Washington Journal of Law, Technology & Arts

Volume 4 | Issue 4 Article 6

5-23-2008

To Mine or Not to Mine: Recent Developments in the Legal Ethics Debate Regarding Metadata

Boris Reznikov

Commercial and Corporate
Cite as: Boris Reznikov, *To Mine or Not to Mine: Recent Developments in the Legal Ethics Debate Regarding Metadata*, [4] Shidler J. L. Com. & Tech. [13] (5/23/2008), *at* <http://www.lctjournal.washington.edu/Vol4/a13Reznikov.html>

TO MINE OR NOT TO MINE: RECENT DEVELOPMENTS IN THE LEGAL ETHICS DEBATE REGARDING METADATA

by Boris Reznikov[1]

Abstract

The American Bar Association recently decided that attorneys are not violating the Model Rules of Professional Conduct by reviewing opposing parties' electronic documents for metadata. The stance taken by the American Bar Association contradicts views from ethics committees in other jurisdictions that have determined that lawyers who examine metadata are acting unethically. This Article summarizes the American Bar Association's decision, as well as the other opinions on metadata, to help practicing attorneys understand the proper ethical considerations they must make when determining whether to look into an electronic document's metadata.

Table of Contents

INTRODUCTION

<1>In August 2006, the American Bar Association ("ABA") established that it is ethical for attorneys to examine ("mine") metadata in the electronic documents they receive from opposing parties.[2] According to the ABA, nothing in the Model Rules of Professional Conduct ("MPC" or "Model Rules") prohibits attorneys from reviewing or using confidential information that could be found in this metadata.[3] The ABA's position opposes ethical decisions from several other jurisdictions that have issued opinions regarding metadata. These jurisdictions' ethics boards have characterized a lawyer's inspection of metadata as dishonest and

consequently unethical.[4] This Article analyzes the ABA's recent ruling and the other metadata opinions to provide practitioners with guidance about the correct ethical approach to metadata mining.[5] The Article only discusses the examination of metadata that takes place outside the discovery context when attorneys voluntarily exchange electronic documents.[6]

METADATA AND THE PRACTICE OF LAW

<2>Metadata literally means "data about data," but this definition fails to provide one with a clear understanding of the word.[7] A federal court has therefore explained metadata to be data that describes "the history, tracking, or management of an electronic document" and includes information such as user permissions, file names, location, format, tracked changes, commentary, and creation and access dates.[8] Metadata can be separated into two categories: (1) application metadata, which is embedded in the file about which it provides information, such as tracked changes; and (2) system metadata, which is stored externally rather than being embedded in the file and is used by the computer's file system to store demographics about each file, such as the last access date of a document.[9] These two forms of readily accessible metadata combine to provide users with helpful information about their electronic documents.[10]

<3>Although the information that metadata provides can serve a valuable function for all users, including attorneys, it may also hurt clients when crucial information is transmitted to opposing parties through the metadata.[11] For instance, metadata that can be helpful to attorneys, such as the creation date of a document, may become critical data that requires protection when parties in a lawsuit are trying to establish "who knew what when."[12] It can also be harmful for clients when during negotiations an electronic document that contains an internal "redlined" change or comment regarding the settlement amount is sent to the opposing party.[13]

OPINIONS FIND THAT MINING METADATA IS UNETHICAL

<4>Ethics boards from New York, Florida, Alabama, and the District of Columbia have issued guidelines for attorneys regarding the mining of metadata. All four boards have concluded that attorneys who mine opposing parties' metadata are acting unethically.

i. New York

<5>The New York Committee on Professional Ethics ("Committee") was the first to publish a decision regarding the ethical obligations of attorneys in relation to metadata.[14] In Opinion 749, issued in 2001, the Committee recognized that "modern computer technology enables sophisticated users who receive documents by electronic transmission to

'get behind' what is visible on the computer screen" to find potentially vital information.[15] The Committee concluded that using technology to view metadata was in conflict with DR 1-102(A)(4) and (5) from New York's Lawyer's Code of Professional Responsibility (the "Code").[16] These provisions of the Code, which are equivalent to ABA Model Rule 8.4, ban conduct "involving dishonesty or fraud" that is "prejudicial to the administration of justice."[17] The Committee felt that the spirit of these rules would be violated because there is strong public policy in favor of preserving confidentiality, which forms the basis of the attorney-client relationship.[18]

<6>In 2003, the Committee expanded its ethical views regarding metadata by publishing Opinion 782.[19] The Committee held that a "lawyer who uses technology to communicate with clients must use reasonable care with respect to such communication, and therefore must assess the risks attendant to the use of that technology and determine if the mode of transmission is appropriate under the circumstances."[20] Thus, when attorneys electronically transmit documents, they must ensure that their clients' confidential information is not inadvertently disclosed.[21] The Committee's decision in Opinion 749 was also reaffirmed by Opinion 782, which corroborated that lawyers who receive documents through electronic transmissions have an obligation to not exploit the unauthorized or inadvertent client confidences contained within the metadata of these files.[22]

<7>In sum, attorneys in New York have an ethical duty to refrain from examining or utilizing metadata. Additionally, they must take reasonable precautions to prevent accidental disclosures of confidential client information through metadata.

ii. Florida

<8>The Florida Bar's Ethics Department ("Department"), in September 2006, also issued an opinion regarding metadata.[23] The Department approached the question in a manner that was similar to New York's Committee. First, the Department ruled that in order for Florida lawyers to maintain confidentiality under Rule 4-1.6(a) they "must take reasonable steps to protect confidential information in all types of documents and information that leave the lawyers' offices, including electronic documents and electronic communications with other lawyers and third parties."[24] Second, under Rule 4-4.4(b), which parallels the MPC provision, attorneys who inadvertently obtain information through metadata must notify the sender of this fact.[25] Lastly, the Department found that when lawyers get electronic documents or communications from other attorneys they must abstain from attempting to mine metadata that the recipients know or should know is not intended for them.[26] Therefore, as in New York, Florida attorneys would be violating their state bar's ethical rules if they were to mine metadata.

iii. Alabama

<9>In March 2007, the Alabama State Bar's Office of the General Counsel ("General Counsel") published Opinion Number: 2007-02 declaring that mining metadata is unethical.[27] The General Counsel explicitly adopted the New York Committee's views and ruled that a receiving attorney has an ethical obligation to refrain from examining metadata because it would constitute "an impermissible intrusion on the attorney-client relationship" in violation of Rule 8.4 of the Alabama Rules of Professional Conduct, which is based on the MPC.[28] Additionally, similar to New York and Florida, the General Counsel determined that attorneys must use reasonable care when transmitting electronic documents to ensure that client confidences or secrets are not disclosed.[29]

iv. District of Columbia

<10>The District of Columbia Bar ("D.C. Bar") became the most recent ethics committee to prohibit metadata mining when in September 2007 it issued Opinion 341: Review and Use of Metadata in Electronic Documents.[30] This decision was not surprising since earlier in the year the D.C. Court of Appeals adopted a broader version of ABA Model Rule 4.4(b) that specifically mandated attorneys to not examine any document that they knew had been inadvertently sent.[31] Although the D.C. Bar expressed that the purpose of the recently modified Rule 4.4(b) dealt with the inadvertent disclosure of whole documents, it found no reason why this provision should "not also apply to an inadvertently transmitted portion of a writing that is otherwise intentionally sent," such as metadata.[32]

THE ABA OPINION

<11>After the New York decision in 2001, attorneys in other states were anticipating an opinion from the ABA's Standing Committee on Ethics and Professional Responsibility ("Standing Committee") to give them guidance on how to deal with metadata. This ruling would be important because most lawyers practice in states that use the ABA's Model Rules as the basis for their attorneys' ethical code.[33]

<12>The Standing Committee finally ruled on this matter in August 2006, and it took the opposing view of New York in issuing ABA Formal Opinion 06-442: Review and Use of Metadata.[34] The Standing Committee first observed that the Model Rules do not contain any specific provisions that would forbid attorneys from reviewing and using metadata.[35] According to the Standing Committee, the closest rule from the MPC that could possibly apply is Rule 4.4(b).[36] This Rule only provides that "[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."[37] Thus, even if the communication of metadata was inadvertent, Rule 4.4(b) does not

comment on the ethical requirements of an attorney's review or use of metadata.[38] The Standing Committee noted that Comment [3] to Rule 4.4(b) indicates that this is the correct interpretation of the provision because attorneys who obtain an inadvertently sent document *may*, but are not mandated to return it unread, "as a matter of professional judgment."[39]

<13>The Standing Committee explicitly rejected New York's analysis that the review of metadata by attorneys would be unethical because it violates Rule 8.4 and the ban against "dishonesty, fraud, deceit, or misrepresentation."[40] Instead, the Standing Committee determined that the recent addition of Rule 4.4(b), adopted in 2002, shows that the intent of the MPC was to avoid any other constraints on receiving attorneys' conduct besides the duty to provide notice to the sender about the inadvertent disclosure.[41] The Standing Committee chose not to rule on how attorneys would determine when a transmission of an electronic document is "inadvertent" within the meaning of Rule 4.4(b) and consequently triggers the requirement to notify the opposing party.[42]

<14>Lastly, the Standing Committee rationalized its decision by observing that attorneys can limit the chance of inadvertently transmitting metadata in electronic documents through proactive efforts.[43] Suggestions from the Standing Committee include: (1) limiting the creation of metadata in the first place; (2) eliminating or "scrubbing" certain embedded information before providing the file to others; and (3) supplying a different version of the document that would not contain metadata, such as a hard copy, a fax, or an image of the document.[44] Although not stated directly in its opinion, the Standing Committee's suggestions imply that similar to New York's Code, the Model Rules require attorneys to protect client confidences.[45] Thus, the ABA opinion, as a whole, places the burden solely on sending attorneys to ensure that damaging metadata is not transmitted to opposing parties.[46]

<15>It is important to note that New York's Opinion 749 was issued shortly after lawyers first discovered the potential consequences of transmitting metadata. The New York Committee even noted in its ruling that it was unclear how a lawyer could ensure that unintended metadata was not transferred to another party.[47] The ABA, on the other hand, had developed a more comprehensive understanding of metadata before adopting its position.[48] Nevertheless, the ABA's opinion has received criticism from legal scholars and has been unsuccessful in persuading the ethics boards of Florida, Alabama, and the District of Columbia to permit metadata mining.[49]

MARYLAND ADOPTS ABA VIEWPOINT

<16>Following the release of the ABA's ethical opinion, the Maryland State Bar Association's Committee on Ethics ("MSBA") issued a ruling about metadata as well.[50] The MSBA disagreed with the decisions of

other jurisdictions and chose to instead side with the ABA. The MSBA stated that there is no ethical violation when receiving attorneys use or review metadata without first checking to see whether the sender intended to transmit the metadata.[52] Further, the MSBA reasoned that because Maryland has not yet adopted Rule 4.4(b) of the MPC, Maryland attorneys are not required to notify the lawyer who sent the documents that there may be an inadvertent transmission.[53] Still, just like the other metadata opinions, the MSBA established that attorneys in Maryland do have an ethical obligation to use reasonable measures to prevent a client's confidential information from being revealed through metadata.[54]

CONCLUSION: THE CURRENT STATE OF MINING METADATA

<17>At this time, there are conflicting views about whether attorneys may ethically mine metadata outside the discovery context. Attorneys who practice in jurisdictions where ethics boards have issued opinions regarding metadata, such as New York, Florida, Alabama, the District of Columbia, and Maryland, should abide by their board's rulings. Lawyers in other jurisdictions, however, can still use the ABA's advisory opinion as guidance in their ethical decisions on mining metadata.[55] Even though the ABA's formal opinions do not carry precedential weight, courts look to them for advice in interpreting the Model Rules that most attorneys are required to follow.[56] Under any circumstances, all attorneys should take reasonable precautions to ensure that client confidences are not disclosed through metadata.[57]

PRACTICE POINTERS

Practitioners should consider a number of options to ensure that unintended metadata is not revealed to opposing parties:

- Limit the amount of metadata that can be found in an electronic document. Most software programs allow users to download additional metadata removal tools or turn off features that produce metadata. For more information, visit the website of the software publisher.[58]
- Obtain third party software products that permit users to remove metadata from specific files. These programs can also be used to eliminate metadata from emails.[59]
- Save the document as an RTF (Rich Text Format) file before electronically transmitting it.[60]
- Print out and scan the document to turn it into a PDF (Portable Document Format) copy, which will prevent the recipient from being able to access the original version.[61]
- Convert the document to a PDF. This essentially changes the document's multifaceted data into a basic image with some

very basic metadata.[62]

- If the danger of revealing confidential information is high and time is not an issue, then consider providing a "hardcopy" of the document by faxing it or mailing it.[63]

<< Top

Footnotes

1. Boris Reznikov, University of Washington School of Law, Class of 2008. Thank you to Professor Anita Ramasastry (University of Washington School of Law), Professor Robert H. Aronson (University of Washington School of Law), Craig Ball (Trial Attorney and Computer Forensics Expert), and Ari Okano. Readers should note that this Article only discusses ethics opinions regarding metadata that were issued before January 2008.

2. ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 06-442: Review and Use of Metadata (2006), *available at* http://www.pdfforlawyers.com/files/06_442.pdf.

3. *Id.*

4. *See* N.Y. Comm. on Prof'l Ethics, Op. 749 (2001), *available at* http://www.nysba.org/AM/Template.cfm?Section=Ethics_Opinions&CONTENTID=6533&TEMPLATE=/CM/ContentDisplay. ; Prof'l Ethics of the Fla. Bar, Op. 06-2 (2006), *available at* http://www.floridabar.org/tfb/tfbetopin.nsf/SearchView/ETHICS,+OPINION+06 2?opendocument; Ala. State Bar Office of the Gen. Counsel, Op. No. 2007-02 (2007), *available at* http://www.alabar.org/ogc/fopDisplay.cfm?oneId=412.

5. While a few states have explicitly prohibited metadata mining, bar associations in California and Oklahoma hold seminars to teach lawyers how to look into metadata in order to help their clients. J. Craig Williams, *Tech Law: The Importance of Deleting Metadata…And How to Do It*, 49 Orange County Lawyer 48, 49 (2007). The ABA's advisory opinion, thus, comes at a good time and will hopefully assist attorneys who are confused by the inconsistent views taken by various jurisdictions.

6. This Article does not discuss metadata mining that takes place during the discovery phase of trial because the Federal Rules of Civil Procedure now provide guidelines in this area. *See* Fed. R. Civ. P. 16(b), 26(f), 33(d), 34(a), and 37(f).

7. *See* Peter Mierzwa, *Young Lawyers Section: Metadata: Now You Don't See It – Now You Do*, 20 CBA Record 52, 52 (2006); *see also* Craig Ball, *Beyond Data about Data: The Litigator's Guide to Metadata* (2005), http://www.craigball.com/metadata.pdf ("Ask an electronic evidence expert, 'What's metadata?' and there's a good

chance you'll hear, 'Metadata is data about data' – another answer that's 100% accurate, and totally useless").

8. Williams v. Sprint/United Mgmt. Co., 230 F.R.D. 640, 646 (D. Kan. 2005). *See also* Ball, *supra* note 7 ("Metadata is evidence, typically stored electronically, that describes the characteristics, origins, usage, and validity of other electronic evidence"). The following is a more complete list of potential metadata that may be in a document, along with the information that it can reveal: authors, comments, company or firm name, computer name, document revisions, document versions, embedded objects or non-visible portions of embedded OLE (object linking and embedding) objects, fast saves, file location, file properties, headers and footers, hidden text, hyperlinks, initials, linked objects, matching font, network or server name, personalized views, revisions, small font, summary details, styles, template information, tracked changes, undo/redo history, and versions. *See* Sheila Blackford, *Managing Your Practice: Metadata: Danger or Delight?* 66 Or. St. B. Bull. 29, 30 (May 2006); *see also* The Sedona Conference Working Group, *The Sedona Guidelines: Best Practice Guidelines and Commentary for Managing Information and Records in the Electronic Age*, Appendix E (Sept. 2005), *available at* http://www.thesedonaconference.org/content/miscFiles/TSG9_05.pdf .

9. Ball, *supra* note 7.

10. Many commentators have referred to metadata as being "hidden." *See* Ala. State Bar Office of the Gen. Counsel, Op. No. 2007-02, *supra* note 4 ("For the purposes of this Opinion, metadata may be loosely defined as data hidden in documents that is generated during the creation of those documents"); American Bar Association, *What's the Meta with Metadata?* (Jan. 2006), http://www.abanet.org/media/youraba/200601/article01.html ; Ball, *supra* note 7. This view, however, is misleading. Although there is one type of application metadata that requires specialized computer forensic tools to be extracted and interpreted, most metadata is available to the average computer user. *See* Ball, *supra* note 7.

11. *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 (2005), *available at* http://www.lctjournal.washington.edu/Vol1/a008Cole.html; *see also* The Sedona Conference Working Group, *supra* note 8.

12. *See* ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 06-442: Review and Use of Metadata, *supra* note 2; *see also* Ala. State Bar Office of the Gen. Counsel, Op. No. 2007-

02, *supra* note 4 ("The disclosure of metadata contained in an electronic submission to an opposing party could lead to disclosure of client confidences and secrets, litigation strategy, editorial comments, legal issues raised by the client, and other confidential information").

13. *See* ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 06-442: Review and Use of Metadata, *supra* note 2; *see also* David Hricik, *I Can Tell When You're Telling Lies: Ethics and Embedded Confidential Information*, 30 J. LEGAL PROF. 79 (2005/2006) (A recent example of the potential consequences of metadata comes from an attorney who was negotiating a contract between his client and lawyers from a large software company. Throughout the negotiations, both parties used the "track changes" feature of Microsoft Word to propose amendments to the contract. The parties would email these changes back and forth to each other. Attorneys for the large software company also made comments on the Word document that were intended to remain internal, such as the terms of the contract, negotiating positions, and bottom-lines. Unfortunately, the lawyers for the large software company did not realize that this information was embedded into the document and could be accessed by opposing counsel with a simple "click of a button." This is exactly what the other attorney did, and he had a clear advantage in negotiations from that point on because he knew the software company's critical bargaining information).

14. *See* N.Y. Comm. on Prof'l Ethics, Op. 749, *supra* note 4 (The Committee specifically addressed whether lawyers may ethically use available technology to "surreptitiously examine" electronic documents).

15. *Id.*

16. *Id.*

17. *Id.*

18. *Id.* (The Committee cited MMR/Wallace Power & Indus. Inc. v. Thames Assocs., 764 F.Supp. 712, 718-19 (D. Conn. 1991), where the court observed that the "spirit if not the letter of ethical rules" prevents attorneys from obtaining, inadvertently or not, confidential information about the opposing party's litigation strategy).

19. *See* N.Y. Comm. on Prof'l Ethics, Op. 782 (2004), *available at* http://www.nysba.org/AM/Template.cfm?Section=Ethics_Opinions&CONTENTID=6871&TEMPLATE=/CM/ContentDisplay. (The Committee was specifically addressing the following question: "Does a lawyer who transmits documents that contain 'metadata' reflecting client confidences or secrets violate DR 4-101(B)")?

20. *Id.* The Committee cites DR 4-101(B)(1), which prohibits attorneys from "knowingly" revealing confidential information

of a client, and DR 4-101(D), which states that an attorney "shall exercise reasonable care to prevent his or her employees, associates, and others whose services are utilized by the lawyer from disclosing or using confidences or secrets of a client." *Id*.

21. *Id.*

22. *Id.*

23. *See* Prof'l Ethics of the Fla. Bar, Op. 06-2, *supra* note 4 (The Department was directed by the Board of Governors of the Florida Bar to issue an opinion "to determine ethical duties when lawyers send and receive electronic documents in the course of representing their clients").

24. *Id.* Rule 4-1.6(a) provides as follows:

> (a) Consent Required to Reveal Information: A lawyer shall not reveal information relating to representation of a client except as stated in subdivisions (b), (c), and (d), unless the client gives informed consent.

The comment to Rule 4-1.6 further provides:
A fundamental principle in the client-lawyer relationship is that the lawyer maintain confidentiality of information relating to the representation. The client is thereby encouraged to communicate fully and frankly with the lawyer even as to embarrassing or legally damaging subject matter. *Id.*

25. *Id.* Rule 4-4.4(b) is concerned with inadvertent disclosures of information and states:

> 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. *Id.*

26. *Id.* This metadata must be considered by receiving attorneys as "confidential information which the sending lawyer did not intend to transmit." The transmitted metadata, therefore, cannot be reviewed by attorneys because the Department has interpreted the comment to Rule 4-4.4(b) to prohibit this. *Id.*

27. *See* Ala. State Bar Office of the Gen. Counsel, Op. No. 2007-02, *supra* note 4 (The General Counsel answered the following question: "Is it unethical for an attorney to mine metadata from an electronic document he or she receives from another party")?

28. *Id.* ("The mining of metadata constitutes a knowing and deliberate attempt by the recipient attorney to acquire

confidential and privileged information in order to obtain an unfair advantage against an opposing party").

29. *Id.*

30. D.C. Bar, Op. 341: Review and Use of Metadata in Elec. Documents (2007), *available at* http://www.dcbar.org/inside_the_bar/contact_us/index.cfm (The D.C. Bar was answering the numerous inquiries it had received regarding a lawyer's ethical obligations towards metadata). Opinion 341 separates the issues regarding metadata mining into two categories: (1) outside the discovery context, and (2) inside the discovery context. *Id.* The latter issue is not discussed in this Article.

31. *Id.* The District of Columbia's new Rule 4.4(b) provides as follows:

> A lawyer who receives a writing relating to the representation of a client and knows, before examining the writing, that it has been inadvertently sent, shall not examine the writing, but shall notify the sending party and abide by the instructions of the sending party regarding the return or destruction of the writing. *Id. Compare with* ABA Model Rule 4.4(b), *infra* note 37.

The D.C. Bar's more expansive version of Rule 4.4(b) was adopted after prior decisions in the jurisdiction determined that attorneys who knowingly review inadvertently sent documents from opposing parties are acting dishonestly and consequently violating Rule 8.4(c), a provision that is equivalent to the one in the Model Rules. *See* D.C. Bar, Op. 341: Review and Use of Metadata in Elec. Documents, *supra* note 30.

32. *Id.* The D.C. Bar qualified its ruling by requiring attorneys to only refrain from mining when they had "actual prior knowledge" that the metadata was inadvertently provided, a determination that would be fact-dependent. The D.C. Bar felt that this condition was a better approach due to the frequent, mutually helpful, and usually harmless exchange of electronic documents between attorneys. Further, the requirement under Model Rule 1.6, which applies in the District of Columbia, already compels lawyers to take reasonable steps to ensure that client confidences are not revealed. *Id.*

33. A version of the MPC is enacted in 47 states and the District of Columbia. Carolyn M. Branthoover and Karen I. Marryshow, *Ethical Considerations in Light of the Recent E-Discovery Amendments to the Federal Rules*, n. 1, January 2007, http://www.klgates.com/newsstand/Detail.aspx?publication=3581. The three states in which the Model Rules

are not followed are New York, Maine, and California. *Id.*

34. *See* ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 06-442: Review and Use of Metadata, *supra* note 2.

35. *Id.* The ABA opinion assumes that the receiving attorney has acted ethically and in accordance with the law in obtaining the electronic documents. *Id.* at n. 6.

36. *See* ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 06-442: Review and Use of Metadata, *supra* note 2.

37. *Id.* Comment [2] to Rule 4.4 explains that the notification requirements are only in place so that the sender is able to take protective measures after their inadvertent disclosure. The Comment warns that other applicable law that is outside the scope of the MPC may require an attorney to take further steps beyond notification. *Id.* at n. 6.

38. *See* ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 06-442: Review and Use of Metadata, *supra* note 2. The Standing Committee chose not to rule on whether the sending of metadata would constitute an inadvertent or advertant transmission. Instead, the Standing Committee simply observed that the decision may be fact specific. *Id.* at n. 7.

39. *See* ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 06-442: Review and Use of Metadata, *supra* note 2.

40. *Id.*

41. *Id.*

42. *Id.*

43. *Id.*

44. *Id.*

45. *See Editorial: Preventing Metadata Disclosure*, N.J. LAW JOURNAL (Nov. 29, 2006); Jason Krause, *Metadata Minefield: Opinions Disagree on Whether It's Ethical to Look at Hidden Electronic Information*, ABA JOURNAL (Apr. 2007), *available at* http://www.abajournal.com/magazine/metadata_minefield/ ("'Without saying so, the clear implication is that if you ignore the issue and disclose client information or adversely affect the client's position, you run the risk of running afoul of other rules,' says Dunn. 'Rule 1.6 on protecting client confidentially or 1.1 on competence are two that readily come to mind.'").

46. *See Editorial: Preventing Metadata Disclosure*, *supra* note 45.

47. *See* N.Y. Comm. on Prof'l Ethics, Op. 749, *supra* note 4. The Committee, therefore, might not have considered that metadata can be "scrubbed", or removed, before being sent to opposing counsel. *See* Practice Pointers, *infra*, for methods

that can be used by attorneys to limit or remove metadata.

48. The primary focus of Opinion 749 seems to be on the use of technology to spy on the strategy of the opposing attorney. *See* Krause, *supra* note 45; Mierzwa, *supra* note 7. Opinion 749, therefore, does not thoroughly analyze the issue and leaves certain questions unanswered. Are attorneys "using technology" when they check the "properties" of documents that were electronically transmitted to them by opposing counsel? This simple procedure of "right-clicking" the document reveals metadata such as the date the file was created and the name of the author. Opinion 749 implies that this is unethical, which draws a lot of criticism from technologically adept attorneys who are concerned about the implications of banning the practice. These lawyers analogize mining metadata to having a hard-copy contract, obtained legitimately through discovery, fingerprinted to determine which different individuals have had the contract in their possession. This would be condoned by most ethical rules, and thus some attorneys even believe that they "could be giving their client the short shrift by not looking at the metadata." *See* Jessica M. Walker, *What's a Little Metadata Mining Between Colleagues*, Daily Business Review (Apr. 21, 2006).

49. *See* David Hricik, *Mining for Embedded Data: Is it Ethical to Take Intentional Advantage of Other Peoples Failures?*, 8 N.C. J. L. & Tech. 231 (2007) (arguing that courts should hold the transmission of embedded data to be either per se or presumptively inadvertent transmissions and lawyers should refrain from mining this data).

50. *See* Md. State Bar Ass'n, Comm. on Ethics, Opinion 2007-092 (2006) (The question posed to the MSBA dealt with the ethics of viewing and/or using metadata).

51. *Id.*

52. *Id.*

53. *Id.*

54. *Id.*

55. While other states have not released formal opinions on metadata at this time, there are some general practices that are emerging. Lawyers in Oregon have dealt with the notion of metadata as being an inadvertently sent document and therefore, according to Rule 4.4 of the Oregon Rule of Professional Conduct, attorneys must notify opposing counsel if they "know or should know" that the document was not intended to be sent with the metadata. *See* Blackford, *supra* note 8. Further, Illinois' past opinions imply that the Illinois State Bar Association would permit reviewing metadata. *See* Mierzwa, *supra* note 7. Both of these states have not had a chance to revisit their ethical viewpoints since the ABA's

advisory opinion.

56. *See, e.g.*, Aiken v. Bus. and Indus. Health Group, Inc., 885 F.Supp.1474, 1478 (D.Kan. 1995); Olson v. Snap Products, Inc., 183 F.R.D. 539, 544 (D.Minn 1998); In re United Mine Workers of Am. Employee Benefit Plans Litig., 156 F.R.D. 507, 511-12 (D.D.C. 1994). *See also* State Bar of Cal. Standing Comm. on Prof'l Responsibility and Conduct, Formal Op. No. 1983-71, *available at* http://calbar.ca.gov/calbar/html_unclassified/ca83-71.html ("Although there is apparent widespread misconception, the ABA Model Code of Professional Responsibility, like sister state rules and court opinions, is not binding in California although it may be persuasive in those instances where there is no controlling rule of professional conduct, statute, or Court ruling in California"); Branthoover, *supra* note 33.

57. The determination of whether an attorney took reasonable precautions should depend on the circumstances of each individual case. Alabama's General Counsel explained that an analysis of this question should include the consideration of the following factors: (1) steps taken by the attorney to prevent the disclosure of metadata; (2) the nature and scope of metadata revealed; (3) the subject matter of the document; and (4) the intended recipient. Thus, for purposes of an example, a lawyer would need to "exercise greater care" when transmitting electronic documents to opposing parties than e-filing pleadings with courts because "[t]here is simply a much higher likelihood that an adverse party would attempt to mine metadata, than a neutral and detached court." *See* Ala. State Bar Office of the Gen. Counsel, Op. No. 2007-02, *supra* note 4.

58. *See* Cole, *supra* note 11; Blackford, *supra* note 8; Mierzwa, *supra* note 7.

59. *See id.*

60. *See* Cole, *supra* note 11; Blackford, *supra* note 8.

61. *See id.*

62. *See* Cole, *supra* note 11; Mierzwa, *supra* note 7.

63. *See id.*

Errata

(updated September 23, 2008):

1. Footnote 30 should refer to http://www.dcbar.org/for_lawyers/ethics/legal_ethics/opinions/opinion341.cfm **not** http://www.dcbar.org/inside_the_bar/contact_us/index.cfm

2. Footnote 50 should refer to Md. State Bar Ass'n, Comm. on Ethics, Opinion 2007-09 (2006), **not** Md. State Bar Ass'n,

Comm. on Ethics, Opinion 2007-092 (2006).