justin Fong

BRINGING GUNS TO A GUN FIGHT: WHY THE ADVERSARIAL SYSTEM IS BEST SERVED BY A POLICY COMPELLING ATTORNEYS TO ETHICALLY MINE FOR METADATA

JUSTIN FONG[*]

> "'Well, in our country,' said Alice, still panting a little, 'you'd generally get to somewhere else—if you run very fast for a long time, as we've been doing.'
>
> 'A slow sort of country!' said the Queen. 'Now, here, you see, it takes all the running you can do, to keep in the same place. If you want to get somewhere else, you must run at least twice as fast as that!'"
>
> —Lewis Carroll's Through the Looking-Glass[1]

I. INTRODUCTION

The American legal system is an adversarial system. Like trial by combat, it is rooted in the ideal that justice and truth will be found in the wake of battle. In place of seasoned soldiers and knights, however, are two lawyers, brandishing wit instead of metal, to win the heart and mind of the court to each lawyer's interpretation of the case. While created hundreds of years ago, this system still applies to this day. The world today, however, is much different from the world when the adversarial system was first established. Today's world is one of unprecedented innovation and technological progress. In the last fifty years communication has advanced from weeklong letters to instant video conversations, and from behemoth computers to powerful devices that fit in our pockets.

In their expansive utilitarian nature, these technological advances have entwined themselves into the legal field as well. No longer must case briefs be written by hand or discovery be limited to paper form. These

---

* J.D./M.B.A. Candidate (2016), Washington University in St. Louis; B.A. (2011), International Studies Economics, University of California, San Diego. I would like to thank my family, friends, and loved ones for support not only in writing this Note, but also in all my life endeavors. Without their love and support, none of this would have been possible. Also I would like to thank the the Jurisprudence Review Editorial Staff for their dedication and patience in ensuring the quality of this Note.

1. LEWIS CARROLL, THROUGH THE LOOKING-GLASS ch. II (Project Gutenberg, Millenium Fulcrum ed. 1.7 2013) (1871), http://www.gutenberg.org/files/12/12-h/12-h.htm.

developments, however, are not gratis. With each technological innovation affecting the field of law, attorneys' standards for competence and diligence have been amplified.[2] Specifically, in the field of discovery, questions have arisen regarding lawyers' duties and metadata mining. Metadata is "data about data,"[3] and can be found in documents, emails, and essentially any other electronically stored information ("ESI").[4] Mining, on the other hand, refers to a lawyer's ability to cull through ESI to find relevant evidence.[5] Metadata's significance spurs from its ability to reveal everything from changes made to the document to who the author is, or even when the author last accessed the document.[6] More importantly, a lawyer's ability to use metadata more effectively than opposing counsel may just be the crucial difference between incrimination and exculpation; it could be described as bringing a gun to a knife fight.

This Note aims to demonstrate that lawyers should have a duty to mine metadata in the adversarial system. Part II will introduce the adversarial process and explain the intricacies of metadata. Part III will argue that in the adversarial system, attorneys should be compelled to mine for metadata. Part III.a will demonstrate that metadata is part of a document and that metadata is valuable as evidence. Part III.b will continue by illustrating that the ban of mining metadata is misplaced, for the burden lies on the transmitting attorney to protect confidential information. Further, due to metadata's importance and the ability to ethically mine for metadata, the receiving attorney has a duty to mine metadata under Rules 1.1 and 1.3 of the Model Rules of Professional Conduct.[7] Part III.c will show that while arguments against metadata mining—it is costly and may reveal privileged information—are not unfounded, they are regressive and overly broad. Finally, Part IV will reveal that due to the value of metadata and the policy implications of denying metadata mining, the adversarial system is best served by creating a policy compelling lawyers to mine metadata.

---

2. *See* Crystal Thorpe, Note, *Metadata: The Dangers of Metadata Compel Issuing Ethical Duties to "Scrub" And Prohibit the "Mining" of Metadata*, 84 N.D. L. REV. 257 (2008) (citing Maureen Cahill, Presentation at the Alexander Campbell King Law Library, University of Georgia School of Law: The Internet: Complicating Legal ethics, but Full of Resources to Help You Understand the Complications 4 (Mar. 7, 2007), *available at* http://digitalcommons.law.uga.edu/cgi/viewcontent.cgi?article=1036&context=speeches (noting how Model Rules 1.1, 1.3, and 1.6 relate to metadata concerns).

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

4. *Id.* at 652.

5. *See id.*

6. *See id.*

7. *See* MODEL RULES OF PROF'L CONDUCT R. 1.1, 1.3 (2013).

II. BACKGROUND OF THE ADVERSARIAL SYSTEM AND METADATA

A. The Adversarial System

The basis of the adversarial system is that "truth with respect to a disputed matter is more likely to emerge before an impartial fact finder and justice more likely to be rendered if *each* litigant presents his own case and version of the facts in the light most favorable to him."[8]

The adversarial system is rooted in the concept of giving litigants the fairest opportunity to present their story, adhering to the notion that everyone deserves an opportunity to be heard.[9] The adversarial system thus seeks to implement two values.[10] First, it seeks to directly serve litigants by allowing them a voice in the legal process.[11] Second, and more importantly, the adversarial system "helps assure that the parties will be motivated to place before the court the strongest proofs and arguments they can muster. The effect of two-sided presentations is to expand the information available to the court to an extent far beyond the amount the court could have acquired through its own investigation."[12] As Lord Eldon observed, "Truth is best discovered by powerful statements on both sides of the question."[13]

B. Metadata

Metadata is "data about data" and generally describes the "history, tracking, or management of an electronic document."[14] While typically not

---

8. William G. Young, John R. Pollets & Christopher Poreda, *Operation of the Adversary System—Purpose of the Law of Evidence*, 19 MASS. PRACTICE: EVIDENCE § 102.1 (2d ed. 2008).

9. JOHN THIBAUT & LAURENS WALKER, PROCEDURAL JUSTICE: A PSYCHOLOGICAL ANALYSIS 38–39, 68 (1975). *See also* Stephen Landsman, *The Decline of the Adversary System: How the Rhetoric of Swift and Certain Justice Has Affected Adjudication in American Courts*, 29 BUFF. L. REV. 487, 526 (1980).

10. Young, Pollets & Poreda, *supra* note 8.

11. *Id.*

12. *Id.*

13. *Ex parte* Elsee, (1830) 1 MONTAGU & BLIGH 69, 70 n.(a) (quoting *Ex parte* Lloyd (Nov. 5, 1822) (unreported)). *See also* Irving Kaufman, *Does the Judge Have a Right to Qualified Counsel?*, 61 A.B.A. J. 569 (1975)."Adversary system" is defined in law as the "network of laws, rules and procedures characterized by opposing parties who contend against each other for a result favorable to themselves." BLACK'S LAW DICTIONARY 49 (5th ed. 1979). *See also* "adversary" in WEBSTER'S THIRD NEW INT'L DICTIONARY: OF THE ENGLISH LANGUAGE UNABRIDGED 31 (1961) ("[T]he Anglo-American system of procedure for conducting trials under strict rules of evidence with the right of cross-examination and argument, one party with his witnesses striving to prove the facts essential to his case and the other party striving to disprove those facts or to establish an affirmative defense").

14. *Williams*, *supra* note 3, at 646 (internal quotation marks omitted).

difficult to find, metadata is "usually not apparent to the reader viewing a hard copy or a screen image."[15]

One source courts may rely on for guidance on addressing metadata is *The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age*. In Appendix F, metadata is defined as "information about a particular data set which describes how, when and by whom it was collected, created, accessed or modified and how it is formatted (including data demographics such as size, location, storage requirements and media information)."[16] Additionally, Appendix E further defines metadata to include "all the contextual, processing, and use information needed to identify and certify the scope, authenticity, and integrity of active or archival electronic information or records."[17]

There are three types of metadata—substantive, system, and embedded metadata.[18] "Substantive metadata, also known as *application metadata* is created as a function of the application software used to create the document or file . . . ."[19] Examples of substantive metadata include prior edits, editorial comments, and word processing data.[20] Additionally, this type of metadata can track the revision history of a document, such as the "Track Changes" feature does in Word.[21]

System metadata "reflects information intentionally created by the user or by the organization's information management system."[22] System metadata consists of the author, the date and time of creation, and the date a document was modified.[23] System metadata is extremely relevant if the authenticity of a document becomes an issue or if establishing, "among

15. FED. R. CIV. P. 26(f) advisory committee's note.

16. The Sedona Conference, *The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age* 94 (Sept. 2005), *available at* https://the sedonaconference.org/publication/Managing%20Information%20%2526%20Records (click September 2005 link, enter requested information).

17. *Id.* at 80.

18. The Sedona Conference, *Commentary on Ethics and Metadata* 2 (March 2012), *available at* https://thesedonaconference.org/publication/The%20Sedona%20Conference%C2%AE%20Commentary%20on%20Ethics%20%2526%20Metadata (click March 2012 link, enter requested information).

19. *Id.* (citation omitted).

20. *Id.*

21. *See* MICROSOFT, *Track Changes While You Edit*, SUPPORT.OFFICE.COM, https://support.office.com/en-US/Article/Track-changes-while-you-edit-024158a3-7e62-4f05-8bb7-dc3ecf0295c4 (last visited Oct. 22, 2014).

22. The Sedona Conference, *The Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Production* 46 cmt. 12.a (July 2005), *available at* https://thesedonaconference.org/publication/The%20Sedona%20Principles (click July 2005 link, enter requested information).

23. *See id.*

other things, who received what information and when[]" is important to the claims or defenses of a party.[24] While it does not appear in the onscreen or printed version of a document, like substantive metadata may, system metadata can be accessed relatively easily by simply checking the properties of a document.

Embedded metadata includes "text, numbers, content, data, or other information that is directly or indirectly inputted into a native file by a user and which is not typically visible to the user viewing the output display of the native file."[25] Examples of embedded metadata "include spreadsheet formulas, hidden columns, externally or internally linked files (such as sound files), hyperlinks, references and fields, and database information."[26] Similar to substantive metadata, embedded metadata can appear on screen, in printed form, or can be hidden completely. [27]

III. LAWYERS SHOULD BE COMPELLED TO MINE FOR METADATA

Lawyers should be compelled to mine for metadata for several reasons. First, metadata is part of a document and can be extremely valuable to a lawyer in its ability to authenticate documents or provide formulas. Second, the duties of a lawyer under the Model Rules and the majority of bar associations suggest that the burden of safe-guarding metadata lies with the transmitting lawyer under Rule 1.6, not with the receiving lawyer.[28] The receiving lawyer has a duty to mine for non-confidential information under Rules 1.1 and 1.3.[29] Finally, arguments against mining data—such as it is too costly or is protected information—are regressive, for compelling metadata mining can actually reduce costs, and the arguments are overly broad, for not all metadata is protected information. Because the Model Rules and the majority of bar associations contend that the burden of removing privileged information should be on the transmitting attorney, and because the arguments against mining metadata are unpersuasive, lawyers ought to have a duty to mine metadata.

---

24. *See* Hagenbuch v. 3B6 Sistemi Electtronici Industriali S.R.L., No. 04 C 3109, 2006 U.S. Dist. LEXIS 10838, at *10 (N.D. Ill. Mar. 8, 2006).

25. Aguilar v. Immigration and Customs Enforc. Div. of U.S. Dep't of Homeland Sec., 255 F.R.D. 350, 354–55 (S.D.N.Y. 2008) (internal quotation marks omitted). *See also* Lake v. City of Phoenix, 222 Ariz. 547, 550 n.5 (Ariz. 2009).

26. *Aguilar*, *supra* note 25, at 355.

27. *See id.*

28. *See* MODEL RULES OF PROF'L CONDUCT R. 1.6 (2013).

29. *See* MODEL RULES OF PROF'L CONDUCT R. 1.1, 1.3 (2013).

A. Metadata is Part of the Document and is an Invaluable Source of Evidence

Metadata serves a legitimate use in the legal field. Some argue that mining for metadata is similar to searching for something removed from the document, like "looking through [someone's] briefcase when she steps out of the room."[30] However, this statement is grossly inaccurate, for metadata mining "is simply the process of examining the entirety of an electronic document," and "is thus unlike briefcase snooping, where a lawyer has every reason to believe and expect that her briefcase is free from snooping eyes."[31] Additionally, metadata can be very useful as it can offer "a range of intellectual access points for an increasingly diverse range of users . . . " such as providing a transactional lawyer with information regarding who edited a company memorandum about its financial status or future sales projections.[32] Due to metadata's integral role in documents and potential importance in evidence, lawyers should be compelled to mine for it.

1. Metadata is Part of the Document

Courts mandating documents to be produced in native form with metadata included indicates metadata's integral role in documents. Under Federal Rule of Civil Procedure 34(b)(2)(E)(ii), in the course of discovery, if no form is specified for producing ESI, the responding party "must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form . . . ."[33] In *Aguilar v. Immigration and Customs Enforc. Div. of U.S. Dep't of Homeland Sec.,* the court stated that "if the ESI is kept in an electronically-searchable form, it 'should not be produced in a form that removes or significantly degrades this feature.'" [34] The court further noted that the specific guidelines in discovery advocate for documents to be produced in their native format.[35] "Native format"

30. *See* Andrew M. Perlman, *The Legal Ethics of Metadata Mining*, 43 AKRON L. REV. 785, 794 (2010).

31. *Id.*

32. Anne J. Gilliland, *Setting the Stage*, *in* INTRODUCTION TO METADATA 1, 6 (Murtha Baca ed., 2d ed. 2008).

33. FED. R. CIV. P. 34(b)(2)(E)(ii).

34. *Aguilar*, *supra* note 25, at 355 (quoting FED. R. CIV. P. 34(b) advisory committee's note, 2006 amendment); *see also 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) (documents stripped of metadata allowing searches do not comply with Rule 34(b)).

35. *Id.*

refers to the original format of a document or the format produced by the program, such as .doc for Word or .ppt for PowerPoint, which includes all forms of metadata.[36] This indicates that some courts consider metadata an integral part of a document.

Furthermore, some courts have specifically stated that metadata is part of the document. In *Lake v. City of Phoenix*, the court found that metadata should be treated as part of the document itself, as opposed to separate information from the initial record.[37] In *Lake*, the plaintiff requested public records to utilize as evidence that he was demoted for whistleblowing after reporting his supervisor's misconduct.[38] The plaintiff specifically sought notes documenting supervisory performance, as well as the accompanying system metadata ("true creation" date, access dates for each time the file was accessed, including who accessed the file as well as print dates, etc.) for fear that the files were backdated, but was denied by the defendant.[39]

In response, the Arizona Supreme Court unanimously held that metadata in an electronic document is part of the underlying document and that it "forms part of the document as much as the words on the page."[40] The court reasoned that:

> It would be illogical [to conclude that parties] can withhold information embedded in an electronic document, such as the date of creation, while they would be required to produce the same information if it were written manually on a paper public record.[41]

Through court findings such as the one in *Lake*, metadata can be considered part of a document and should be scrutinized as such by lawyers.

2. Metadata is Important

Metadata is an invaluable source of evidence and can be utilized in multiple areas of the law.[42] System metadata can certify "the authenticity

36. *Aguilar*, *supra* note 25, at 353 n.4.
37. *Lake*, *supra* note 25.
38. *Id.*
39. *Id.*
40. *Id.* at 550.
41. *Id.* at 551.
42. The Sedona Conference Working Group on Electronic Document Retention and Production Sedona, AZ, *The (2004) Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Production*, THE SEDONA CONFERENCE JOURNAL 2004, 151, 192 cmt. 12.a (2004).

and degree of completeness of the content"[43] of objects and "provide some of the information an information professional might have provided in a physical reference or research setting."[44] Embedded metadata "establishes and documents the context of the content . . ." and "identifies and exploits the structural relationships that exist between and within information objects . . . ."[45]

Through these multiple uses, courts have come to recognize metadata's importance. In *Williams v. Sprint*, the plaintiff requested Excel documents to analyze whether age was a factor in terminating his employment.[46] After two years, the defendant produced the documents in TIFF format, which the plaintiff complained was insufficient because the data and formulas, embedded metadata, were inaccessible.[47] Consequently, the court ordered the defendant to produce the files in their native format, which the defendant did only after scrubbing the file names, dates of modifications, history of revisions, and printout dates as well as locking the cells (i.e., erasing the system and embedded metadata).[48] The defendants argued that this information was irrelevant.[49] The court found the defendant's argument inadequate.[50] In a watershed decision, the court favored the plaintiff's right to disclosure, finding that metadata can be "the key to showing the relationships between the data; without such metadata, the tables of data would have little meaning."[51] Accordingly, metadata is clearly an important part of a document and lawyers should thus be compelled to mine it.

B. Model Rules and the Majority of Bar Associations Suggest A Lawyer Has A Duty to Mine for Metadata

While not difficult to access, the path to mining metadata is not a smooth road. The main roadblock that prevents mining metadata stems from ethical concerns, specifically ABA Model Rule of Professional Conduct section 4.4(b). Under the ABA Model Rules, section 4.4(b) states "a lawyer who receives a document relating to the representation of the

43. Gilliland, *supra* note 32, at 6.
44. *Id.* at 3.
45. *Id.*
46. *See Williams*, *supra* note 3, at 641.
47. *Id.* at 643.
48. *Id*. at 641.
49. *Id.* at 644.
50. *Id.*
51. *Id.* at 647.

lawyer's client and knows or reasonably should know that the document was inadvertently sent shall promptly notify the sender."[52] While acknowledging that the sender must be notified, this Model Rule, however, does not comment on whether the receiving lawyer should "refrain from looking at the document . . . ."[53] ABA Model Rule 1.6 suggests that the ethical focus of mining for metadata should be placed on the sending lawyer, as it is not difficult to erase metadata, and the sending lawyer is in the best position to prevent confidential information from being sent.[54] Additionally, a receiving lawyer's only affirmative duties in regard to metadata can be seen as limited to ABA Model Rule 1.1 and 1.3, duties to diligently and competently represent his or her clients.[55] Furthermore, multiple bar associations have found that lawyers can and should ethically mine for metadata.[56] Accordingly, the ABA Model Rules and bar association interpretations of ethical rules suggest that lawyers should be compelled to mine metadata.

1. Adherence to the Model Rules by Sending Lawyers Would Preclude Ethical Violations by Receiving Lawyers

Through the Model Rules, an ethical focus on the receiving lawyer of a document with metadata is misplaced. A majority of the burden should lie with the sending lawyer instead of receiving lawyer because it is not difficult to prevent the information from being released, and placing the burden on the sender is the most efficient method of dealing with any ethical dilemma of mining metadata.

Under the ABA Model Rules, section 1.6 states that a "lawyer shall not reveal information relating to the representation of a client."[57] Comment 4 states that this "prohibition also applies to disclosures by a lawyer that do not in themselves reveal protected information but could reasonably lead to the discovery of such information by a third person."[58] Furthermore,

52. ELLEN J. BENNETT, ELIZABETH COHEN & MARTIN WHITTAKER, ANNOTATED MODEL RULES OF PROFESSIONAL CONDUCT 427 (7th ed. 2011).

53. David Hricik, *Mining for Embedded Data: Is It Ethical to Take Intentional Advantage of Other People's Failures?*, 8 N.C. J. L. & Tech. 231, 237 (2007).

54. MODEL RULES OF PROF'L CONDUCT R. 1.6 (2013).

55. MODEL RULES OF PROF'L CONDUCT R. 1.1, 1.3 (2013).

56. ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 442 at 3 (2006); Md. St. Bar Ass'n Comm. on Ethics, Ethics Docket 09 (2007); Wash. St. Bar Ass'n. Op. 2216 (2012); Vt. State Bar Ass'n Ethics Op. 01 (2009); D.C. Bar Legal Ethics Comm., D.C. Op. 341 (2007); Colo. Bar Ass'n Ethics Comm., Op. 119 (2007); W. Va. Bar Ass'n, Lawyer Disciplinary Bd., L.E.O. 01 (2009); Or. State Bar Ass'n Ethics Op. 2011-187.

57. BENNETT, COHEN & WHITAKER, *supra* note 52, at 92.

58. MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 4 (2013).

comment 19 states that "[w]hen transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients."[59]

Living in the Information Age, lawyers should not have difficulty learning how to protect metadata. Information is freely available about this subject with companies like Microsoft who offer support information for scrubbing metadata from their documents.[60] In addition, bar associations, including those in Oklahoma and California, hold seminars that teach lawyers how to scrub metadata.[61] With the availability of metadata scrubbers and the number of continuing legal education programs on the subject of ESI, the inclusion of metadata in ESI should be viewed less and less as an understandable error and more as simply lackadaisical lawyering.[62] Given that metadata can be obtained with relative ease and the abundance of information on how to scrub metadata, the ethical burdens of metadata should be placed on the sending attorney.

While this position may seem a bit draconian in regards to placing such a heavy burden on the sender, it is the most efficient. [63] If the sender carries out his or her duty to guard confidential information from being disclosed, the question of the ethics of mining metadata would be nonexistent. The only information that would be released would be information that the sender had intended to be released. As a result, the action of mining for the metadata would not be subject to claims under the ethics rules, attempting to frame metadata mining as dishonest, for confidential metadata would not be present. Accordingly, the ethical burden should be placed on the sending attorneys, for if they complied with their duties, no ethical issues would be present and attorneys could freely mine for metadata.

---

59. MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 19 (2013).

60. *See* J. Craig Williams, *The Importance of Deleting Metadata . . . And How to Do it*, 49 ORANGE COUNTY LAWYER 48 (2007).

61. *Id.*

62. *See* Perlman, *supra* note 30, at 792 ("a transactional lawyer who receives electronic documents as part of due diligence may have a legitimate interest in knowing who edited a company's memorandum . . . because it is simply a business document . . . there is no reason to conclude that it is confidential or otherwise protected.").

63. *See* Cal. Comm. On Prof'l Responsibility & Conduct, Ethics Op. 2010-179 (2010) (because of the "ever-evolving nature of technology" and differences in security features, lawyers must "ensure the steps are sufficient for each form of technology being used and must continue to monitor the efficacy of such steps.").

2. Model Rules Illustrate That A Receiving Lawyer's Only Ethical Obligations In Regard to Metadata Are To Diligently Represent Their Clients

Under the ABA Model Rules, the only affirmative duties that the receiving lawyer has are enumerated under sections 4.4(b), 1.1, and 1.3. Under 4.4(b) the receiving lawyer only has to notify the opposing lawyer that he or she has received information that he or she reasonably believes to be inadvertently sent.[64] Comment 3 also states "[w]here a lawyer is not required by applicable law to do so, the decision to voluntarily return such a document or delete electronically stored information is a matter of professional judgment ordinarily reserved to the lawyer[,]" not an ethical obligation.[65]

While a receiving lawyer may not have an ethical obligation to return the document under the Model Rules, a receiving lawyer does have the duty to act competently and diligently. Under the Model rules, section 1.1 states a "lawyer shall provide competent representation to a client."[66] Competent representation includes "inquiry into and analysis of the factual and legal elements of the problem, and use of methods and procedures meeting the standards of competent practitioners."[67] A lawyer in providing competent representation must investigate all relevant facts, which would include metadata. Comment 5 further explicates that the "required attention and preparation are determined in part by what is at stake; major litigation and complex transactions ordinarily require more extensive treatment than matters of lesser complexity and consequence."[68] Under the Model Rules, section 1.3 states "a lawyer shall act with reasonable diligence in representing a client."[69] Modern diligence should include a working knowledge of information architecture, compelling lawyers to understand the concept of metadata.

Under Model Rules 1.1 and 1.3, a receiving lawyer has a duty to mine for metadata. In *People v. Boyle*, a lawyer was found in violation of 1.1 by failing to prepare adequately for a hearing by failing to discover readily

64. MODEL RULES OF PROF'L CONDUCT R. 4.4(b) (2013).

65. MODEL RULES OF PROF'L CONDUCT R. 4.4 cmt. 3 (2013); ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 05-437 (2005) (lawyer's only ethical obligation under Rule 4.4(b) is to promptly notify sender).

66. MODEL RULES OF PROF'L CONDUCT R. 1.1 (2013).

67. MODEL RULES OF PROF'L CONDUCT R. 1.1 cmt. 5 (2013).

68. *Id.*

69. MODEL RULES OF PROF'L CONDUCT R. 1.3 (2013).

available evidence supporting an asylum petition.[70] Similarly, a lawyer failing to mine metadata can be found to have failed to discover readily available evidence and to be in violation of 1.1, for if a document is provided in its native format, metadata in ESI is readily available. System metadata is easily accessible, simply by checking the properties of a file on a computer. Embedded metadata is visible in formulas and application metadata, such as tracked changes, and is easily found. As previously noted, metadata is important and can be the pivotal difference in determining a conviction, or even an asylum grant. Accordingly, competent representation would require an attorney to mine metadata.

Similarly, in *In re Ungar*, a lawyer was found in violation of 1.3 for failing to investigate all the terms of an aggregate settlement negotiated by co-counsel so that his clients could decide whether to accept the agreement.[71] Mining metadata is arguably similar to investigating the terms of a settlement. In investigating the terms of a settlement, a lawyer is expected to both be able to comprehend the terms and to be able to locate which are truly important.[72] Mining metadata requires similar diligence and knowledge. Combined with the duty to guard information of one's client, the obligation of a lawyer to diligently represent one's client supports placing an affirmative duty to mine for data on the attorney.

3. The Majority of Bar Associations Condone or Actually Compel Metadata Mining

A main argument against the mining of metadata is that the act is dishonest or fraudulent. Several bar associations, including Alabama, Arizona, Florida, Maine, and New Hampshire, have opted to prohibit the mining of metadata.[73] Opponents of metadata mining look to section 8.4 of the ABA Model Rules. Section 8.4(c) states, "it is professional misconduct for a lawyer to . . . engage in conduct involving dishonesty, fraud, deceit or misrepresentation."[74] Model Rule 1.0(d) defines "fraud," as "conduct that is fraudulent under the substantive or procedural law of the applicable

70. *See* People v. Boyle, 942 P.2d 1199 (Colo. 1997).

71. *In re* Ungar, 25 So.3d 101 (La. 2009).

72. *See id.*

73. Ala. St. Bar Office of Gen. Counsel, Formal Op. 02 (2007) (limiting its conclusion to the non-litigation context); St. Bar of Ariz. Ethics Comm., Ethics Op. 03 (2007); Fla. Bar ethics Dep't, Ethics Op. 02 (2006); Me. Bd. Of Overseers of the Bar, Prof'l Ethics Comm. Op. 196 (2007); N.H. Bar Ass'n, Ethics Comm. Op. 4 (2008–2009).

74. MODEL RULES OF PROF'L CONDUCT R. 8.4 (2013).

jurisdiction and has a purpose to deceive."[75] Some courts have interpreted dishonesty as conduct that "[evinces] a lack of honesty, probity or integrity in principle; a lack of fairness and straightforwardness."[76] Misrepresentations, however, have been described as "statements made with reckless disregard for the truth."[77] Opponents of metadata mining argue that an active search for metadata, or "mining," "'crosses the line' from upholding a duty of diligent representation to engaging in conduct that is dishonest, deceitful, and prejudicial to the administration of justice" for it seeks to give the receiving lawyer an unfair advantage over the sending lawyer.[78] The New York Bar Association Committee on Ethics and Professional Responsibility has even stated that a lawyer who "get[s] behind" visible documents and mines confidential information "violates the letter and spirit of ethical obligations."[79]

This modified view can only be described as overtly irresponsible for it seeks to "spare the rod and spoil the child," or the negligent sending lawyer, for it allows a sending attorney to carelessly send information. Contrastingly, bar associations seeking to avoid this wanton behavior have instead found a "receiving lawyer would be doing nothing wrong by 'gleaning' clues as to the sending attorney's strategies, confidences, secrets, and intentions by analyzing the document's metadata[,]" for a receiving lawyer's duty to his or her opposing counsel is to only provide notice.[80]

Among others, Maryland, the District of Columbia, Oregon, Colorado, West Virginia, Washington, and the Vermont State Bar Associations fall under this category and have advised that metadata mining should be required.[81] These associations argue that metadata generally does not carry protected or confidential information.[82] With confidential information

75. MODEL RULES OF PROF'L CONDUCT R. 1.0(d) (2013).

76. *In re* Obert, 89 P.3d 1173 (Or. 2004); *cf. In re* Scanio, 919 A.2d 1137, 1141 (D.C. 2007).

77. *In re* Surrick, 338 F.3d 224 (3d Cir. 2003).

78. Elizabeth W. King, *The Ethics of Mining for Metadata Outside of Formal Discovery*, 113 PENN. ST. L. REV. 801, 820 (2009) (citing N.Y. State Bar Ass'n Comm. on Prof'l Ethics, Op. 749 at 3 (2001); N.Y. County Law. Ass'n Comm. on Prof'l Ethics, Op. 738 at 3 (2008); Me. Prof'l ethics Comm. of the Bd. Of Overseers of the Bar, Op. 196, at 3 (2008)).

79. N.Y. State Bar Ass'n Comm. on Ethics and Prof'l Responsibility, Formal Op. 749 (2001).

80. Thorpe, *supra* note 2, at 274 (citing ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 06-442 (2006) (providing ABA's view on the issue of metadata)).

81. ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 442 at 3 (2006); Md. St. Bar Ass'n Comm. on Ethics, Ethics Docket 09 (2007); Wash. St. Bar Ass'n. Op. 2216 (2012); Vt. State Bar Ass'n Ethics Op. 01 (2009); D.C. Bar Legal Ethics Comm., D.C. Op. 341 (2007); Colo. Bar Ass'n Ethics Comm., Op. 119 (2007); W. Va. Bar Ass'n, Lawyer Disciplinary Bd., L.E.O. 01 (2009); Or. State Bar Ass'n Ethics Op. 2011-187.

82. ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 442 at 3 (2006).

nonexistent, the mining of metadata can simply be seen as retrieving information that is already present in the document and is unprotected. Similar to reading the footnotes of a paper, metadata can be seen as additional information that a lawyer can use to learn more about the document as a whole. Opponents of metadata mining rely on the large assumption that metadata mining is "typically undertaken in an effort to reveal inadvertently sent confidential information."[83] The majority of bar associations contest, however, that most documents do not contain confidential information, and that lawyers may have legitimate reasons for mining the non-confidential metadata.[84]

The ABA has addressed the issue of mining metadata. In 2006, the ABA applied this narrow obligation to the context of the review and use of metadata in electronic documents, holding that the Model Rules permit a receiving lawyer "to review and use embedded information contained in email and other electronic documents."[85] The ABA's position further "place[d] the entire burden of protecting against disclosure of confidential information on the sending attorney, and recommend[ed] that sending attorneys scrub metadata from electronic documents, avoid creating metadata in the first place, and refrain from sending documents electronically."[86] The ABA concluded that there is not an ethical rule "expressly prohibiting the conduct, and the only affirmative obligation of the receiving attorney is to notify the sending attorney."[87]

In addition, some bar associations have stated that lawyers may actually have an affirmative duty to mine for metadata. The D.C. Bar concedes "where a lawyer knows that a privileged document was inadvertently sent, it is a dishonest act under D.C. Rule 8.4(c) for the lawyer to review and use it without consulting with the sender."[88] The D.C. Bar follows this statement, however, by stating that when the privileged nature of the document is not apparent on its face, there is no obligation to refrain from reviewing it.[89] Furthermore, the D.C. Bar has actually noted the duty of diligent representation under D.C. Rule 1.3 may trump confidentiality concerns and compel attorneys to mine metadata.[90]

---

83. Perlman, *supra* note 31, at 792.
84. *Id.* at 792.
85. ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 06-442 at 1 (2006)
86. King, *supra* note 78, at 822 (citing ABA Comm. On Ethics and Prof'l Responsibility, Formal Op. 06-442, at 4-5 (2006)).
87. *Id.* at 821–22.
88. D.C. Bar Legal Ethics Comm., Op. 341 D.C. Op. (2007).
89. *Id.*
90. *Id.*

Accordingly, the majority of bar associations view the mining of metadata as ethical and, thus, attorneys should be compelled to mine metadata in their diligent representation of their clients.

C. Arguments Against Mining Metadata

The strongest arguments against allowing metadata mining are that metadata mining is expensive and that it is privileged information protected under the work-product doctrine. Opponents of mining metadata argue that due to the vast amounts of metadata, mining can be extremely expensive, which is true. Furthermore, metadata can show the mindset of the attorney, and thus be protected under the work-product doctrine. The flaws in these arguments are, however, that increased activity in mining metadata can help reduce costs and that the abandonment of using metadata is a regressive step. Additionally, while some metadata can be protected under work-product doctrine, a majority of the useful metadata such as system metadata, cannot. Accordingly, while these are valid arguments against metadata mining, they are too regressive and broad.

1. Mining Metadata is Expensive

One argument against mining metadata is that it is expensive. This claim is not unfounded. With the advantages of electronic storage, including convenience and space saving, have come the cons of its vast enormity. Considering that 1 gigabyte of storage can be converted to approximately 7,000 files (around 130 kilobytes per file), it can take hundreds of hours for attorneys to review such files. Taking into account attorney billing rates, reviewing gigabytes of data can cost hundreds of thousands of dollars. Additionally, this is under the assumption that each file is easily produced.

In *Zubulake v. UBS Warburg LLC*, a major issue at trial was the total cost of production.[91] It would have been extremely expensive to retrieve all the backup tapes of the company emails because the files were kept in a format that was not easy to access.[92] During the course of the trial approximately 600 emails were produced, restoration of which would have cost an estimated $175,000 exclusive of attorney review time.[93] Accordingly, the court developed a seven factor test for cost shifting:

91. *See* Zubulake v. UBS Warburg LLC, 217 F.R.D. 309 (S.D.N.Y. 2003).
92. *Id.* at 318.
93. *Id.* at 312.

"(1) [t]he extent to which the request is specifically tailored to discover relevant information; (2) [t]he availability of such information from other sources; (3) [t]he total cost of production, compared to the amount in controversy; (4) [t]he total cost of production, compared to resources available to each party; (5) [t]he relative ability of each party to control costs and its incentive to do so; (6) [t]he importance of the issues at stake in litigation; and (7) [t]he relative benefits to the parties of obtaining the information."[94]

However, all of the seven factors were not treated equally. The first and second factor, the marginal utility test, were considered to be the most important.[95] Factors three, four, and five addressed the cost of production for the parties.[96] Factor six, the court noted, is rarely an issue and was not in *Zubulake*, and factor seven, the relative benefits of production between the requesting and producing party, was considered the least important because it could be presumed that the production would favor the requesting party.[97] While metadata mining is expensive, this reason cannot be an excuse to ban metadata mining. Contrastingly, it is a reason to increase efforts to mine metadata. As time has shown, increased activity in a market lowers the cost of the supply. In a simple economic model, the more supply there is compared to demand, the lower the market price. An increase in the amount of people mining metadata will attract more professionals to the field and thus lower the cost of utilizing third parties.

Additionally there have been two methods that attorneys have begun using, claw-backs and quick peeks, to reduce costs. Federal Rule of Evidence 502(b), adopted in 2008, references inadvertent disclosure, stating that "when made in a federal proceeding or to a Federal office or agency, the disclosure does not operate as a waiver in a Federal or State proceeding if: (1) the disclosure is inadvertent; (2) the holder of the privilege or protection took reasonable steps to prevent disclosure; and (3) the holder promptly took reasonable steps to rectify the error, including (if applicable) following the Federal Rule of Civil Procedure 26(b)(5)(B)."[98] The Advisory Committee's Note explains that Rule 502 "contemplates enforcement of 'claw-back' and 'quick peek' arrangements as a way to avoid the excessive costs of pre-production review for

94. *Id.* at 322.
95. *Id.* at 323.
96. *Id.*
97. *Id.*
98. FED. R. EVID. 502(b).

privilege and work product."[99] Under a claw-back agreement, the parties can agree (and a court can order) that, if a party inadvertently produces a privileged document, the receiving party must return it.[100] This eliminates the need for the producing party to take "reasonable steps" (or in some cases, any steps) to prevent the disclosure of the privileged information. Quick peek, on the other hand, provides access to documents or ESI prior to production to try to reduce the cost of processing and production by trying to convince an opposing party that it is asking for irrelevant documents. Through the use of claw-backs and quick peeks, the cost of mining metadata can be significantly decreased.

2. Metadata is Privileged Information

Another strong argument for a ban on producing metadata and, consequently, the mining of metadata, is that metadata is protected under the work product doctrine. Under Federal Rule of Evidence 502, "work product protection" is defined as the protection that applicable law provides for tangible material (or its intangible equivalent) prepared in anticipation of litigation or for trial.[101]

United States v. Wirth is perhaps the most relevant and largest proponent for the restriction of metadata in discovery motions. In *Wirth*, the defendants were charged with tax evasion.[102] The defendants moved under Rule 16 and the *Brady* doctrine for an order compelling "production of rough notes from each interview conducted by the Government in connection with this case and all draft interview summaries in electronic format with metadata intact."[103]

Rule 16 "requires the Government to allow the defendant to inspect, copy, or photograph all books, papers, documents, data, photographs, [or] tangible objects . . . if the item is material to the preparation of the defense."[104] "Material" as defined for Rule 16 refers to anything that is "helpful to the defense."[105] Metadata fits under the umbrella of Rule 16 for information regarding who accessed documents or if changes were made to the document could be helpful in the preparation of the defense. The *Brady* doctrine comes from *Brady v. Maryland,* where it was held that a

99. FED. R. EVID. 502 advisory committee's note.
100. *Id.*
101. FED. R. EVID. 502(g).
102. United States v. Wirth, 2012 WL 1110540 (D. Minn. Apr. 3, 2012).
103. *Id.* at *1.
104. *Id.* at *2.
105. United States v. Vue, 13 F.3d 1206, 1208 (8th Cir. 1994).

defendant is denied due process of the law if his conviction is undermined by the failure of the prosecution to reveal the existence of potentially exculpatory evidence that might have made a difference in the outcome of the trial.[106] Furthermore, in *United States v. Bagley*, Justice Blackmun noted that material evidence must be disclosed if there is a "reasonable probability that, had the evidence been disclosed to the defense, the result of the proceeding would have been different."[107]

The government contended that this information was protected under the work-product doctrine. The work-product doctrine protects material prepared by an attorney acting for a client in anticipation of litigation, as well as investigators and other agents for the attorney.[108] The court found that "*Brady* mandates disclosure of exculpatory evidence notwithstanding the work-product doctrine, except where work product is solely mental impressions, conclusions, or legal theories, i.e. so-called 'opinion work product.'"[109] Electronic draft summaries with intact metadata were considered work product revealing the attorney's mental process and were therefore entitled to stronger protection than other types of work product.[110]

Additionally, the court stated that "[m]etadata, almost by definition, shows the mental processes of the drafter of a document by revealing the drafter's drafting decisions and steps" and should thus be considered opinion work.[111] Accordingly, the court held that notes and summaries that are work product are shielded from disclosure under Rule 16, and if the work product is opinion work product, such as electronic files with metadata, it is protected from disclosure under *Brady*.[112]

Under *U.S. v. Wirth*'s logic, the work product doctrine acts like a shield for mining metadata, for metadata can be seen as protected information, and thus is protected from disclosure and metadata mining. This interpretation, however, is overly broad as only certain metadata should fall under this category. Under *Wirth*, application metadata like the Track Changes function in Word might be protected because it might show the

106. Brady v. Maryland, 373 U.S. 83 (1963).

107. United States v. Bagley, 473 U.S. 667, 682 (1985).

108. *See* United States v. Nobles, 422 U.S. 225, 236–40 (1975) (extending work-product doctrine to criminal, as well as civil, discovery); *see also* FED. R. CRIM. P. 16(a)(2).

109. *Wirth*, *supra* note 102, at *3.

110. *Id.* at *4.

111. *Id. See also* Rachel K. Alexander, *E-Discovery Practice, Theory, and Precedent: Finding the Right Pond, Lure, and Lines Without Going on A Fishing Expedition*, 56 S.D. L. Rev. 25, 36 (2011) (noting metadata "might include creation and editing dates, author and user names, comments, and historical data identifying specific document modifications").

112. *Wirth*, *supra* note 102, at *4.

thought process of the attorney drafting the document. System metadata, however, is created by the computer or system itself, and consists of information such as who created the document or when the document was modified. Work created by a machine can hardly be seen as depicting the mental process of the drafter of the document and would thus fall outside the scope of *Wirth.* Embedded metadata, such as a formula in Excel, is more ambiguous for it could be seen as depicting the thought process of an attorney in calculating values. However, under this approach almost everything that an attorney does can be seen as part of his or her thought process. Accordingly, while certain aspects of metadata can be seen as protected under the work product doctrine, much of metadata is not privileged and should be mined.

IV. THE ADVERSARIAL SYSTEM WOULD BE BEST SERVED BY A POLICY COMPELLING METADATA MINING

A policy compelling receiving lawyers to mine metadata enhances thorough advocacy by forcing lawyers to diligently protect sensitive information as well as encouraging lawyers' efforts to scrutinize documents. With the adoption of ever-advancing technology in the legal field, lawyers have a duty to keep themselves informed about the tools that they use. Encouraging metadata mining would drive lawyers on both sides of the legal process to heighten their competence; not only would sending lawyers be forced to take greater measures to protect the information they send, but receiving lawyers would also have to further scrutinize and investigate metadata. Accordingly, the foundation of the adversarial system argues for a policy that compels lawyers to mine for metadata.

A. The Adversarial Process Requires Lawyers to Advance with Technological Advances

The practice of law is not stagnant but rather evolves with the times. With advances in technology, the duty of diligence requires lawyers to be reasonably knowledgeable with the tools they use. Even New York, the biggest proponent of banning metadata mining, admits that reasonable care may require lawyers to "stay abreast of technological advances and the risks involved with electronic transmissions," and thus obliges lawyers to be familiar with technology to avoid harming their clients.[113]

113. *See* N.Y. State Bar Ass'n Comm. on Ethics and Prof'l Responsibility, Formal Op. 782 (2004).

Furthermore, diligent lawyers are becoming more technologically competent and have become more aware of metadata and the precautions required to prevent the spread of confidential information.[114] As some have argued "it would be unfair to punish those that know how to use technology well and reward others for not learning how to use technology."[115]

B. Clear Duties to Mine Metadata Enhance the Adversarial System

Compelling lawyers to mine metadata would raise the bar of competency, create a more equal advocacy system, and ultimately enhance the adversarial system. Several bar associations opt to prohibit the mining of metadata, arguing that this prohibition protects against dishonest actions of mining. This rule lowers the standards of advocacy. By preventing receiving lawyers from mining metadata, these bars are essentially allowing the sending lawyers to negligently send ESI. Furthermore, these bars lower the standards for receiving lawyers as well. Receiving attorneys would no longer need to act with reasonable diligence in representing their clients, because under this standard they do not need to investigate the entire document. Essentially, this policy seeks to lower the standards of diligence for both sending and receiving lawyers.

Conversely, a policy that requires receiving lawyers to ethically mine for metadata would raise the bar of competency for lawyers. Sending lawyers would be put on notice that receiving lawyers have a duty to mine metadata, and as a result they would understand that any information that they send *will* be subject to review by the receiving lawyer. Accordingly, all electronically stored information sent by the sending lawyer will be seen as information that was intentionally sent, as opposed to protected confidential information. Consequently, sending attorneys would no longer be able to raise the defense that information that they negligently sent was privileged and thus would be forced to scrutinize more intensely the information they are sending. An affirmative duty to mine for metadata would also require receiving lawyers to increase their diligence. They would no longer be able to rely on the crutch that the data was not intentionally sent or that such actions constituted dishonesty, and they would be forced to thoroughly examine each document. Consequently, a policy that places an affirmative duty on receiving lawyers to ethically mine for metadata would not only enhance sending lawyers' scrutiny in

114. *Id.*
115. Thorpe, *supra* note 2, at 280 (citation omitted).

sending documents under Rule 1.6, but also increase the level of diligent representation of receiving lawyers under Rules 1.1 and 1.3.

Clear duties to mine metadata data would not only force lawyers to become more adept in their field, but would also create a more equal advocacy system. New York and other opponents of mining metadata seek to retreat from the evolution of technology, arguing that those who are technologically proficient have an unfair advantage over those who are lacking, and this is inherently unfair.[116]

The truth is that those who are technologically more proficient *will* have an advantage. The dividing point is, however, that this advantage is not unfair, but rather part of the legal field. The principles of the adversarial system are not that different from biology and evolution. In biology, the Red Queen Hypothesis states that one must run as fast as one can, simply to stay in place, alluding to a biological theory that organisms must do everything they can just to stay alive, or keep up.[117] In the legal field, the adversarial mindset should drive litigators to "run as fast as they can" in an effort to bring the most competent representation possible for their clients. A policy that compels lawyers to ethically mine for metadata seeks to level the playing field by requiring everyone to "bring a gun to a gun fight," instead of allowing for mishaps for when one is less than equipped. While there will still be some unfairness, as some lawyers may be better with technology, a widespread duty to mine metadata would at least put all attorneys on notice, and the fairness disparity will result from differences in skill as opposed to ignorance.

C. Courts Have Begun to Recognize the Importance of Competence in Electronic Discovery

In the age of electronic discovery, courts have begun to recognize that lawyers must be competent with technology.[118] No longer can attorneys feign ignorance in the field of electronics and claim that their inadequacy is simply a result of computer illiteracy. Courts have found that attorneys now must not only be familiar with the field of electronically stored information, but also proficient enough to successfully navigate it. The

116. Ala. State Bar Ass'n Comm. on Ethics and Prof'l Responsibility, Formal Op. RO-2007-02 (2007).

117. *See* Leigh Van Valen, *A New Evolutionary Law*, 1 EVOLUTIONARY THEORY 1 (1979).

118. Thomas Newcomb Hyde, *Staying Out of Trouble: Legal Ethics in a Digital Era*. 32 No. 3 TRIAL ADVOC. Q. 23 (2013).

ability to mine and scrub metadata is consistent with this notion. Consequently, attorneys should be compelled to mine for metadata.

In *Martin v. Northwestern Mut. Life Ins. Co.*, a lawyer sought benefits from Northwestern Mutual for being disabled.[119] Northwestern Mutual in turn requested information about Martin's income when disabled, which was repeatedly denied.[120] Suspecting that there was still information that Martin did not produce, Northwestern subpoenaed both Martin's bookkeeper and his fiancée, finding that there were boxes of evidence that Martin claimed did not exist.[121] When questioned at court about his behavior, Martin claimed that he should not be sanctioned, as his failure to produce documents was due to his computer illiteracy, which rendered him unable to retrieve any electronically stored information.[122] The court found that claim was "frankly ludicrous" and imposed sanctions of expenses and attorney's fees."[123]

From *Martin*, attitudes from judges about electronic evidence point to a growing intolerance of computer inadequacy. Judges now expect that attorneys should be able to obtain electronic evidence. As previously stated, metadata is part of electronic evidence, and proficiency in retrieving electronic evidence would include an ability to mine metadata.

Additionally in *Chen v. Dougherty*, a plaintiff sued for employment discrimination and won on the claim for retaliation.[124] The lawyer accordingly sought attorney fees.[125] The court, however, found that the attorney had caused a discovery dispute by failing to offer search terms for the electronic discovery produced, causing the opposing party to produce over 50,000 documents. The court held that "the lawyer's inhibited ability to participate meaningfully in electronic discovery tells the court that she has novice skills" and penalized her by reducing her fees.[126]

Chen points to the growing sentiment that not only should attorneys be familiar with computers and ESI, but also that attorneys need to be proficient. Attorneys can no longer just be able to use a computer and ESI, but now must be able to work the more intricate areas of such fields. Metadata, consequently, is part of being competent in the field of

119. Martin v. Northwestern Mut. Life Ins. Co., No. 804CV2328T23MAP, 2006 WL 148991, at *1 (M.D. Fla. Jan. 19, 2006).
120. *Id.*
121. *Id.*
122. *Id.*
123. *Id.* at *2.
124. Chen v. Dougherty, No. C04-987 MJP, 2009 WL 1938961 (W.D. Wash. July 7, 2009).
125. *Id.* at *2.
126. *Id.*

electronic discovery, and attorneys should thus be required to mine for metadata.

Lastly, in *William A. Gross Constr. Assoc. v. Amer. Mfrs. Mut.*, the parties requested "the use of thousands of additional search terms . . ." from a non-party.[127] The court wrote: "This case is just the latest example of lawyers designing keyword searches in the dark, by the seat of the pants, without adequate (indeed, here, apparently without any) discussion with those who wrote the e-mails."[128] The court further explained counsel must be able to understand how to carefully craft appropriate keywords, with input from the ESI custodians "to assure accuracy in retrieval and elimination of 'false positives.'"[129] The court added that "[i]t is time that the Bar—even those lawyers who did not come of age in the computer era—understand this."[130]

William points to a final sentiment that understanding how to use computers and electronic evidence is not enough, suggesting that expertise rather than competency is the standard. *William* shows that simply being able to create search terms is not sufficient anymore, and attorneys must instead be able to work with ESI custodians and establish patterns when finding evidence. This level of sophistication is actually quite a high bar, as it requires not only legal expertise in recognizing patterns in evidence, but also technological expertise in crafting search terms. At this level, attorneys would be expected to not only be able to mine for metadata but also to determine how to create patterns for mining metadata so that metadata can be mined efficiently. While this standard is potentially harsh on all those who lack technological finesse, *William* can be seen as a push towards driving attorneys to becoming technologically savvy professionals.

Through *Martin*, *Chen*, and *William*, courts views towards electronic evidence can be seen to have evolved towards stricter standards of competency. Attorneys are not only expected to be familiar with electronic evidence, but also to be competent and even proficient in its use. Accordingly, courts have recognized the importance of electronic evidence and that attorneys should be able to mine for metadata proficiently.

---

127. William A. Gross Constr. Assoc. v. Amer. Mfrs. Mut., 256 F.R.D. 134, 134 (S.D.N.Y. 2009).
128. *Id.* at 135.
129. *Id.* at 136.
130. *Id.*

V. CONCLUSION

Lawyers should be compelled to mine for metadata as it is a valuable source of evidence, the Model Rules of Professional Conduct suggest that lawyers have a duty to mine for metadata, attacks against metadata are unfounded, and the adversarial process would best be served by lawyers mining for metadata. Mining for metadata is not unethical, because most metadata does not contain confidential information, and sending lawyers should be aware of what information they disclose. Metadata is a core part of a document, and therefore a lawyer, under Rules 1.1 and 1.3, should have a duty to scrutinize it in acting competently. Arguments against metadata, such as cost and privilege, are unfounded because widespread mining of metadata would reduce costs and not all metadata is privileged. Finally, mining metadata helps achieve the root goal of the adversarial process: litigants advocating for their clients to their fullest capacities with as much information as possible to achieve the truth. Accordingly, the legal system is best served by a policy compelling lawyers to mine for metadata.