North Dakota Law Review

Volume 84 | Number 1 Article 9

1-1-2008

Metadata: The Dangers of Metadata Compel Issuing Ethical Duties to "Scrub" and Prohibit the "Mining" of Metadata

Crystal Thorpe

METADATA:
THE DANGERS OF METADATA COMPEL ISSUING ETHICAL DUTIES TO "SCRUB" AND PROHIBIT THE "MINING" OF METADATA

"The economic and technological triumphs of the past few years have not solved as many problems as we thought they would, and, in fact, have brought us new problems we did not foresee."[1]
–Henry Ford

I. INTRODUCTION

"Metadata" is a new term in the lexicon of attorneys.[2] It is often referred to as the modern "lawyer's favorite cyber bo[o]gie man."[3] However, "[o]nly 10 percent or less [of lawyers] seem to absorb just how dangerous metadata can be."[4] Ignorance of metadata is no excuse, whereas it has been analogized to the statement made by Richard Dreyfuss, as Hooper, in *Jaws*, "I think that I am familiar with the fact that you are going to ignore this particular problem until it swims up and bites you."[5]

With the advent of electronic communications, attorneys in their respective states, and in particular the American Bar Association (ABA), are compelled to invade the world of technology, and as a result, the world of metadata.[6] Indeed, some states have already set the trend by imposing an ethical duty on both the sending and the receiving attorney to appropriately manage metadata.[7] On one end is a duty to avert hidden data from becoming "mined."[8] In other words, attorneys have a duty to "scrub" electronic

---

1. Jima Anne Kato, *The Brave New World of Electronic Discovery and Document Management*, 49 ORANGE COUNTY LAW. 6, 6 (2007).

2. Sylvia E. Stevens, *Metadata: Guarding Against the Disclosure of Embedded Information*, 67 OR. ST. B. BULL. 9, 9 (2007).

3. Lawrence M. Friedman, *What, Me Worry About Metadata?*, 18 CBA REC. 43, 43 (2004).

4. Sharon D. Nelson & John W. Simek, *Metadata: What You Can't See Can Hurt You*, 32 L. PRAC. 28, 28 (2006).

5. *Id*.

6. J. Craig Williams, *The Importance of Deleting Metadata . . . And How to Do It*, 49 ORANGE COUNTY LAW. 48, 48 (2007).

7. Peter Mierzwa, *Metadata: Now You Don't See It–Now You Do*, 20 CBA REC. 52, 52 (2006).

8. *See id*. at 57 (describing various methods to manage metadata, but proffering the adoption of a standardized scrubbing procedure).

documents for metadata.[9] At the other end of the spectrum is a duty to avoid the use of technology to spy on an opponent,[10] thereby prohibiting an attorney from "intentionally tak[ing] advantage of other people's failures."[11] Attorneys have a duty to prohibit "mining" for metadata.[12]

Part II of this note provides an overview of what metadata is, the purposes it serves, and its relevance in the legal profession.[13] Part II.A explains how metadata pervades the world of technology by providing a detailed discussion of the purpose hidden data serves and the hazards it creates within various computer software programs, including Microsoft Word, Word Perfect, and Adobe Acrobat.[14] In addition, the dangers of metadata that lurk within the legal profession are addressed.[15] Part II.B examines the ABA Model Rules of Professional Conduct that at a minimum set up a framework with which to handle metadata dangers.[16] As an illustration, Model Rules 1.1, 1.3, 1.6, 8.4, and 4.4 are discussed in detail.[17] Part II.B also examines states that have issued ethics opinions directly addressing metadata concerns.[18] However, the essence of this note advocates that the ABA, as well as individual states, establish a consistent ethical standard pertaining to "scrubbing" and "mining" for metadata.[19] As a result, Part II.C advocates corresponding ethical duties on both the sending and receiving attorney, in which specific ethical obligations are addressed.[20]

---

9. Nelson & Simek, *supra* note 4, at 28. To "scrub" an electronic document is to remove metadata. *Id.*

10. *See, e.g.*, Jason Krause, *Metadata Minefield: Opinions Disagree on Whether It's Ethical to Look at Hidden Electronic Information*, 93 A.B.A. J. 32, 32 (2007) (noting how some jurisdictions prohibit attorneys from using technology to spy on opposing counsel).

11. 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, 247 (2007) [hereinafter Hricik, *Mining for Embedded Data*].

12. *See* discussion *infra* Part II.B.2.a-c (noting that jurisdictions impose a duty on recipient attorneys to preclude looking for metadata). "Mining" a document is defined as intentionally seeking out and viewing metadata within an electronic document. Ala. State Bar Ass'n Comm. on Ethics and Prof'l Responsibility, Formal Op. RO-2007-02 (2007), *available at* http://www.alabar.org/ogc/PDF/2007-02.pdf.

13. *See* discussion *infra* Parts II.A.1-4 (defining metadata by explaining its purpose, its accessibility, and the dangers it creates within the legal profession).

14. *See* discussion *infra* Part II.A.1-3 (explaining the advantages and disadvantages of metadata within computer software programs).

15. *See* discussion *infra* Part II.A.4 (noting the relevance of metadata in legal document preparation, contract litigation, and electronic discovery).

16. *See* discussion *infra* Part II.B.1.a-d (setting out the ABA Model Rules that discuss metadata concerns).

17. *Id.*

18. *See* discussion *infra* Part II.B.2.a-d (noting the various ways jurisdictions have addressed metadata).

19. *See* discussion *infra* Part II.C.1-5 (proposing a new ABA Model Rule that imposes a duty to "scrub" metadata and prohibits the "mining" of metadata).

20. *Id.*

Finally, Part III proposes that the present Rules of Professional Conduct in North Dakota are insufficient to cover metadata concerns, and therefore, North Dakota should take action and implement guidelines consistent with other trend-setting jurisdictions.[21]

II. METADATA

With the arrival of the digital age come the dangers of metadata.[22] This new term in the vocabulary of attorneys requires an in depth definition to illustrate the purposes of metadata, as well as the accessibility of metadata and its prevalence in the legal profession.[23] In addition, the inception of metadata creates a number of ethical issues, which the ABA Model Rules of Professional Conduct have failed to fully address.[24] However, a few states have taken the initiative to issue ethics opinions persuasive to the legal profession on the topic of metadata.[25] Nevertheless, the heart of this note urges the imposition of ethical obligations on the sending attorney to "scrub" for metadata and on the receiving attorney to abstain from the "mining" of metadata.[26]

A. WHAT IS METADATA?

Metadata must first be defined and illustrated to demonstrate both its beneficial purposes and the inevitable hazards related to it.[27] As such, a

---

21. *See* discussion *infra* Part III (indicating that the present North Dakota Rules of Professional Conduct are inadequate in addressing future ethical standards applicable to metadata).

22. *See* Philip J. Favro, *A New Frontier in Electronic Discovery: Preserving and Obtaining Metadata*, 13 B.U. J. SCI. & TECH. L. 1, 2 (2007) (noting the significance of technological innovations, the issues technology raises, and in particular, the presence of metadata in the practice of law).

23. *See* Brian D. Zall, *Metadata: Hidden Information in Microsoft Word Documents and Its Ethical Implications*, 33 COLO. LAW. 53, 54 (2004) (defining metadata and its purposes, accessibility, and relevance within the legal profession).

24. *See* Shawn Newman, Metadata: Reflection on an Attorney's Professional Responsibility 2 (Apr. 18, 2005) (unpublished manuscript, on file with Widener University School of Law), *available at* http://www.cctinstitute.com/docs/05S-ED/EDO5SnewmanPaper.pdf (indicating that the Model Rules merely provide guidance as to ethical standards when dealing with metadata).

25. *See id*. at 2 (pointing out a few jurisdictions that have issued ethics opinions to absolve metadata dangers).

26. *See* Mierzwa, *supra* note 7, at 52 ("The importance of managing metadata has been elevated to the level of an ethical duty in some jurisdictions."). "Scrubbing" is the act of purging an electronic document of metadata. Nelson & Simek, *supra* note 4, at 28. "Mining" is the act of deliberately searching for and viewing metadata. Ala. State Bar Ass'n Comm. on Ethics and Prof'l Responsibility, Formal Op. RO-2007-02 (2007), *available at* http://www.alabar.org/ogc/PDF/2007-02.pdf.

27. *See* Zall, *supra* note 23, at 54 (explaining the purposes of metadata); *see also* Favro, *supra* note 22, at 4 (discussing the hazards of metadata).

detailed explanation on the accessibility of metadata is required.[28] Lastly, it is imperative to show how metadata implicates the legal profession.[29]

1. *The Definition of Metadata*

"[D]ocuments are the lifeblood of attorneys."[30] However, the practice of law is no longer driven by paper transactions, but rather by paperless operations.[31] The arrival of the digital age has transformed the world and, in particular, the legal system.[32] Computers are improving productivity by enabling attorneys to easily and quickly modify documents.[33] In addition, wireless networks have expanded over the last decade.[34] This increased usage of digital data has not changed the practice of law; attorneys still spend a great amount of time drafting and reviewing documents.[35]

However, the digital era brings with it a decreased capacity to sufficiently control documents and safeguard confidential data.[36] Moreover, the movement into the digital world has not changed an attorney's obligation to protect client confidences pursuant to the rules governing professional conduct.[37] With the onset of the digital world, attorneys are forced to quickly adapt to technologies that alter the practice of law.[38] Thus, practicing attorneys should be cautioned that it is an absolute necessity to acquire a basic understanding of ongoing technological innovations.[39]

---

28. *See* Zall, *supra* note 23, at 54 (explaining metadata and its purposes); *see also* Favro, *supra* note 22, at 4 (discussing metadata dangers).

29. *See* Campbell C. Steele, *Attorneys Beware: Metadata's Impact on Privilege, Work Product, and the Ethical Rules*, 35 U. MEM. L. REV. 911, 914-23 (2005) (indicating the relevance of metadata in the practice of law).

30. Ellen Freedman et al., *The Lawyer's Guide to Mobile Computer Security*, 29 PENN L. 32, 34 (2007).

31. Favro, *supra* note 22, at 2.

32. *Id*.

33. *See* Andrew Beckerman-Rodau, *Dealing With Digital Data in the Practice of Law: Do You Know Where Your Data Is?*, 2006 J. INTERNET L. 3, 3, *available at* http://www.lawprofessor.org/resources/pdf/periodicals/journal-of-internet-law.pdf (explaining that networked computers and Internet connections allow for the instant transferring of documents).

34. *See id*. (noting that wireless Internet access is increasingly available in various locations, including coffee shops, hotels, airports, and residences).

35. *Id*.

36. *Id*.

37. *See id*. (noting that attorneys are required to use reasonable efforts to protect client confidences from inadvertent disclosure); *see also infra* Part II.B.1.a-d (discussing the ABA Model Rules applicable to professional conduct with regard to metadata).

38. *See generally* Favro, *supra* note 22, at 2-4 (discussing the transformation from paper transactions to paperless operations).

39. *See generally* Eleanor B. Kellett, *Unintended Consequences: Maintaining Basic Understandings of Technology—An Ethical Obligation*, 18 S.C. LAW. 42, 48 (2006) (advocating an ethical obligation to understand the ramifications of technology in client representation).

Steven Ballmer, the CEO of Microsoft, supplied the paradigm, "business leads technology."[40] This equation premises the conclusion that "technology leads the law."[41] As new technologies create methods of performing business better, the law must assimilate the material impact of these technological advancements.[42] Yet numerous issues arise at the crossroads of digital data and the practice of law, although this note touches only on the issue of metadata within electronic communications.[43]

"Metadata pervades the digital world in which we live."[44] By definition, metadata is data that provides information about other data.[45] It is information that computer software programs embed in documents, which makes it possible to discern: who drafted the document, when it was created, for which client the document was created, what alterations were made to the document, and a multitude of other information, all of which may include confidential information.[46] In short, metadata is digital information pertaining to a document's characteristics including its origin, usage, and validity.[47] Metadata is the how, when, and by whom an electronic document is created and formatted.[48]

A document may look like a two-dimensional piece of paper on a computer screen, but in reality it is germane to a three-dimensional file folder.[49] The version on the screen is the top document, but behind the screen is the remainder of the folder.[50] In emailing this document, the entire folder is sent, which includes all prior versions, dates of alterations, edits, time spent on edits, identity of editors and authors, and any notes attached.[51] Furthermore, metadata may be invisible in various places within a document, but accessible to virtually anyone that can open electronic

---

40. *Id*.

41. *Id*.

42. *See id*. (noting that software vendors compete to find the newest and best versions of programs, and that the "technology that you knew and understood yesterday may not work the same way as the newer version that you are using today").

43. Beckerman-Rodau, *supra* note 33, at 3 (noting that numerous legal issues regarding digital data have not been addressed by courts, but some states have provided ethics opinions as guidance).

44. David Hricik, *I Can Tell When You're Telling Lies: Ethics and Embedded Confidential Information*, 30 J. LEGAL PROF. 79, 81 (2006) [hereinafter Hricik, *Telling Lies*].

45. Merriam-Webster, http://www.merriam-webster.com/dictionary/metadata (last visited Jan. 8, 2008).

46. Williams, *supra* note 6, at 48.

47. Favro, *supra* note 22, at 7.

48. Stevens, *supra* note 2, at 9.

49. David L. Brandon, *The Hidden Perils of Metadata*, LPL ADVISORY (ABA Standing Comm. on Lawyers' Prof'l Liab.), Fall 2006, at 2.

50. *Id*.

51. *Id*.

files.[52] As a result, the repercussions of releasing metadata can have either a positive or negative impact, depending on how documents are created and shared.[53]

2. *The Purpose of Metadata*

Metadata is not a new concept, as it was initially developed by software programmers who worked in collaborative environments where information was commonly shared.[54] In fact, metadata by itself is not sinister; it is intended to be useful to the creator of a document.[55] It marks a trail, operating like a log or diary, in which a project travels until its completion including who contributed to the project and what was retained or abandoned.[56] Therefore, it is quite useful for non-adversarial projects where creation of a specific document requires contribution from multiple parties.[57] As another example, an author of a document, prior to creating a new document from an old one, may check the date of the last modification to determine whether it is up-to-date.[58] Additionally, some metadata is necessary to format and store a document.[59] In essence, the purpose of metadata is to "enhance the editing, viewing, filing, and retrieval" of documents.[60]

Notwithstanding the beneficial purposes of metadata, such data may be hazardous because it is not "invisible" to everyone, but may inadvertently become viewable or accessible.[61] Additionally, even if the average user does not see the metadata, it is consistently present and easily accessible.[62] One must be mindful that an electronic document's previous history, including revisions, is discoverable from its metadata.[63] These prior versions create a foreseeable risk in which the unwary can be trapped by

---

52. Carole Levitt & Mark Rosch, *Computer Counselor: Making Metadata Control Part of a Firm's Risk Management*, 28 L.A. LAW. 40, 40 (2005).

53. Zall, *supra* note 23, at 54.

54. *Id.*

55. Levitt & Rosch, *supra* note 52, at 40.

56. Zall, *supra* note 23, at 54.

57. *Id.*

58. Levitt & Rosch, *supra* note 52, at 40.

59. Zall, *supra* note 23, at 54.

60. David Hricik & Robert R. Jueneman, *The Transmission and Receipt of Invisible Confidential Information*, 15 THE PROF. LAW. 18, 18 (2004).

61. Favro, *supra* note 22, at 4.

62. *See* Newman, *supra* note 24, at 3 (explaining that metadata is not seen, yet is easily retrieved from a number of programs); *see also* Levitt & Rosch, *supra* note 52, at 40 ("Metadata may be accessed by anyone who can open the electronic file, including clients and opposing counsel.").

63. Newman, *supra* note 24, at 3-4.

metadata.[64] The ignorance of metadata may lead to the release of sensitive information in documents, resulting in public humiliation.[65] Even worse, such ignorance can lead to the inadvertent disclosure of confidential information.[66]

Thus, if metadata is appropriately understood and utilized, it can provide an incredible service to attorneys in client representation.[67] However, if metadata is unknown, improperly controlled, or ignored, an attorney may encounter significant problems in effective client representation.[68] It is therefore imperative to understand the existence and easy accessibility of metadata by recognizing how it is created and where it is found in various software programs.[69]

3. *How to Access Metadata*

Some metadata is accessible quite easily through Microsoft Word user interface, but other metadata is accessible only through extraordinary means.[70] On the one hand, with the mere click of a computer mouse or with the aid of a "metadata viewer," an average computer user could retrieve metadata.[71] On the other hand, a computer forensics expert with additional time and a sophisticated computer software program could ascertain the document's metadata even if the author erased the information from the

---

64. *See* Jembaa Cole, *When Invisible Electronic Ink Leaves Red Faces: Tactical, Legal, and Ethical Consequences of the Failure to Remove Metadata*, 1 SHIDLER J. L. COM. & TECH. 8, 8 (2005) (indicating how metadata presents a risk in the practice of law, such as within the use of templates for drafting documents or in contract negotiations).

65. *Id.* For example, the United Kingdom government posted on its website a report regarding Iraq's weapons of mass destruction. *Id.* The government asserted that the report was current and original. *Id.* However, metadata revealed that the document was a collection of documents written years earlier by civilians who plagiarized the information from a thesis. *Id.*

66. *Id.* For an overview of how courts decide whether inadvertent disclosure of confidences or secrets waives the attorney-client privilege, *see generally* Steele, *supra* note 29, at 914-23. For example, the attorney-client privilege may be waived by inadvertent disclosure where an attorney intends to disclose communications to one party, but a third party becomes the unintended recipient. *Id.* at 917.

67. *See* Favro, *supra* note 22, at 12-13 (noting the value of metadata in authenticating documents, establishing document authenticity, demonstrating document integrity, and its ability to function as a management and security device).

68. *See id.* at 7-11, 13 (discussing the nature and significance of metadata hazards and its effect on client representation).

69. *See* Zall, *supra* note 23, at 54-55 (indicating that more attorneys are now assessing the risks of metadata by becoming aware of how metadata is created and accessed).

70. *See* Hricik & Jueneman, *supra* note 60, at 18 (noting that some metadata may only be accessible by "opening a document in a low-level binary file editor").

71. Zall, *supra* note 23, at 53. *See* Sheila Blackford, *Metadata: Danger or Delight?*, 66 OR. ST. B. BULL. 29, 33 (2006) (questioning ethical implications of viewing metadata found in electronic files received from opposing counsel). The use of a "Meta Data Reviewer" to explore and export information from a file has been questioned as unethical. *Id.* Such a software program can be purchased at www.princetonsoftwarecompany.com for $19.95. *Id.*

document.[72] For those in the practice of law a substantial amount of fear revolves around metadata in computer software programs including Microsoft Word, Corel Word Perfect, and Adobe Acrobat portable document file (PDF).[73]

a. Microsoft Word

Metadata is ubiquitous in Microsoft Word.[74] It may be found in various menu items, but the "Properties" item, which is located in the "File" menu, is the key location.[75] For example, the properties of a document may reveal the author and the date the document was created, as well as revisions.[76] Another form of embedded data is created by using "Fast Saves."[77] If this feature is enabled, the deleted information remains invisible within the document, and the receiver of such document may open the document and easily see all of the sender's prior revisions.[78]

However, the most significant feature of Word is "Track Changes," which creates a record of each and every modification.[79] A problem arises if an author does not know the feature is turned on and the screen does not reveal any modifications.[80] The changes are "invisible," yet accompany the Word file once it is transmitted, and the receiver can easily reveal the changes and revisions.[81] In addition, the "Track Changes" feature potentially permits the user to observe the text of an unrelated document, which the author used as a template for the file at hand.[82]

Another form of embedded data accompanying Word documents is "Comments."[83] Comments are great for collaborative purposes because colleagues may make comments on a file, such as suggestions or clarifications, and then exchange the file.[84] However, these comments are embedded within the file and travel with the file throughout the exchanges.[85]

---

72. Zall, *supra* note 23, at 53.
73. Friedman, *supra* note 3, at 43.
74. Hricik, *Telling Lies*, *supra* note 44, at 83. *See generally id.* at 83-89 (providing a specific, yet simple example of metadata).
75. *Id.* at 83.
76. *Id.*
77. *Id.* at 86.
78. *Id.*
79. *Id.* at 85.
80. *Id.*
81. *Id.*
82. Favro, *supra* note 22, at 86.
83. Hricik, *Telling Lies*, *supra* note 44, at 86.
84. *Id.*
85. *Id.*

The last example of embedded data in Word is found within the "Versions" feature, where all prior versions of a document are embedded within a file, and the recipient of the electronic document may view any prior version.[86] Moreover, other Microsoft programs contain metadata, such as Power Point.[87] However, embedded data is not foreign beyond Microsoft products.[88]

b. Word Perfect

Metadata is also utilized in Corel Word Perfect.[89] Word Perfect contains less descriptive information in its "Properties" file than Microsoft Word, and therefore less embedded information, but the feature can enable customized information.[90] Furthermore, Word Perfect contains a "Multiple Undoes" feature, in which the recipient of a file may "undo" previous revisions to the document.[91] However, the search for metadata does not end with Word Perfect.[92]

c. Adobe Acrobat

Finally, converting a file to Adobe Acrobat does not rid a file completely of metadata.[93] Adobe contains considerably less metadata, but nevertheless the author's name, time of creation, and alternations are visible.[94] Metadata hides in virtually all computer software programs, and these programs are employed daily in the practice of law.[95]

4. *Metadata in the Legal Profession*

Attorneys rely considerably on computer software programs in the digital age, which makes metadata a consistently present liability in their practice.[96] As attorneys become increasingly aware of metadata, questions arise in regard to the sending and receiving of documents containing

---

86. *Id*.

87. *See id*. at 87 (explaining that "Speaker's Notes" within Power Point also contain metadata, where text is visible to the speaker, but invisible when projected).

88. *Id*. at 88.

89. *Id*.

90. *Id*.

91. *Id*.

92. *Id*.

93. *Id*.

94. *Id*.

95. *See* Cole, *supra* note 64, at 8 ("Computer software is programmed to produce metadata."); *see also* Hricik, *Telling Lies*, *supra* note 44, at 82-83 (clarifying that embedded data has a purpose, but is found in programs commonly used in the practice of law).

96. Steele, *supra* note 29, at 942.

embedded information in the course of negotiation, due diligence, investigation, and litigation.[97] Metadata may reflect strategy considerations, legal issues, legal advice, or editorial comments.[98] While not all information may reveal confidences or secrets, such privileged information may be revealed, which could be either embarrassing or a detriment to the client.[99]

a. Document Preparation

One potential problem occurs in the production of documents and communications via electronic media.[100] Attorneys frequently prepare documents or pleadings with templates.[101] Templates retain all prior information, including metadata.[102] Therefore, a former client's name and information may be discovered in the original document.[103] If that same document is sent to either a new client or opposing counsel, the outcome could be not only humbling, but also result in a breach of the duty of confidentiality or a waiver of an attorney-client privilege.[104]

b. Contract Litigation

Other potential problems with metadata are likely to arise in contract negotiations where a multitude of attorneys will review a single electronic contract that undergoes a number of revisions from both sides of the table.[105] Frequently used revision tools, such as the "Insert Comment" function or the "Track Changes" function will memorialize changes and generate indefinite metadata.[106] Comments or changes may divulge negotiation strategies, debilitate bargaining power, and imperil attorney-client privileges.[107] As an example, the following illustrates a potential metadata disaster in the legal profession:

---

97. Stevens, *supra* note 2, at 9.

98. *See* N.Y. State Bar Ass'n Comm. on Ethics and Prof'l Responsibility, Formal Op. 749 (2001), *available at* http://www.nysba.org/AM/Template.cfm?Section=Home&section=Opinions_676_750&template=/CM/ContentDisplay.cfm&ContentFileID=3934 (concluding that an attorney may not ethically make use of computer technology to examine electronic documents to access confidences relating to another attorney's client).

99. *Id.*

100. Cole, *supra* note 64, at 8.

101. *Id.*

102. *Id.*

103. *Id.*

104. *Id.*

105. *Id.*

106. *Id.*

107. *Id.*

> Attorney A e-mails an electronic draft of a settlement agreement to her client for review. The settlement agreement is a modified form that Attorney A borrowed from a previous, unrelated matter with the same client. Unbeknownst to Attorney A, another attorney at her firm enabled the "Versions" feature of the document to assist with drafting another settlement in an unrelated matter.
>
> After reviewing the draft, the client makes several electronic edits and comments directly to the document. One of the client's comments indicates that, although she prefers to settle the matter at $75,000, she is prepared to go as high as $100,000. The client attaches the MS Word document with her edits and comments to an e-mail and sends it back. Attorney A reviews the client's comments, deletes the reference to the settlement parameters, and finalizes the changes.
>
> Without cleaning up the metadata, Attorney A e-mails the document to opposing counsel, Attorney B, for approval. Attorney B accesses the metadata in the document and reviews the prior versions, edits, and authors of the document. Attorney B now knows the client's monetary settlement limits, what changes the client wanted made to the document, and even what terms and conditions the client agreed to in prior settlements.[108]

Unfortunately, this apparently innocuous exchange of an electronic document resulted in a metadata disaster.[109]

c. Electronic Discovery

"E-discovery," in the discovery phase of litigation, is known as the production of electronic documents.[110] However, e-discovery "has been an ongoing thorn in the side of the federal judiciary," while judges and litigants strive to keep up with technological innovations.[111] With the arrival of the digital age, the "legal landscape has unquestionably changed[,]" but the purposes of discovery are still to narrow and refine issues.[112] As a result, the new "digital litigator" must adapt to the electronic age.[113] Indeed, it is now commonplace to rely on e-discovery of digital data in lieu

108. Zall, *supra* note 23, at 56.

109. *Id.*

110. Salvatore Joseph Bauccio, *E-Discovery: Why and How E-mail Is Changing the Way Trials are Won and Lost*, 45 DUQ. L. REV. 269, 269 (2007) .

111. *Id.*

112. Favro, *supra* note 22, at 3.

113. *Id.*

of paper documents, which radically changes discovery.[114] Moreover, courts have been known to reject attempts to provide paper documents instead of digital data.[115]

However, pursuant to e-discovery demands, parties risk the disclosure of unknown embedded data.[116] The consequences include inadvertent disclosure of trade secrets, proprietary information, and attorney-client privileged data.[117] In addition, the disclosure of attorney-client privileged information may result in a waiver of the privilege.[118] In fact, courts have employed considerably different approaches to decide whether an inadvertent disclosure of client confidences waives the attorney-client privilege.[119] Thus, while the law is adapting to meet the problems of metadata within electronic discovery, courts disagree on the issue.[120] In *Williams v. Sprint/United Management Co.*,[121] the court prescribed the modern standard for the electronic discovery of metadata by holding that the producing party shall produce the electronic documents with metadata intact unless such party invokes a protective order.[122]

Courts are not the only authority to have addressed the issue of metadata in e-discovery.[123] In fact, "there is hope on the horizon" as the

---

114. Beckerman-Rodau, *supra* note 33, at 6.

115. *Id.* at 7. *But see* Brandon, *supra* note 49, at 2 (stating that some court rules, such as California Rule of Court 342(i), mandate electronic brief filing).

116. Beckerman-Rodau, *supra* note 33, at 6.

117. *Id.*

118. *Id.*

119. *See* Steele, *supra* note 29, at 917-18 (outlining the three different approaches taken by the court). The "strict approach" holds that the disclosure of attorney-client privileged data is a waiver of that privilege. *Id.* The "lenient approach" holds that a waiver requires intent to release a right, but an inadvertent disclosure lacks intent because, by definition, it is unknowing. *Id.* at 920. The "circumstances approach" probes factors as to whether reasonable precautions were employed to protect the privilege. *Id.* at 918.

120. *See, e.g.*, Ky. Speedway, LLC v. NASCAR, No. 05-138-WOB, 2006 U.S. Dist. LEXIS 92028, at *22-23 (E.D. Ky., Dec. 18, 2006) (articulating a presumption against the production of metadata in electronic discovery); Wyeth v. Impax Lab., Inc., No. 06-222-JJF, 2006 U.S. Dist. LEXIS 79761, at *4-5 (D. Del. Oct. 26, 2006) (finding that the emerging trend is against the electronic discovery of metadata). These courts did not address the issue of whether metadata may be precluded from discovery production as either work-product or privileged information. *See* Thomas V. Laprade, *Can–Should–*FDIC v. Singh *Survive the Amendments to the Federal Rules of Civil Procedure?*, 22 ME. B. J. 86, 89 (2007) (pointing out that these courts only relied on "emerging standards of electronic discovery" and did not address the exclusion of metadata from work product or privileged information). *But see* Hagenbuch v. 3B6 Sistemi Elettronici Industriali S.R.L., No. 04 C 3 109, 2006 U.S. Dist. LEXIS 10838, at *8-9, 12 (D. Ill. Mar. 8, 2006) (ordering the production of metadata within electronic media); Williams v. Sprint/United Mgmt. Co., 230 F.R.D. 640, 656 (D. Kan. 2005) (concluding that metadata should remain intact in the production of electronic documents).

121. 230 F.R.D. 640 (D. Kan. 2005).

122. *Williams*, 230 F.R.D. at 656.

123. *See generally* Derek S. Witte & D. Andrew Portinga, *E-Discovery and the New Federal Rules of Civil Procedure: They Apply to You*, 86 MICH. B. J. 36, 37-40 (2007) (providing recent

Federal Rules of Civil Procedure and the Federal Rules of Evidence meet the realities of e-discovery.[124] After approval by the United States Supreme Court, the proposed amendments to the Federal Rules of Civil Procedure, which directly address the discovery of electronically stored information including metadata, took effect as of December 1, 2006.[125] These rules provide much needed explicit guidance and take an affirmative step toward acknowledging the complexity of electronic discovery.[126] Therefore, recent court decisions that uphold the value of metadata to ensure the integrity and reliability of documents have set a trend that will continue with the amendments to the Federal Rules of Civil Procedure, thus compelling a presumption as to the preservation and production of pertinent metadata.[127]

In short, metadata is managed nearly every day in the legal profession.[128] The ramifications of metadata run the gamut from embarrassment to malpractice.[129] Nonetheless, the ethical obligations regarding the handling of metadata in the legal profession are either nonexistent or are inconsistent amongst the states.[130]

B. THE CURRENT LAW APPLICABLE TO METADATA

The advent of technological advancements has opened a "Pandora's Box" of ethical issues in the practice of law.[131] Attorneys within their respective states are required to adhere to ethical rules of professional conduct as promulgated by their state bar associations.[132] State bar associations use the ABA Model Rules of Professional Conduct or the Model Code of Professional Responsibility as a guide when establishing rules regarding

---

court decisions and a detailed overview of how the "e-discovery amendments" endeavor to address difficulties that electronically stored evidence presents in discovery).

124. Kathleen Peterson & Todd Nunn, *Electronic Discovery, Inadvertent Production and the New Federal Rules*, 48 ORANGE COUNTY LAW. 14, 14 (2006).

125. *See* Witte & Portinga, *supra* note 123, at 37 (noting that the amendments altered Rules 16, 26, 33, 34, 37, and 45 of the Federal Rules of Civil Procedure).

126. Peterson & Nunn, *supra* note 124, at 16. The rules set the framework, but the parties must use the rules as tools for protection. *Id.*

127. *See generally* Favro, *supra* note 22, at 5, 17-21 (discussing the impact and consistency of the amendments, as well as case law regarding metadata preservation and production). The amendments do not explicitly address metadata preservation and production, but instead provide general guidance. *Id.* at 18. However, several pre-2006 decisions set the current theme of "document integrity" for the preservation and production of metadata. *Id.* at 13.

128. Nelson & Simek, *supra* note 4, at 28.

129. *Id.*

130. *See generally* Steele, *supra* note 29, at 943-47 (providing an overview of how the ABA and a few states have reacted to the ethical implications materializing from the inadvertent disclosure of metadata).

131. *See generally id.* at 927, 942-47 (discussing how metadata vastly impacts ethical obligations on both the disclosing and receiving attorney).

132. Newman, *supra* note 24, at 6.

ethical conduct.[133] Thus, each state may have different ethical rules, but generally all states' rules parallel the ABA Model Rules.[134]

While the ABA Model Rules do not specifically address metadata, they do provide guidance regarding ethical norms in the legal profession and provide a structure in which to consider metadata concerns.[135] However, a few states have issued ethics opinions which are persuasive to the legal profession as to the handling of metadata.[136] Additionally, other state ethics opinions have addressed technological issues in general, which may aid the interpretation of metadata issues in the near future.[137]

1. *ABA Model Rules of Professional Conduct*

In addressing metadata concerns, the ABA Model Rules do not provide a black-letter rule.[138] Rather, these rules only provide guidance as to ethical standards.[139] The following ABA Model Rules touch on ethical issues pertinent to metadata.[140]

---

133. Steele, *supra* note 29, at 927.

134. *See, e.g.*, Robert A. Creamer & Thomas P. Luning, *An Introduction to the Proposed New Illinois Rules of Professional Conduct*, 17 CBA REC. 25, 25 (2003) (stating that Illinois and at least forty-two other states have adopted the ABA Model Rules in some form).

135. Newman, *supra* note 24, at 2.

136. *Id.* The authoritative status of ethics opinions may vary from state to state; however, generally they are advisory and not binding on attorneys, although an attorney following the opinion may be entitled to protection from discipline. Interview with Alice R. Senechal, Attorney, Robert Vogel Law Office, in Grand Forks, N.D. (Feb. 13, 2008) [hereinafter Interview with Senechal].

137. *Id. See, e.g.*, Colo. State Bar Ass'n Comm. on Ethics and Prof'l Responsibility, Formal Op. 108 (2000) (discussing the inadvertent disclosure of confidential or privileged documents); Alaska State Bar Ass'n Comm. on Ethics and Prof'l Responsibility, Formal Op. 98-2 (1998) (concluding that attorneys are free to communicate by e-mail, but should caution clients that the communication is not absolutely secure); Ohio State Bar Ass'n Comm. on Ethics and Prof'l Responsibility, Formal Op. 99-2 (1999) (finding that attorneys do not violate an ethical duty by communicating through e-mail without encryption).

138. Newman, *supra* note 24, at 2.

139. *Id.*

140. *See generally* Hricik, *Mining for Embedded Data*, *supra* note 11, at 237-40 (indicating the significance of Model Rule 4.4(b) as it relates to the inadvertent disclosure of documents containing metadata); 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); Newman, *supra* note 24, at 6-9 (noting that Model Rules 1.6 and 8.4 are related to the issue of metadata).

a. Model Rules 1.1 and 1.3

ABA Model Rule 1.1 provides: "A lawyer shall provide *competent* representation to a client."[141] In addition, Model Rule 1.3 provides: "A lawyer shall act with reasonable *diligence* . . . in representing a client."[142] Every technological advancement impacting the practice of law amplifies the definitions of both competence and diligence.[143] The practice of law, at a minimum, implores attorneys to establish the basics of online research to access recent changes and developments in the law.[144] Those attorneys that transfer information electronically must identify and react to security concerns.[145] In addition, attorneys must acknowledge "information architecture" and advise clients about document disclosure and retention.[146] Therefore, attorneys must understand that metadata is stored within the majority of electronic files and take the appropriate action to protect digital data.[147]

b. Model Rule 1.6

ABA Model Rule 1.6 provides: "A lawyer shall not reveal information relating to the representation of a client."[148] This rule is the platform in regard to the attorney-client privilege and the duty to preserve client confidences.[149] Therefore, it is proposed that by the "very hidden nature of metadata, the inadvertent disclosure of a client's secret adverse to his interest would go to the heart of this rule."[150]

Moreover, the comments to Model Rule 1.6 are apposite to the concept of creating metadata and protecting client confidences.[151] Comment 2 emphasizes trust as the hallmark of the attorney-client relationship by encouraging full and frank communication to an attorney, including embarrassing

141. MODEL RULES OF PROF'L CONDUCT R. 1.1 (2002), *available at* http://www.abanet.org/cpr/mr pc/mrpc_toc.html (emphasis added).

142. *Id*. at 1.3.

143. Cahill, *supra* note 140, at 4.

144. *Id*.

145. *Id*.

146. *Id*.

147. *Id*.

148. MODEL RULES OF PROF'L CONDUCT R. 1.6 (2002), *available at* http://www.abanet.org/cpr/mr pc/mrpc_toc.html.

149. Newman, *supra* note 24, at 6.

150. *Id*.

151. MODEL RULES OF PROF'L CONDUCT R. 1.6 (2002), *available at* http://www.abanet.org/cpr/mr pc/mrpc_toc.html. *See* Newman, *supra* note 24, at 7 (pointing out that the comments to Model Rule 1.6 are germane to the issue of metadata).

or even legally damaging material.[152] Electronic communication is increasingly imperative to the attorney-client relationship.[153] Therefore, adverse consequences of metadata disclosure are reasonably foreseeable to an attorney.[154]

Comment 4 provides that Model Rule 1.6 prohibits "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."[155] Thus, the comment suggests that attorneys should take appropriate measures to eliminate sensitive metadata from documents or work related to all client representations.[156]

Comment 16 reinforces that an attorney "must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation."[157] This comment is interpreted to make an attorney responsible for the actions of those under his supervision in order to ensure that a client's information is preserved and protected.[158] As applied to the concept of metadata, the attorney is solely responsible for any documents or files electronically sent out at his or her direction.[159] Therefore, under Model Rule 1.6, it is imperative that attorneys, as well as their office professionals, understand the risks associated with metadata and employ appropriate precautions to prevent the disclosure of sensitive metadata.[160]

c. Model Rule 8.4

ABA Model Rule 8.4 provides: "It is professional misconduct for a lawyer to . . . engage in conduct involving dishonesty, fraud, deceit, or

152. MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 2. (2002), *available at* http://www.abanet.org/cpr/mrpc/mrpc_toc.html. *See* Newman, *supra* note 24, at 7 (highlighting the relation of metadata to Comment 2 of Model Rule 1.6).

153. Newman, *supra* note 24, at 7.

154. *Id.*

155. MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 4 (2002), *available at* http://www.abanet.org/cpr/mrpc/mrpc_toc.html. *See* Newman, *supra* note 24, at 7 (finding that Comment 4 "parlays the metadata concern" whereas Model Rule 1.6(a) applies to disclosures that could lead to discovery of protected information by a third party).

156. Newman, *supra* note 24, at 7-8.

157. MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 16 (2002), *available at* http://www.abanet.org/cpr/mrpc/mrpc_toc.html. *See* Newman, *supra* note 24, at 8 (stating that Comment 16 accentuates the importance of safeguarding a client's information in competent representation).

158. Newman, *supra* note 24, at 8.

159. *Id.*

160. *Id.*

misrepresentation."[161] This rule arguably speaks to the acceptability of "mining" metadata, or reading another's metadata and looking for client confidences or secrets.[162] In reality, it is a good example of professional misconduct for an attorney to "mine" the metadata of an electronic document and use the information gained to his or her client's favor.[163] One would likely consider such conduct to be dishonest and "not within the norms of the [legal] vocation."[164]

While zealous representation of a client is likely to lure an attorney to "mine" electronic documents for advantages, reviewing metadata would be in violation of opposing counsel's work product privilege.[165] The result is an unfair advantage to the attorney's client.[166] In addition, it would appear deceitful to any third party observant.[167] However, as this note explains, authorities are split as to the concept of dishonesty within the meaning of Model Rule 8.4(c) when viewing embedded confidential data.[168]

d. Model Rule 4.4

ABA Model Rule 4.4(b) provides: "A lawyer who receives a document relating to the representation of the lawyer's client and knows or reasonably should know that the document was inadvertently sent shall promptly notify the sender."[169] This rule is also applicable to electronic modes of transmission that will be read or transferred into a readable form.[170] However, Rule 4.4(b) does not address whether an attorney must or should refrain from reading into or looking at the document.[171] Rather, the rule only imposes the obligation of notice.[172] Comment 2 explains that the purpose of the notice is to allow the sending attorney to take protective measures, but whether additional steps are required by the recipient attorney is beyond the

161. MODEL RULES OF PROF'L CONDUCT R. 8.4 (2002), *available at* http://www.abanet.org/cpr/mr pc/mrpc_toc.html.

162. Newman, *supra* note 24, at 8.

163. *Id*. at 8-9.

164. *Id*. at 9.

165. *Id*.

166. *Id*.

167. *Id*.

168. Hricik, *Mining for Embedded Data*, *supra* note 11, at 242. *See* discussion *infra* Part II.B.2.a (noting the split in authorities as to the ethical obligations of the receiving attorney).

169. MODEL RULES OF PROF'L CONDUCT R. 4.4 (2002), *available at* http://www.abanet.org/cpr/mrpc/mrpc_toc.html.

170. *Id*.

171. *Id*. *See* Hricik, *Mining for Embedded Data*, *supra* note 11, at 237 (indicating that notice is the only requirement imposed by Model Rule 4.4(b)).

172. MODEL RULES OF PROF'L CONDUCT R. 4.4 (2002), *available at* http://www.abanet.org/cpr/mr pc/mrpc_toc.html. *See* Hricik, *Mining for Embedded Data*, *supra* note 11, at 237 (imposing only the requirement of notice within Model Rule 4.4(b)).

scope of the Model Rules.[173] Comment 3 also indicates that since the recipient attorney is not mandated by law to return the document unread, the decision to return the document voluntarily is a matter of professional judgment reserved to the attorney.[174] While this rule was drafted in response to the issue of inadvertent faxes, the theory is that it should also apply to situations involving metadata where the receiving attorney knows or should know that the embedded data was sent inadvertently.[175]

It is imperative to clarify the difference between what is done inadvertently versus what is done intentionally because ethical obligations under Model Rule 4.4(b) only arise in the presence of inadvertence.[176] An analogy between transmitting metadata intentionally and inadvertent transmissions is obvious: an attorney intentionally sends a contract to the opposing attorney, but inadvertently includes a mark-up of the contract, which contains comments received from the client.[177] Thus, the lawyer intentionally transmitted the contract, but by no means intended to transmit the mark-up.[178] The difference is that the metadata is not a separate file, "but is 'in' the intentionally sent file."[179] Thus, the transmission of embedded data is inadvertent.[180] Therefore, if a state bar follows ABA Model Rule 4.4(b), it is a logical argument that the attorney receiving the file with metadata must not examine the data, and should notify the sender.[181]

However, the ABA found that a receiving attorney is free to "mine" and use embedded data, even if electronic documents were provided by the opposing attorney.[182] According to the ABA, the receiving attorney 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.[183] The ABA recognized that its stance is contrary to various legal

---

173. MODEL RULES OF PROF'L CONDUCT R. 4.4 cmt. 2 (2002), *available at* http://www.abanet.org/cpr/mrpc/mrpc_toc.html.

174. *Id*. at 4.4 cmt. 3.

175. Steele, *supra* note 29, at 947.

176. Hricik, *Telling Lies*, *supra* note 44, at 98.

177. *Id*. at 99.

178. *Id*.

179. *Id*.

180. *Id*.

181. *Id*. *See* discussion *infra* Part II.B.2.a (expanding on New York's agreement with the conclusion that the recipient attorney must notify the sending attorney).

182. *See* ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 06-442 (Aug. 5, 2006), *available at* http://www.pdfforlawyers.com/files/06_442.pdf (providing the ABA's view on the issue of metadata); *see also* Williams, *supra* note 6, at 48 (noting the importance of stripping metadata based on the ABA's conclusion).

183. ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 06-442 (Aug. 5, 2006), *available at* http://www.pdfforlawyers.com/files/06_442.pdf. *See Gleaning Advantage From Metadata OK, Says ABA*, CONSUMER FIN. SERVS. L. REP., Nov. 29, 2006 [hereinafter *Gleaning*

ethics opinions, which find it impermissible and dishonest to search documents with metadata.[184] However, the ABA held that the single provision relevant to the concept of metadata only mandates the receiving attorney to notify the sender when he or she knows or should know that the document was inadvertently sent.[185] In addition, the ABA committee made clear that the opinion did not address circumstances where documents are received "through criminal, fraudulent, deceitful, or otherwise improper conduct."[186]

Nevertheless, the inadvertent disclosure of client confidences, in the form of metadata, may result in a waiver of attorney-client privilege or work-product protection.[187] The disclosure may also result in a breach of the duty of confidentiality.[188] Moreover, depending on which state an attorney practices, the act of inadvertently disclosing client confidences or the act of "mining" metadata may be an ethical violation.[189]

2. *State Bar Associations*

Despite the fact that the ABA Model Rules of Professional Conduct have failed to specifically address metadata concerns, states have taken their own initiative.[190] A few states have issued their own respective ethics opinions, which impose ethical obligations on both the sending and receiving attorneys.[191] Thus, these ethics opinions provide guidance to attorneys nationwide as to the appropriate conduct in dealing with the dangers of metadata.[192]

Advantage] (discussing the effect of the ABA's report which found it acceptable for the receiving attorney to use metadata).

184. ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 06-442 (Aug. 5, 2006), *available at* http://www.pdfforlawyers.com/files/06_442.pdf. *See* Williams, *supra* note 6, at 48 (noting the implications of the ABA's ruling that receiving attorneys are free to use metadata).

185. ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 06-442 (Aug. 5, 2006), *available at* http://www.pdfforlawyers.com/files/06_442.pdf. *See* Williams, *supra* note 6, at 48 (addressing the ABA's comment that the recipient attorney does not need to return the document).

186. ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 06-442 (Aug. 5, 2006), *available at* http://www.pdfforlawyers.com/files/06_442.pdf. *See Gleaning Advantage*, *supra* note 183 (pointing out what the ABA ethics opinion did not address).

187. Steele, *supra* note 29, at 913.

188. *Id.*

189. *Id.* at 913, 926.

190. *See* discussion *supra* Part II.B.1.a-d (outlining the ABA Model Rules indirectly relating to metadata and noting the ABA's view on the dangers of metadata).

191. *See* discussion *infra* Part II.B.2.a-c (showing how a growing number of states have set the trend by imposing ethical obligations as a solution to the metadata issue).

192. *Id.* *See* Interview with Senechal, *supra* note 136 (noting that the authoritative status of ethics opinions varies).

a. New York's Opinion Sets the Trend

In 2001, New York set the trend and became the first state to address the issue of metadata.[193] New York Opinion 749 concluded that "[a] lawyer may not make use of computer software applications to surreptitiously 'get behind' visible documents or to trace e-mail."[194] The opinion reasoned that the use of technology to "mine" electronic documents to access confidential information, as well as work-product, "violate[s] the letter and spirit" of ethical obligations.[195] This opinion also recognized that the sending party intends to transmit the "visible" electronic document, but absent an unequivocal direction to the opposite, counsel does not intend the recipient counsel to receive the "invisible" information.[196]

New York characterizes the unintentional disclosure of metadata as "inadvertent" and the subsequent review of it as deliberate, such that the recipient may not access the embedded data.[197] It is not the carelessness of the sending attorney, but rather a deliberate act by the recipient attorney that leads to the disclosure of client confidences.[198] Thus, the recipient attorney who receives files with metadata would know, or at least should know, that the embedded data was not transmitted intentionally.[199] In short, as to the question of whether embedded data is inadvertently transmitted, the authorities are split because, as previously discussed, the ABA rejected the proposal that metadata is always sent unintentionally.[200]

In addition, New York recognized that to "mine" for metadata is dishonest.[201] However, the ABA disagreed.[202] Rather, the ABA found it was not dishonest to review embedded data inadvertently sent by another attorney.[203] This conclusion is untenable because the ABA assumes it is a well-known concept that electronic documents contain embedded data, and such data is retrieved in a comprehensible form.[204] This assumption fails

193. N.Y. State Bar Ass'n Comm. on Ethics and Prof'l Responsibility, Formal Op. 749 (Dec. 14, 2001), *available at* http://www.nysba.org/AM/Template.cfm?Section=Home&section=Opinions_676_750&template=/CM/ContentDisplay.cfm&ContentFileID=3934.

194. *Id*.

195. *Id*.

196. *Id*. *See* Hricik & Jueneman, *supra* note 60, at 18 (discussing the New York opinion as recognizing the fact that the sending attorney unintentionally discloses metadata).

197. Hricik, *Telling Lies*, *supra* note 44, at 99.

198. *Id*.

199. Hricik, *Mining for Embedded Data*, *supra* note 11, at 239.

200. *Id*. at 239-40. *See* discussion *supra* Part II.B.1.d. (discussing inadvertent versus intentional transmissions).

201. Hricik, *Mining for Embedded Data*, *supra* note 11, at 245.

202. *Id*. at 244-45.

203. *Id*.

204. *Id*. at 245.

because the majority of attorneys in small firms or solo practice are unaware of the existence of metadata.[205] Moreover, the assumption does not alter the fact that embedded data will be sent only when an attorney makes a mistake or, in other words, through an inadvertent transmission.[206] No attorney intentionally sends confidential information to opposing counsel.[207] Nevertheless, the ABA concludes it is not dishonest to "mine" for metadata.[208] Thus, New York contributes to a split in authority with regard to the issue of whether "mining" for metadata is dishonest.[209]

In 2004, New York addressed the issue of inadvertently transmitting metadata by issuing Opinion 782.[210] This opinion imposed a duty on lawyers to utilize reasonable care to prevent the disclosure of confidential material contained in metadata within documents sent electronically to opposing counsel.[211] New York noted that not all metadata contains confidences or secrets but such embedded data in particular circumstances could reveal confidential information resulting in embarrassment or detrimental consequences to a client.[212]

The opinion provided that reasonable care will depend on the circumstances, but includes: (1) the document subject matter; (2) whether there were comments on multiple drafts from different sources; (3) whether the document was a template; and (4) the identity of the intended recipient.[213] Moreover, "reasonable care" may require an attorney to "stay abreast of technological advances" and the risks involved with electronic transmissions.[214] Thus, attorneys who use technology have an ethical obligation to be familiar with technology to avoid harming clients.[215] New York was the first state to address ethical obligations in regard to metadata, and other states have followed the trend.[216]

---

205. *Id*. at 246. Significantly, a study conducted in late 2004 reported that "only 43% of respondents were aware that embedded data even existed." *Id*.

206. *Id*.

207. *Id*.

208. *Id*. at 245.

209. *Id*. at 242, 245.

210. Mierzwa, *supra* note 7, at 55.

211. N.Y. State Bar Ass'n Comm. on Ethics and Prof'l Responsibility, Formal Op. 782 (2004), *available at* http://www.nysba.org/AM/Template.cfm?Section=Ethics_Opinions&CONTENTID=6871&TEMPLATE=/CM/ContentDisplay.cfm.

212. *Id*.

213. *Id*.

214. *Id*.

215. Brandon, *supra* note 49, at 2.

216. *See* Fla. State Bar Ass'n Comm. on Ethics and Prof'l Responsibility, Formal Op. 06-2 (2006), *available at* http://www.floridabar.org/tfb/TFBETOpin.nsf/b2b76d49e9fd64a5852570050067a7af/0a1b5e3a86df495a8525714e005dd6fd?OpenDocument (establishing an ethics opinion

b. Florida Follows the Opinion of New York

In 2006, Florida became the second state to test the issue of metadata.[217] As stated by a Florida Bar Board of Governor member, "I have no doubt that anyone who receives a document and mines it . . . is unethical, unprofessional, and un-everything else."[218] Florida analogized "mining" metadata to "rifling through someone's briefcase."[219]

In order to illustrate the critical issue of "mining" for metadata, the Florida Bar Board of Governors provided an example.[220] A senior partner and President of the Florida Bar was working on a brief requested by another firm.[221] The firm asked that the brief be e-mailed instead of faxed, and when the firm received it they "mined" it for metadata.[222] They found a historical sequence of each and every modification to the document, including communications to the client.[223]

The Florida Bar Executive Director implored the board to remember that the problem with metadata will only grow as the practice of law increasingly relies on electronic data.[224] For example, he noted that the following year the Florida Supreme Court would require attorneys to file all documents electronically.[225] As a result of their findings, the Florida Professional Ethics Committee resolved two critical issues: (1) whether it is unethical for the recipient attorney to "mine" metadata from an electronic document received from the sending attorney; and (2) whether the sending attorney has an ethical obligation to take reasonable precautions to ensure that metadata is removed prior to transmitting electronic documents.[226] Thus, the State of Florida, like New York, imposed a corresponding duty on

---

consistent with the New York approach, which imposes reciprocal ethical duties on the sending and receiving attorney).

217. *Id.*

218. *See generally* Gary Blankenship, *What's in Your Document? Board Says It's Unethical to Mine Hidden Data From E-texts*, Jan. 1, 2006, http://www.floridabar.org/DIVCOM/JN/jnnews01.nsf/0/c3f75b4e10e94f78852570e50051b23e?OpenDocument# (discussing the Florida Bar Board of Governors' view on the "mining" of metadata). In contemplating whether an ethics opinion or bar rule was necessary to regulate the "mining" of metadata, the board "voted unanimously for a motion to express its sentiment that metadata mining is something lawyers should not do." *Id.*

219. Jonathan Hauer, *Metadata: The Invisible Threat*, ARIZ. EMP. L. LETTER, July 2007, at 1.

220. Blankenship, *supra* note 218.

221. *Id.*

222. *Id.*

223. *Id.*

224. *Id.*

225. *Id.*

226. Fla. State Bar Ass'n Comm. on Ethics and Prof'l Responsibility, Formal Op. 06-2 (2006), *available at* http://www.floridabar.org/tfb/TFBETOpin.nsf/b2b76d49e9fd64a5852570050067a7af/0a1b5e3a86df495a8525714e005dd6fd?OpenDocument.

both the sending and receiving lawyer. [227] However, Florida is not the last state to uphold this trend.[228]

c. Alabama's Opinion Follows the Trend

Alabama joined the movement of imposing corresponding ethical obligations.[229] As of March 2007, Alabama issued Ethics Opinion RO-2007-02 in regard to both the disclosure and "mining" of metadata.[230] The holding of this opinion is consistent with New York Opinions 749 and 782 and Florida Opinion 06-2.[231] Alabama answered the following two issues in the affirmative: (1) whether under Rule 1.6 attorneys have a duty to use reasonable care when sending electronic documents in order to prevent disclosure of metadata containing confidential information of clients; and (2) whether in the absence of express authorization from the court, it is impermissible for an attorney to "mine" metadata in an electronic document that he or she inadvertently received from another party.[232]

In regard to the former issue, whether an attorney exercises reasonable care depends on the circumstances of each case.[233] Alabama, like New York, employed the same factors in order to determine "reasonable care."[234] These factors included the following: (1) the scope and/or nature of the metadata; (2) the steps taken to prevent the disclosure of metadata; (3) the subject of the document; and (4) the intended recipient.[235] As for the latter issue, the use of digital technology to "mine" client confidences revealed in metadata is "an impermissible intrusion on the attorney-client relationship" and an ethical violation of the Rules of Professional of Conduct.[236]

Alabama emphasized that confidentiality is the central tenet of the attorney-client relationship.[237] Alabama agreed with New York that "mining" for metadata is a deliberate attempt by the receiving attorney to access confidential information in order to obtain an unfair advantage against

---

227. *Id.*

228. *See* Ala. State Bar Ass'n Comm. on Ethics and Prof'l Responsibility, Formal Op. RO-2007-02 (2007), *available at* http://www.alabar.org/ogc/PDF/2007-02.pdf (finding a solution to the metadata issue by imposing ethical obligations on attorneys).

229. *Id.*

230. *Id.*

231. *Id.*

232. *Id.*

233. *Id.*

234. *Id.* *See supra* text accompanying note 212 (listing the factors New York used in determining whether "reasonable care" was utilized).

235. *Id.*

236. Ala. State Bar Ass'n Comm. on Ethics and Prof'l Responsibility, Formal Op. RO-2007-02 (2007), *available at* http://www.alabar.org/ogc/PDF/2007-02.pdf.

237. *Id.*

opposing counsel.[238] Thus, the "mining" of metadata to uncover confidential information would constitute misconduct.[239]

Alabama is not the last state to impose corresponding ethical obligations on the sending and receiving attorney; most recently Arizona joined the trend-setting jurisdictions.[240] In fact, in the next three to four years, an explosion of ethics opinions is expected.[241] In addition, other jurisdictional opinions are persuasive on the issue of metadata.[242]

d. Other Jurisdictions

The majority of the remaining states have not directly addressed the issue of metadata; however, they have indirectly addressed similar issues pertaining to prior technological issues.[243] These opinions could be analogized with that of New York, Florida, Alabama, and Arizona.[244] It is commonly suggested that as technology and knowledge of its capacity continue to change, those governing the conduct of the legal profession will need to remain adaptable.[245]

On the other hand, a minority of states take the counter position.[246] For example, Oklahoma and California bar association seminars teach attorneys how to find metadata.[247] In addition, the Maryland State Bar Association's Committee on Ethics concluded, like the ABA, that it would not be an ethical violation for an attorney to look at metadata received from opposing counsel.[248] One critic argued that it would be unfair to punish those that know how to use technology well and reward others for not learning how to use technology.[249]

Nevertheless, the rules and the law need to change with technology.[250] Thus, the positions of various jurisdictions should adapt quite rapidly.[251]

---

238. *Id.*

239. *Id.*

240. *See* Ariz. State Bar Ass'n Comm. on Ethics and Prof'l Responsibility, Formal Op. 07-03 (2007), *available at* http://www.myazbar.org/Ethics/opinionview.cfm?id=695 (holding that the sending attorney must take reasonable actions to prevent inadvertent disclosure and the recipient attorney may not examine electronic communications for the purpose of finding metadata).

241. Marcia Coyle, *'Metadata' Mining Vexes Lawyers, Bars*, NAT'L L.J., Feb. 18, 2008, *available at* http://www.law.com/jsp/nlj/PubArticleNLJ.jsp?id=1203075904115.

242. Newman, *supra* note 24, at 10.

243. *Id.*

244. *See, e.g., id.* (listing a number of website links to state ethics opinions, which indirectly address technological issues akin to metadata).

245. Cahill, *supra* note 140, at 3-4.

246. Williams, *supra* note 6, at 49.

247. *Id.*

248. Krause, *supra* note 10, at 32.

249. *Barring Metadata*, INSIDECOUNSEL (InsideCounsel, Chicago, Ill.), July 2006, at 1.

250. Cahill, *supra* note 140, at 3.

With inconsistencies amidst the jurisdictions and no bright-line rule to assist as a guideline to individual states, a valid proposal is needed to bring ethical conduct in line with the metadata issues found in the electronic practice of law.[252]

C. PROPOSING A NEW RULE FOR THE ABA MODEL RULES OF PROFESSIONAL CONDUCT

"Metadata is an ever-present threat" to the practice of law, and heavily impacts an attorney's ethical obligations.[253] The threat of metadata was reiterated by an attorney specializing in computer law and professional liability, in which it was concluded:

> Given the undeveloped nature of the law, the continually evolving technology, the exponential dependence on the Internet to communicate and the potentially catastrophic impact of inadvertent disclosure of a client's secrets or confidence, the issue of metadata protection is likely to continue to plague unwary practitioners and inflate the cost of transaction and litigation representation.[254]

Moreover, as one commentator noted, "[i]mposing an obligation on lawyers to remove confidential information from electronic documents and prohibiting them from mining for such hidden information seems to be preferable to engaging in a high-tech free-for-all."[255]

At this point in time, there are two ethical issues in regard to metadata.[256] The first issue is whether the sending attorney has an affirmative duty to take reasonable precautions to ensure that metadata is protected from inadvertent disclosure or inappropriate production by an electronic document before it is sent.[257] The second issue is whether it is unethical for the recipient attorney to "mine" metadata from an electronic document

---

251. *Id*. at 3-4.

252. *Id*. *See* Brandon, *supra* note 49, at 2 (noting that the standard of care must change as technology changes).

253. Steele, *supra* note 29, at 942.

254. Shari Claire Lewis, *Reckoning With Metadata*, N.Y. L.J., Dec. 19, 2005, *available at* http://www.law.com/jsp/law/sfb/lawArticleFriendlySFB.jsp?id=1134727515889.

255. John Levin, *Legal Ethics: What to Do With Metadata*, 21 CBA REC. 68, 68 (June/July 2007).

256. Steele, *supra* note 29, at 942.

257. *See* Ala. State Bar Ass'n Comm. on Ethics and Prof'l Responsibility, Formal Op. RO-2007-02 (2007), *available at* http://www.alabar.org/ogc/PDF/2007-02.pdf (providing the first issue pertinent to the reasonable care of sending attorney).

received from the sending attorney.[258] The problem surrounding these issues is that the authorities are split.[259]

As previously discussed, a growing number of states have answered the issues in the affirmative; however, the ABA has not mandated a duty to "scrub" metadata, nor has it prohibited the "mining" of metadata.[260] In fact, the ABA re-evaluated the Rules of Professional Conduct but arguably failed to address metadata concerns.[261] Therefore, it is important that the ABA amend the current Model Rules, produce a new rule, or that individual states issue an ethics opinion establishing a duty to "scrub" metadata and prohibit the "mining" of metadata.[262] Moreover, from these duties flow ethical obligations imposed on both the sending and receiving attorney.[263]

1. *The ABA Commission on Evaluation of the Rules of Professional Conduct*

The ABA Commission on Evaluation of the Rules of Professional Conduct (Ethics 2000 Commission) was established in 1997 to evaluate the Model Rules.[264] Among the goals that motivated the Ethics 2000 Commission was the "impact of technology and globalization" and the creation of "national uniformity and consistency."[265] In 2000, the Ethics 2000 Commission proposed a number of significant modifications to the Model Rules and, in 2002, the ABA House of Delegates adopted the majority of the recommended changes.[266]

---

258. *See* Hricik, *Telling Lies*, *supra* note 44, at 80 (addressing the second issue metadata presents when lawyers receive a document with metadata); *see also* Steele, *supra* note 29, at 942, 945-47 (discussing the issue of viewing and using hidden embedded data to the recipient attorney's advantage).

259. *See* Hricik, *Telling Lies*, *supra* note 44, at 96 (noting that in a few jurisdictions the receiving attorney can use misdirected confidential information, while in other jurisdictions there is an ethical duty to provide notice to the sending attorney of the mistake); *see also* Steele, *supra* note 29, at 943 (indicating that because the concept of metadata is new, the ethical obligations have not been fully determined by state bars).

260. *See generally* discussion *supra* Part II.B.1.a-d (discussing the current ABA Model Rules pertaining to metadata); Part II.B.2.a-c (explaining the positions of New York, Florida, and Alabama on the concept of metadata).

261. *See* discussion *infra* Part II.C.1 (discussing the revisions to the Model Rules).

262. *See* discussion *infra* Part II.C.2-5 (advocating rules imposing ethical obligations to "scrub" and prohibit "mining").

263. *Id.*

264. Louise L. Hill, *Online Activities & Their Impact on the Legal Profession: Electronic Communications and the 2002 Revisions to the Model Rules*, 16 ST. JOHN'S J. LEGAL COMMENT 529, 531 (2002).

265. *Id.*

266. *Id.* at 531-32.

As previously mentioned in this article, individual states follow the ethical rules promulgated by the ABA.[267] Thus, as a result of the historical role the ABA has in developing a consensus on ethical standards for the legal profession, the Ethics 2000 Commission found it imperative to address the emerging trends amongst the states in which specific rules differed greatly.[268] In fact, the Ethics 2000 Commission incorporated state experimentations to create rules that would lend themselves to uniform adoption.[269] In addition, as a consequence of the ABA's decision to alter the Model Rules, states across the nation began to reevaluate and revise their own rules.[270]

While the revisions to the Model Rules provided much needed guidance in particular areas of the law, such as within the realm of technology, many lawyers today remain confused with issues relating to electronic communications.[271] The confusion of these lawyers is not likely to dissipate in the immediate future, because with the evolution of technology, new issues along with old will continue to face attorneys.[272] Therefore, arguably the Ethics 2000 Commission failed to address the ethical issue pertaining to metadata; it would be advantageous for the ABA to: (1) establish a duty to "scrub" metadata; and (2) prohibit the "mining" of metadata.[273]

2. *Advocating a Rule Establishing a Duty to "Scrub" Metadata*

"The lesson to be learned is that what general counsel don't know, or can't see, *can* hurt them."[274] Unfortunately, the majority of lawyers do not know that metadata exists.[275] Nevertheless, metadata is a risk that lawyers face in today's increasingly electronic law practice.[276] Indeed, one of the

---

267. *Id*. at 531.

268. Margaret Colgate Love, *The Revised ABA Model Rules of Professional Conduct: Summary of the Work of Ethics 2000*, 15 GEO. J. LEGAL ETHICS 441, 442 (2002).

269. *Id*.

270. *See* Hill, *supra* note 264, at 532 (noting that in light of the ABA's revision to the Model Rules, at least sixteen states are reevaluating their respective rules).

271. *Id*. at 550-51.

272. *Id*. at 551.

273. *See* discussion *supra* Part II.B.2.a-c (referring to states that have employed an affirmative ethical obligation on the sending and receiving attorney).

274. *See* Keith Ecker, *The Meta Monster: What General Counsel Can't See in a Document Could Cost Them*, INSIDECOUNSEL (InsideCounsel, Chicago, Ill.), July 2006, *available at* http://www.insidecounsel.com/section/department-management/534 (noting that ignoring metadata can cause costly and embarrassing results) (emphasis added).

275. Lewis, *supra* note 254. *See* Hricik, *Telling Lies*, *supra* note 44, at 91-92 (noting that scholars urge that "everybody" knows about metadata, but documents, which are posted by attorneys who should have been aware of metadata concerns, repeatedly end up on the web with embedded data).

276. Lewis, *supra* note 254.

top malpractice threats that attorneys are advised to avoid are the technological issues applicable to metadata.[277] This threat can be avoided through the use of various tools to remove metadata.[278] Furthermore, in the near future attorneys will be precluded from pleading ignorance of metadata.[279] Regardless of the facts suggesting attorneys have no knowledge of metadata, attorneys will be subject to negligence claims.[280] Moreover, if the significance of metadata and its implications on the practice of law have been elevated in some jurisdictions to the level of an ethical obligation, then it appropriately follows that the remainder of the jurisdictions and the ABA should take notice.[281]

Nevertheless, even in the absence of established ethical standards regarding metadata, attorneys should develop a habit of removing metadata prior to transmitting electronic documents.[282] However, it would be prudent if the ABA followed in the footsteps of New York, Florida, Alabama, and Arizona.[283] The ABA should set the standard for the remainder of the states by validating a duty on the sending attorney to "scrub" electronic documents.[284]

3. *The Sending Attorney's Ethical Obligations*

The sending attorney has the utmost duty to avoid disclosing embedded data containing client confidences and secrets.[285] However, if there is no metadata, there can be no transmission.[286] Thus, an attorney may refrain from intentionally or inadvertently sending embedded data by not creating it in the first instance.[287] Yet, to not create data means that attorneys could not take advantage of the benefits that metadata provides in the preparation

277. *Risk Management*, PARTNER'S REP. L. FIRM OWNERS (Inst. of Mgmt. & Admin., New York, NY), May 2007, at 1.

278. *Id*. *See* discussion *infra* Part II.C.3 (providing an explanation on how to remove metadata).

279. *See* Hricik, *Telling Lies*, *supra* note 44, at 92 ("[A]s awareness of embedded data spreads, it will become more difficult for lawyers to contend that transmitting embedded data did not violate the duty of care.").

280. *Id*.

281. Mierzwa, *supra* note 7, at 52.

282. Levitt & Rosch, *supra* note 52, at 41.

283. *See, e.g.*, Ala. State Bar Ass'n Comm. on Ethics and Prof'l Responsibility, Formal Op. RO-2007-02 (2007), *available at* http://www.alabar.org/ogc/PDF/2007-02.pdf (answering yes to an affirmative duty to use reasonable precautions to assure that confidential metadata is protected from inadvertent disclosure via electronic transmission).

284. *Id*.

285. Hricik, *Telling Lies*, *supra* note 44, at 89.

286. *Id*. at 93.

287. *Id*.

of electronic documents.[288] However, computer software programs may be altered to reduce the amount of metadata created.[289] In fact, Microsoft publishes a guideline to minimize metadata fields.[290] For example, "Fast Saves" can be turned off, comments in the "Comment" feature may be deleted, and changes made with the "Track Changes" feature can also be deleted prior to transmitting documents electronically.[291] A more practical method would be to "scrub" or remove metadata.[292]

There are various solutions to reduce or even eliminate embedded data, but the type of communication, such as confidential versus non-confidential, will set the standard for "reasonable care."[293] Microsoft provides a free feature for both Office 2003 and Windows XP, which removes metadata resulting from tools such as the "Track Changes" and "Comments" feature.[294] Yet according to experts, these free add-ons do not remove *all* metadata and are not foolproof.[295] In addition, software tools, which are described as "metadata scrubbers," remove almost all metadata.[296] However, the only version available for the Word Perfect program which provides a removal tool is "Version 13."[297]

Furthermore, converting a document to an Adobe Acrobat portable document file (PDF) format will still contain some metadata, but will not include embedded data.[298] Additionally, converting a document to an image PDF instead of a text PDF will preclude the recipient from manipulating the file "without jumping through hoops."[299] However, the safest

---

288. *Id*.

289. Cole, *supra* note 64, at 8.

290. *Id*.

291. Steele, *supra* note 29, at 948-49.

292. Hricik, *Telling Lies*, *supra* note 44, at 93.

293. *Id*.

294. Steele, *supra* note 29, at 948.

295. Levitt & Rosch, *supra* note 52, at 41. *See* Zall, *supra* note 23, at 58 (noting that Microsoft self-help solutions are not foolproof). An average computer user may neglect to spot an issue and experience difficulties in implementing Microsoft solutions. *Id*. In fact, Microsoft created a disclaimer that its proposed solutions are merely illustrative and without warranty for a specific purpose. *Id*.

296. *See, e.g*., Williams, *supra* note 6, at 49 (noting that software tools, such as ezClean, Workshare Protect, and Metadata Assistant are available for purchase to assist in removing metadata). These "scrubbing" tools go further into Microsoft's free features and practically eliminate metadata in Microsoft files. Steele, *supra* note 29, at 948. *See* Friedman, *supra* note 3, at 47-48 (pointing out that Metadata Assistant is found at www.payneconsulting.com and that it works with a variety of document management systems). The tool supposedly scans files and prompts users to remove metadata before the file leaves the office. *Id*. at 48.

297. Williams, *supra* note 6, at 49. An older version of Word Perfect will require writing a macro to remove metadata. *Id*.

298. *See* Hauer, *supra* note 219, at 1 (indicating that a PDF will still contain metadata, such as a date).

299. *Id*.

way to use PDF files is to print the original document and scan it in as a PDF file.[300] This method completely deletes all metadata from the original version, but is also quite time consuming.[301]

Another option is to simply agree with opposing counsel that transmitting embedded data is presumed unintentional and require the opposing party to return the file upon receipt.[302] In accordance with a written agreement that neither party will "mine" for metadata, both parties can benefit from sharing documents electronically.[303] Moreover, if an agreement is not secured in advance, then at the very minimum the sending attorney will know or have reason to know that opposing counsel intends to "mine" for metadata.[304] However, such agreements may be unreliable because they depend on the trust of counsel, and are not likely to preclude "letting the cat out of the bag."[305]

A final method to prevent the threat of metadata is to use paper rather than electronic documents.[306] In actuality, the only assured solution to avoid sending embedded data is to transmit paper instead of electrons.[307] Unfortunately, this solution defeats the benefits of the technology in the practice of law.[308]

Even if one exercises reasonable care, it is easy to make mistakes, and no particular removal tool may remove all embedded data.[309] In light of these facts, an unattainable standard is not expected of attorneys.[310] However, as advocated by a scholar: "Whichever method you choose, you should consider adopting a standard scrubbing procedure. . . . [I]t is important for you and your clients that you have a workable solution to prevent 'now you don't see it' data from becoming 'now you do.'"[311] In sum, when the concept of metadata enters the mind, "scrub, scrub, scrub" is the logical

300. Steele, *supra* note 29, at 948.

301. *See id.* ("As a result, all metadata in the original version will be deleted."). *But see* Zall, *supra* note 23, at 58 (noting that the PDF file conversion process is conceivably impractical with lengthy documents).

302. Hricik, *Telling Lies*, *supra* note 44, at 95.

303. Zall, *supra* note 23, at 58.

304. *Id.*

305. Hricik, *Telling Lies*, *supra* note 44, at 96.

306. *Id.*

307. *Id.*

308. *Id.*

309. *Id.* at 91.

310. *Id.*

311. Mierzwa, *supra* note 7, at 57. *See* Steele, *supra* note 29, at 943-45 (noting that sending attorneys must safeguard client confidences from inadvertent disclosure, yet few lawyers or firms implement the necessary procedures).

procedure to employ.[312] This way, with the mere click of a button, a client's confidential information will be secure.[313]

4. *Advocating a Rule to Prohibit the "Mining" of Metadata*

It is not only the sending attorney that should have an affirmative ethical obligation to reasonably protect client confidences.[314] The receiving attorney should also have a corresponding duty to abstain from "mining" electronic documents for metadata.[315] Attorneys should not be allowed to "intentionally take advantage of other people's failures."[316]

"Mining" metadata is rationalized as dishonest and deceitful under Model Rule 8.4, and is analogous to looking through another's brief case.[317] With metadata, the receiving attorney is using "technology to spy on opposing counsel."[318] Moreover, Model Rule 8.4(c) is often categorized as a "catch-all," whereas actions that violate subsection (c) also violate other rules.[319] Indeed, various states apply the "catch-all" theory to determine if reviewing embedded data is dishonest.[320] In contrast, the "ABA reasoned that because Model Rule 4.4(b) addresses inadvertent transmission, the issue of dishonest[y] is irrelevant."[321] The ABA claims that whether the recipient attorney knows or should know that the sending attorney's delivery of an electronic file containing metadata was inadvertently disclosed is a subject beyond the realm of the opinion and rules.[322] Nevertheless, the ABA concedes that "metadata can sometimes reveal such critical information as 'who knew what when,' or negotiating strategy and positions."[323]

As a result, the ABA creates a clear contradiction in ethical obligations.[324] The ABA implies that it is not dishonest, fraudulent, or deceitful

---

312. Nelson & Simek, *supra* note 4, at 28.

313. *See* Steele, *supra* note 29, at 950 (concluding that as metadata threats become more widely known, there will be no excuse when client confidences drop into the "wrong hands").

314. *See, e.g.*, Ala. State Bar Ass'n Comm. on Ethics and Prof'l Responsibility, Formal Op. RO-2007-02 (2007), *available at* http://www.alabar.org/ogc/PDF/2007-02.pdf (advocating a duty for both the sending and receiving attorney with regard to metadata).

315. *Id.*

316. Hricik, *Mining for Embedded Data*, *supra* note 11, at 247.

317. Krause, *supra* note 10, at 32.

318. *Id.*

319. Hricik, *Mining for Embedded Data*, *supra* note 11, at 243.

320. *Id.*

321. *Id.*

322. Stevens, *supra* note 2, at 10.

323. Williams, *supra* note 6, at 48-49.

324. *See* Hricik, *Mining for Embedded Data*, *supra* note 11, at 247 ("The characterization of the intentional act of taking advantage of those mistakes as anything less than dishonest is disappointing.").

to take intentional steps to "mine" information known to be confidential or protected under the attorney-client privilege.[325] Therefore, the ABA encourages attorneys to engage in misconduct in explicit violation of Model Rule 8.4.[326] As a consequence, a valid case is made that the solution is to follow the trend-setting jurisdictions by adopting a rule to prohibit the "mining" of metadata.[327] As a result, ethical obligations are imposed on the receiving attorney.[328]

5. *The Receiving Attorney's Ethical Obligations*

Despite imposing a duty on the sending attorney to exercise reasonable care, attorneys will continue to send confidential information inadvertently to opposing counsel.[329] Attorneys will either fail to employ metadata safeguards or the safeguards will fail simply because accidents happen.[330] Therefore, since perfection is improbable the recipient attorney will be put in the unfortunate position of determining how to respond when receiving inadvertent documents.[331] The recipient attorney faces two conflicting questions: (1) was the document inadvertently or intentionally sent; and (2) would it be dishonest to "mine" for metadata.[332]

Adhering to the ABA's proposition that metadata is not always unintentional is perplexing because it essentially "opens the door" to "mining" metadata.[333] In retrospect, why would the sending attorney intentionally include confidences in the form of metadata?[334] Arguably, it is possible that an attorney might receive a document containing metadata from opposing counsel that is confidential, but is "unable to tell whether it occurred intentionally (which seems doubtful) or inadvertently (which is more likely)."[335]

However, at the very minimum, the receiving attorney should have an obligation to notify the sending attorney if the attorney *knows or should*

---

325. *Id.*

326. *Id.*

327. *See, e.g.*, Ala. State Bar Ass'n Comm. on Ethics and Prof'l Responsibility, Formal Op. RO-2007-02 (2007), *available at* http://www.alabar.org/ogc/PDF/2007-02.pdf (discussing the ethical dilemma surrounding the disclosure and "mining" of metadata, and therefore imposing reciprocal ethical duties on both sending and receiving attorneys).

328. *Id.*

329. Hricik, *Mining for Embedded Data*, *supra* note 11, at 232.

330. *Id.*

331. *Id.*

332. *See generally id.* at 235-47 (advocating that the transmission of metadata is certainly inadvertent and that it is dishonest to review metadata).

333. *Id.* at 240-41.

334. *Id.*

335. Hricik, *Telling Lies*, *supra* note 44, at 96.

know that the metadata is transmitted inadvertently.[336] Thus, the threshold determination is whether the intentional delivery of an electronic file that inadvertently contains metadata is in fact inadvertent.[337] Significantly, New York concluded that "counsel plainly does not intend the lawyer to receive 'hidden' material or information[,]" thus the transmission is inadvertent, and any review by the receiving attorney is deliberate.[338]

Consider the fact that it is not the simple opening of a file that will reveal metadata, rather it is intentionally taking steps beyond the double-clicking required to open a file in order to view embedded data.[339] In short, information that appears on its face to be subject to the attorney-client privilege or that appears to be confidential in nature, making it clear that it was inadvertently sent, should not be examined.[340] Rather, the receiving attorney should immediately provide notice to the sending attorney and abide by instructions as to the handling of this inadvertently disclosed confidential information.[341]

However, if the lawyer takes affirmative steps to view embedded data known to be confidential, that lawyer should be found in violation of an ethical obligation for the "mining" of metadata.[342] As this note has emphasized, metadata is invisible, and this is precisely why it is accidentally included in the document.[343] Therefore, for the recipient to find metadata, he or she must deliberately search for the confidential information.[344] To call the seeking of hidden confidences anything other than dishonest is perplexing.[345] Nevertheless, an attorney receiving metadata can and perhaps must contend that the sending attorney waived all protections through the inadvertent transmission of the embedded data.[346]

Indeed, an ethical duty of zealous representation to the recipient's client may require the lawyer to refrain from using the document and to

---

336. *See id*. at 97, 100 (referring to Model Rule 4.4(b), which prescribes the ethical responsibility that arises when one receives information that was not intentionally sent).

337. *Id*. at 98.

338. *Id*. at 99.

339. Hricik, *Mining for Embedded Data*, *supra* note 11, at 241.

340. Hricik, *Telling Lies*, *supra* note 44, at 100.

341. *Id*.

342. *Id*. at 99.

343. Hricik, *Mining for Embedded Data*, *supra* note 11, at 245.

344. *Id*.

345. *See id*. at 247 ("The notion that a lawyer should be permitted to look for inadvertently transmitted embedded data and, thereby, intentionally take advantage of the accidental failure of a colleague to understand the inner workings of software is startling.").

346. Hricik, *Telling Lies*, *supra* note 44, at 101.

seek guidance from the court.[347] However, the majority of states have determined that client confidentiality is more important than the competing ethical obligations on the part of the receiving attorney.[348] Furthermore, even the ABA has determined that in zealously representing a client "there is a limit to the extent to which a lawyer may go 'all-out' for the client."[349]

In regard to the ethical obligations on the inadvertent transmission of metadata, there is no final word.[350] Until metadata dangers are apparent to attorneys throughout the nation, the ABA and individual states should find that the transmission of metadata is either *per se* or presumptively inadvertent.[351] Furthermore, the legal system "should not let lawyers intentionally take advantage of other people's failures" and mandate that attorneys abstain from "mining" metadata and notify the sending attorney upon receipt of such information.[352]

It is time that the ABA and individual states address the two ethical issues pertinent to metadata.[353] The sending attorney should have an affirmative duty to take reasonable precautions to ensure metadata is precluded from inadvertent disclosure prior to electronic transmission.[354] In addition, the receiving attorney should be prohibited from deliberately searching out and viewing metadata received from the sending attorney.[355] In short, the sending attorney should have an ethical obligation to "scrub" electronic documents and the receiving attorney should be prohibited from "mining" metadata.[356] Notwithstanding the ABA's present or future failure to impose such ethical obligations, it is imperative that individual states such as North

---

347. *See id*. (explaining that the recipient attorney may have an ethical obligation to notify the sending attorney of the inadvertent receipt of documents, but pursuant to the duty of zealous representation, may nonetheless argue that the attorney-client privilege has been waived). *But see* Mierzwa, *supra* note 7, at 55 (discussing how New York decided there was no need, in regard to the inadvertent disclosure of metadata, to balance the duty of confidentiality against the duty of zealous representation).

348. *See* Steele, *supra* note 29, at 930 (deciding that the duty of confidentiality outweighs the duty of zealous representation).

349. *See id*. at 934-35 (discussing the ABA's view on zealous client representation).

350. Hricik, *Mining for Embedded Data*, *supra* note 11, at 247.

351. *Id*.

352. *Id*.

353. Steele, *supra* note 29, at 942.

354. *See, e.g*., Ala. State Bar Ass'n Comm. on Ethics and Prof'l Responsibility, Formal Op. RO-2007-02 (2007), *available at* http://www.alabar.org/ogc/PDF/2007-02.pdf (imposing an ethical obligation on sending attorney).

355. *See* Hricik, *Telling Lies*, *supra* note 44, at 79 (discussing the implications of "mining" metadata).

356. *See* discussion *supra* Part II.C.2-5 (proposing a duty to "scrub" and prohibit "mining" of metadata).

Dakota address the issue of metadata by imposing a duty to "scrub" and prohibit the "mining" of metadata.[357]

III. APPLICATION TO NORTH DAKOTA

The dangers of metadata are not foreign to the state of North Dakota.[358] Yet the present North Dakota Rules of Professional Conduct are likely insufficient to address these dangers.[359] Thus, similar to the trend-setting states, it is important for North Dakota to create knowledge of metadata and impose ethical obligations.[360]

A. THE PRESENT NORTH DAKOTA RULES OF PROFESSIONAL CONDUCT

The Joint Committee on Attorney Standards (JCAS) is the mechanism that the North Dakota judicial system uses to comply with the constitutional requirement of the Supreme Court to adopt rules governing attorney discipline and to review issues pertaining to obligations within the legal profession of North Dakota.[361] The purpose of JCAS is to provide a coordinated, complementary, and continuing analysis of issues concerning attorney standards and supervision.[362] In accord with Administrative Rule 38, the JCAS submits recommendations to the State Bar Association Board of Governors (Board) for review and comment prior to submitting the final recommendations to the Supreme Court.[363] After the ABA adopted changes to the Model Rules in 2002 and 2003, the North Dakota Supreme Court requested that the JCAS submit recommendations for amendments to the North Dakota Rules of Professional Conduct.[364] Thus, the JCAS initiated an extensive review in 2002, and thereafter submitted its proposals to the

357. *See* Mierzwa, *supra* note 7, at 52 (advocating the importance of the ABA, as well as individual states, to address metadata issues).

358. *See* discussion *supra* Part II.A.1-4 (discussing what metadata is, as well as its purposes, accessibility, and relevance in the legal profession).

359. *See* discussion *infra* Part III.A. (explaining that the present North Dakota Rules of Professional Conduct are inadequate to address metadata issues within the legal profession).

360. *See* discussion *infra* Part III.B (emphasizing the importance of taking future action in North Dakota to address metadata concerns).

361. N.D. Sup. Ct. Admin. R. 38 Joint Comm. on Att'y Standards (Nov. 16, 1994), *available at* http://www.court.state.nd.us/court/rules/administrative/ar38.htm.

362. *Id.*

363. *Id.*

364. Letter from Alice R. Senechal, Chair, Joint Comm. on Att'y Standards, to Chief Justice Gerald VandeWalle, North Dakota Supreme Court (Oct. 10, 2005) (on file with Penny Miller, Clerk of the North Dakota Supreme Court) [hereinafter Letter from JCAS], *available at* http://www.court.state.nd.us/court/notices/20050353/petition.htm.

Board for comment.[365] Upon receiving such comments, the JCAS altered some, but not all, of the Board's recommendations.[366] The JCAS recommended numerous amendments to the rules and comments in both substance and format to follow the Model Rules.[367]

One recommendation of the JCAS was a proposal to adopt Rule 4.5 regarding inadvertent transmission, which provided:

> (a) A lawyer who receives a document relating to the representation of the lawyer's client and knows or reasonably should know the document was inadvertently sent shall:
>
> (1) promptly notify the sender, and
>
> (2) comply within a reasonable time with the sender's request, if accompanied by a promise of reimbursement of any out-of-pocket expense involved, that the lawyer return the document.
>
> (b) For purposes of this rule, "document" includes facsimile transmissions, electronically received messages, and *metadata* retrievable from an electronic transmission.
>
> (c) For purposes of this rule, a document was inadvertently sent if the sending was deliberate though mistaken act or resulted from the ignorance, negligence, or inattention of the sender or the sender's agent.[368]

The JCAS proposed this rule to govern occurrences in which an attorney receives documents relating to client representation that have been inadvertently transmitted.[369] The proposed rule was predicated on portions of Model Rule 4.4(b), but the JCAS found that the Model Rule was insufficient to provide guidance as to what constitutes an inadvertently sent document and what the attorney should do upon receipt of such a document.[370]

Significantly at issue between the members of the JCAS during the deliberation of the rules was whether the "use" of inadvertent documents

---

365. *Id.*

366. *Id.*

367. *See id.* (stating that the JCAS attempted to follow the ABA Model Rules in either numbering, format, or substance).

368. *See* N.D. Court Rules § III (proposed Oct. 10, 2005) (No. 20050353) [hereinafter N.D. Proposed Amendments], *available at* http://www.court.state.nd.us/court/notices/0050353/contents.htm (providing proposed amendments as recommended by the JCAS) (emphasis added).

369. *See generally id.* at § II (explaining the proposed amendments).

370. *See id.* (indicating that proposed Rule 4.5 is similar to paragraph (a) and subparagraph (1) of Model Rule 4.4(b)).

should be addressed by the proposed rule.[371] One member noted that Model Rule 4.4(b) provides that whether an attorney is to take additional steps beyond notifying the sender is a matter not covered within the Model Rules.[372] Another member stated that it should be explicitly clear whether the receiving attorney can or cannot use the inadvertently received information.[373] While it was noted that the case law and ethics opinions are divided as to the use of inadvertently received information, the members were in general agreement that it would be inadvisable to propose a rule that would allow an attorney unfettered use of such information.[374] A better alternative would be a rule that forbids or at least limits the use of the information.[375]

Another issue was raised pertaining to the use of electronically received documents and the difficulty in completely deleting the document.[376] One member noted, for example, that an email can be "returned," but is in reality still retained in various places throughout the receiving attorney's computer network.[377] This issue was not addressed in the proposed rule, but the JCAS concluded that the proposed rule would provide that in addition to promptly providing notice to the sender, the receiving attorney would be required to comply with a request to return the document.[378]

Therefore, the proposed rule was only adopted in part, whereas the current Rule 4.5, which is applicable to inadvertent transmission, provides:

> (a) A lawyer who receives a document relating to the representation of the lawyer's client and knows or reasonably should know the document was inadvertently sent shall promptly notify the sender.
>
> (b) A lawyer who receives a document under the circumstances creating a duty under this rule does not violate Rule 1.2 or Rule

371. Joint Comm. on Att'y Standards, Meeting Minutes (Aug. 6, 2004), *available at* http://www.court.state.nd.us/court/committees/jt_asc/minutesaugust2004.htm.

372. MODEL RULES OF PROF'L CONDUCT R. 4.4(b) (2002), *available at* http://www.abanet.org/cpr/mrpc/mrpc_toc.html. *See* Joint Comm. on Att'y Standards, Meeting Minutes (Aug. 6, 2004), *available at* http://www.court.state.nd.us/court/committees/jt_asc/minutesaugust 2004 htm (analyzing Model Rule 4.4(b) while contemplating a new Rule 4.5 in North Dakota).

373. Joint Comm. on Att'y Standards, Meeting Minutes (Aug. 6, 2004), *available at* http://www.court.state.nd.us/court/committees/jt_asc/minutesaugust2004.htm.

374. *Id*.

375. *Id*.

376. *Id*.

377. *Id*.

378. N.D. Proposed Amendments, *supra* note 368, § III (outlining the proposed new Rule 4.5).

> 1.4 by not communicating to or consulting with the client regarding the receipt or the return of the document.[379]

Comment 1 to Rule 4.5 notes that the rule acknowledges that lawyers sometimes receive electronic files that are mistakenly sent by opposing parties, their lawyers, or third parties.[380] The only duty imposed on the lawyer is merely to notify the sender, but as to whether a lawyer shall take additional steps or whether the attorney-client privilege has been waived are matters beyond the scope of the rules.[381] Furthermore, the term "document" as read into this rule includes email and other electronic modes of transmission subject to a readable format.[382] However, neither the adopted rule nor its comments include any reference to metadata, unlike paragraph (b) of the proposed rule.[383] Comment 2 indicates that the option to voluntarily return a document unread is a professional judgment reserved to the lawyer.[384]

Unfortunately, North Dakota Rule 4.5 leaves open the question of whether a receiving attorney must abstain from using an inadvertently sent electronic document to "mine" for metadata.[385] In addition, a sending attorney is left with no standard of care as to how to preclude the release of metadata when sending files electronically.[386] Thus, an attorney in North Dakota is left with no direction as to how to handle the dangers of metadata.[387]

B. THE FUTURE NORTH DAKOTA RULES OF PROFESSIONAL CONDUCT

The State of North Dakota needs to take action and impose corresponding duties on both sending and receiving attorneys.[388] North

---

379. N.D. R. OF PROF'L CONDUCT R. 4.5, *available at* http://www.court.state.nd.us/rules/conduct/frameset.htm. The current North Dakota Rules of Professional Conduct became effective on August 1, 2006. *Id.*

380. *Id.*

381. *Id.*

382. *Id.*

383. *Id.* *See* N.D. Proposed Amendments, *supra* note 368, § III (referring to "document" as including metadata).

384. N.D. R. OF PROF'L CONDUCT R. 4.5 cmt. 2., *available at* http://www.court.state.nd.us/rules/conduct/frameset.htm.

385. *Id.*

386. *See id.* (referring to only the receiving lawyer in the black-letter rule and comment).

387. *See id.* (making no reference to metadata concerns within the North Dakota Rules of Professional Conduct).

388. *See, e.g.*, Fla. State Bar Ass'n Comm. on Ethics and Prof'l Responsibility, Formal Op. 06-2 (2006), *available at* http://www.floridabar.org/tfb/TFBETOpin.nsf/b2b76d49e9fd64a5852570050067a7af/0a1b5e3a86df495a8525714e005dd6fd?OpenDocument (imposing reciprocal ethical duties on sending and receiving lawyers because metadata has created new ethical obligations in the practice of law).

Dakota should be on the forefront of metadata, and in considering the appropriate action to take, the North Dakota State Bar should research the ethics opinions issued by the trend-setting jurisdictions.[389] The two duties imposed by these jurisdictions—"scrubbing" and prohibiting "mining"—would effectively address the metadata dangers that exist in the electronic practice of law.[390]

Indeed, members of the JCAS made incredible leeway in discussing the significance of the use of inadvertently received information, and in particular the inclusion of "metadata" when defining the term "document" in the proposed black-letter rule of North Dakota Rule 4.5.[391] Therefore, North Dakota is moving towards the forefront of the metadata issue.[392] Nevertheless, action should be taken by either issuing an ethics opinion or proposing a rule to regulate metadata.[393]

In the alternative, North Dakota may wait to see if the ABA creates or alters the Model Rules to quell the metadata issues.[394] However, in the meantime it is imperative to voice concern about metadata to respective attorneys within the state.[395] At the very minimum, it is important to educate North Dakota attorneys about metadata and its consequences.[396] Indeed, protecting oneself from inadvertently disclosing client confidences or secrets starts with a knowledge of metadata.[397] However, to wait and see without addressing metadata issues allows the sending attorney to

---

389. *See* discussion *supra* Part II.B.2.a-c (detailing the ethics opinions of New York, Florida, and Alabama, which address metadata concerns in the practice of law).

390. *See id*. (discussing the reciprocal ethical duties imposed on both the sending and receiving attorney in the trend-setting jurisdictions).

391. Joint Comm. on Att'y Standards, Meeting Minutes (Aug. 6, 2004), *available at* http://www.court.state.nd.us/court/committees/jt_asc/minutesaugust2004.htm.

392. *Id*.

393. *See* discussion *supra* Part II.C.1-5 (advocating the importance of establishing ethical obligations that pertain to metadata). In North Dakota, ethics opinions are issued by the State Bar Association Ethics Committee, but are advisory only. Interview with Senechal, *supra* note 136. However, if an attorney follows an ethics opinion, he or she is protected from discipline. *Id*. Furthermore, an attorney dealing with an issue at hand may urge for the issuance of an ethics opinion. *Id*.

394. *See* Letter from JCAS, *supra* note 364 (noting that the JCAS reviewed the North Dakota Rules upon the ABA's changes to the Model Rules).

395. *See, e.g.*, Blankenship, *supra* note 218 (indicating that Florida passed a motion to express its sentiment about metadata during the time an ethics opinion was being created). Attorneys and their respective law firms should also implement policies for the handling of metadata. *Id*.

396. *See* Cole, *supra* note 64, at 8 (stating that the first step to managing metadata is education and awareness).

397. Jan Sylanski, *Threat of Metadata and Malpractice Initiates Problems for Attorneys*, 3 LAW. J. 8, 8 (2001).

mistakenly disclose client confidences and the receiving attorney free reign to "mine" for client confidences.[398]

North Dakota Rule 4.5 is arguably insufficient to address this ethical dilemma.[399] In fact, it may be prudent to retain the proposed amendments and re-contemplate the word "metadata" within the rule.[400] Nevertheless, merely including the word "metadata" in Rule 4.5 may not adequately inform attorneys of their respective duties as to sending and receiving inadvertent information containing embedded data.[401] In fact, even addressing the "use" of inadvertently received information without addressing metadata could also be insufficient to equip attorneys with direction when it comes to handling the inadvertent transmission of metadata within electronic documents.[402] Thus, it follows that North Dakota should establish detailed guidelines consistent with the trend-setting states.[403]

IV. CONCLUSION

As this note has discussed, the digital era has transformed legal practice.[404] However, the advent of technology and electronic communications does not coincide with a relaxation of legal ethics.[405] In actuality, the ramifications of modern technology may create considerable dangers within the practice of law.[406] Therefore, attorneys must always be cautious not to overlook the ethical pitfalls that technological advancements present.[407] One such pitfall, as this note has emphasized, is metadata.[408]

---

398. *See generally* Mierzwa, *supra* note 7, at 53-56 (reasoning why ethical duties are imposed on both sending and receiving attorneys when it comes to dealing with metadata).

399. *See* Hricik, *Mining for Embedded Data*, *supra* note 11, at 237-38 (noting that jurisdictions that have adopted Model Rule 4.4(b) have imposed, at a minimum, an obligation to notify the sending attorney).

400. *See* N.D. Proposed Amendments, *supra* note 368, § III (defining the term "document" as including metadata retrieved from electronic files).

401. *See* discussion *supra* Part II.B.1.d (explaining why Model Rule 4.4(b) does not adequately address metadata dangers).

402. *See* Joint Comm. on Att'y Standards, Meeting Minutes (Aug. 6, 2004), *available at* http://www.court.state.nd.us/court/committees/jt_asc/minutesaugust2004.htm (pointing out the difficulty in completely deleting electronic documents within the receiver's computer program).

403. *See, e.g.*, Mierzwa, *supra* note 7, at 53-56 (noting that Illinois's ethical duties in regard to metadata are less than clear, but trend-setting states have distinctively addressed ethical duties in managing metadata).

404. *See* discussion *supra* Part II.A.4 (discussing the repercussions of technology in the practice of law).

405. Gretchen M. Nelson, *Practicing Law Ethically in a Changing Technological World*, 35 THE BRIEF 32, 32 (2006).

406. *Id.* at 32-33.

407. *Id.* at 32.

408. *See* discussion *supra* Parts II.A.2, 4 (examining the dangers that metadata presents).

Metadata pervades the digital world by allowing beneficial uses within various software programs and effective electronic communication.[409] However, metadata also creates potential hazards within different facets of the legal profession.[410] On one hand, an attorney does not need to stay awake at night fretting about metadata, but the savvy way to practice is the secure way to practice.[411] On the other hand, complete ignorance of metadata runs the gamut from embarrassment to legal malpractice.[412]

Metadata proffers distinctive issues for both the sending and receiving attorney of electronic communication.[413] The sender must decide whether to "scrub" files for metadata, and the recipient must determine whether to refrain from "mining" files in search of metadata.[414] However, the trend in a growing number of states is to employ: (1) an affirmative duty on the sending attorney to use reasonable care in sending electronic files that may contain metadata; and (2) an affirmative duty on the receiving attorney to abstain from "mining" documents for confidential information that the sender did not intentionally transmit.[415]

While the trend-setting states New York, Florida, Alabama, and Arizona have issued ethics opinions addressing the aforementioned obligations, the ABA has not imposed a black-letter rule on the issue of metadata.[416] Instead, authorities are split.[417] There is no consistency amongst jurisdictions, and no bright-line rule exists to guide an attorney's ethical conduct when confronted with the hazards created by metadata.[418] Thus, the rules need to change with technology.[419] As this note advocates, the ABA and individual states should consider following in the footsteps of the experimental states by imposing an affirmative duty on both the sending and recipient attorney to "scrub" and prohibit the "mining" of metadata.[420]

---

409. Hirick, *Telling Lies*, *supra* note 44, at 81. *See* discussion *supra* Part II.A.2-4 (discussing the benefits and hazards of metadata and its relevance in the legal profession).

410. *Id*.

411. Blackford, *supra* note 71, at 34.

412. Nelson & Simek, *supra* note 4, at 28.

413. Nelson, *supra* note 405, at 37-38.

414. *Id*. at 38.

415. *Id*. *See* discussion *supra* Part II.B.2.a-c (discussing the trend in a few states).

416. Newman, *supra* note 24, at 2.

417. Cahill, *supra* note 140, at 3-4.

418. *Id*.

419. *Id*. at 3.

420. *See* discussion *supra* Part II.B-C (noting the current law applicable to metadata and encouraging a new rule for the ABA and individual states).

Similar to the ABA Model Rules, North Dakota's Rules of Professional Conduct arguably do not adequately address metadata concerns.[421] Likewise, it is prudent that North Dakota implement corresponding duties on both the sending and receiving attorney.[422] However, at a minimum, it is imperative to generate knowledge and educate North Dakota attorneys about the dangers of metadata.[423]

Advancements in electronic communications are likely to outpace the ability of both courts and state bar associations to evaluate the technological impact on ethical obligations.[424] Nevertheless, the ABA and individual states should strive to keep pace.[425] Solutions to the metadata conundrum are available.[426] It is time to take action.

Crystal Thorpe[*]

421. *See* discussion *supra* Part III.A (explaining the inadequacy of present rules in North Dakota pertaining to metadata).

422. *See* discussion *supra* Part III.B (advocating future action in North Dakota to address metadata).

423. *Id*.

424. Nelson, *supra* note 405, at 38.

425. *See* Steele, *supra* note 29, at 914 ("Because of the nuances of each technological advancement, legal authorities have struggled to keep pace.").

426. *Id*. at 950.

[*]J.D. Candidate at the University of North Dakota School of Law. Special thanks to my family—Jim, Peggy, Dusty, and Maggie—for their continuous support, encouragement, and patience throughout my academic pursuits. I also thank Magistrate Judge Alice R. Senechal for her guidance on the topic of metadata.