THE ETHICS OF "MINING FOR METADATA"

Andrew J. Cavo[†]

TABLE OF CONTENTS

[†] B.A., Siena College, 2002; J.D., Cornell Law School, 2009. I would like to thank Professor Nelson Roth of Cornell Law School for several key insights into the ethical issues discussed herein, and for supporting this article's publication. A special "thank you" to my parents, brothers and sisters, and in-laws, for their never-ending encouragement and love. And to my wife, Kristen Rose Cavo, whom I adore and without whom I never would have begun.

I. INTRODUCTION

Imagine the following extreme scenario: you represent the defendant in a contract dispute and a junior associate at the plaintiff's firm sends you a Microsoft Word document that purports to represent the plaintiff's final, pay-it-or-we-go-to-trial settlement demand of $10-million. But you suspect the plaintiff would actually settle for far less. So, in a frenzy of zealous representation, you "mine for metadata"; that is, you deliberately search that document's hidden or embedded information. A few mouse clicks reveal a wealth of information: when the document was created, who worked on it, for how long . . . a few more clicks and . . . what's this?! You are still looking at the same document, but it now includes comments in the margins, made during the document's editing process! One such comment from the head partner reads, "We'll tell them $10 million for now, but that's just to feel them out. Our actual bottom line is $750,000." Armed with that information, you counteroffer for $500,000 and eventually settle the case for exactly $750,000. The few minutes it took you to "mine for metadata" (combined with your opposing counsel's inadvertent metadata disclosure) saved your client millions!

Is what you did ethical? The American Bar Association ("ABA") says yes.[1] But the New York County Lawyer's Association Committee on Professional Ethics ("NYCLA Committee") disagrees.[2] In recent opinions on the ethics of "mining for metadata," the ABA and NYCLA Committee come out on opposite sides over whether attorneys may ethically seek such a strategic advantage.

This article examines the ethics of "mining for metadata" in communications between opposing attorneys. I should note at the outset, however, that neither the ABA opinion, the NYCLA opinion, nor this paper addresses metadata's effect on electronic discovery, for several reasons. First, many discovery agreements provide that metadata may be viewed by attorneys.[3] Second, in

[1] *See* ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 06-442 (2006), *available at* http://www.pdfforlawyers.com/files/06_442.pdf (discussing review and use of metadata).

[2] *See* NYCLA Comm. on Prof'l Ethics, Op. No. 738 (2008), *available at* http://www.nycla.org/siteFiles/Publications/Publications1154_0.pdf (discussing the ethics of searching inadvertently sent metadata in opposing counsel's electronic documents).

[3] *Id*. at n.3.

the context of discovery, a lawyer may not alter a document when it would be unethical or unlawful to do so.[4] Finally, and perhaps most importantly, procedural rules of court or law, such as Federal Rule of Civil Procedure 34(b),[5] often override the ethical issues discussed herein.[6] Accordingly, U.S. District Court Judge Shira A. Sheindlin of the Southern District of New York advises that "[o]nce a case enters the discovery phase, attorneys must balance the duties owed under the Model Rules with the requirements of the discovery rules."[7]

Part II of this paper will define "metadata," explain its significance, and describe potential pitfalls for the unwary lawyer. Part III will discuss the conflicting ABA and NYCLA opinions, their underlying rationale, and ways that other states have addressed the ethics of "mining." Part IV will offer practical tips to help attorneys avoid the wrong side of an inadvertent metadata disclosure. Part V will provide a quick and dirty guide on just how to "mine for metadata." Part VI is a brief conclusion.

II. DEFINING "METADATA" AND RECOGNIZING POTENTIAL PITFALLS

Metadata is simply the information embedded within electronic documents.[8] That information typically includes its history, tracking, and management, which may also include changes to that document.[9] Obviously, not all such information reveals the depths of an opponent's psyche to the degree described in the scenario above; for the most part, metadata is a harmless record of an electronic document's various statistics.[10]

---

[4] MODEL RULES OF PROF'L CONDUCT R. 3.4(a) (2004).

[5] Fed. R. Civ. P. 34(b)(2)(E)(ii) ("If a request does not specify a form for producing electronically stored information, a party must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms . . . .").

[6] *See* David Hricik & Chase Edward Scott, *Metadata: The Ghosts Haunting e-Documents*, 13 GA. B. J. 16, 17, 19–20 (Feb. 2008), *available at* http://www.gabar.org/public/pdf/gbj/feb08.pdf (discussing the lawyer's obligation to remove embedded confidential information from documents he or she creates or sends on the client's behalf).

[7] SHIRA A. SCHEINDLIN & DANIEL J. CAPRA, ELECTRONIC DISCOVERY AND DIGITAL EVIDENCE 447 (Thomson/Reuters 2009).

[8] ABA, *supra* note 1, at 1; *see also* Definition of Metadata, http://www.webopedia.com/TERM/m/metadata.html (last visited Oct. 27, 2009) (defining "metadata" as "[d]ata about data.").

[9] *See* Fed. R. Civ. P. 26(f) advisory committee's note.

[10] *See* ABA, *supra* note 1, at 3 ("Not all metadata . . . is of any consequence; most is probably of no import.").

But even such basic information could ensnare the unwary (and unethical) attorney. Imagine billing a client for ten hours spent working on a document between November 3rd and November 10th, only to have that client search the document's basic statistics to learn that you actually spent only five hours total and have not touched it since Halloween! More typically, however, in disputes over "who knew what when" or who the author of a particular document was, even the most fundamental information can prove critical.[11]

A. Common Computer Software Features that Pose Metadata Problems

Further pitfalls accompany today's more advanced features, which could provide an endless supply of strategic information.[12] A non-exhaustive list of Microsoft Word ("Word") features that create metadata includes "track changes," "fast saves," inserting "comments," and saving multiple "versions" of a document.[13]

First and foremost among potential offenders is "track changes," one of Word's most useful components because it permits writers and readers to collaborate by highlighting changes that subsequent users can either accept or reject.[14] Litigators and transactional lawyers alike sing the praises of "track changes" and use it regularly.[15] Problems arise, however, when "track changes" is turned on without the user's knowledge. This can happen when its settings are set to not highlight the changes on-screen.[16] By simply changing those settings, the recipient of a document can view any comments and changes that were made during the document's editing process, thereby revealing the author's mental processes or previous positions.[17]

Similarly, Word's "fast saves" feature reduces the chance of losing data in a power failure, but in doing so retains information

---

[11] *Id*.

[12] Litigation, negotiation, due diligence, and client correspondence are just a few examples of settings particularly sensitive to metadata issues because they involve frequent transfer of electronic files.

[13] *See* Hricik & Scott, *supra* note 6, at 17–19.

[14] *See id.* at 18; *see also* Tom Mighell & Dennis Kennedy, *Staying on Track with Track Changes*, L. PRAC. TODAY, Mar. 2007, *available at* http://www.abanet.org/lpm/lpt/articles/slc03071.shtml.

[15] *See* Mighell & Kennedy, *supra* note 14.

[16] Hricik & Scott, *supra* note 6, at 18.

[17] *See id.*

that the user may think is deleted.[18] As a result, a savvy subsequent reader can view that document's revisions. Another Word feature allows a user to insert "comments" into a document's margins.[19] Data from these "comments" often remain hidden within the document, providing opposing counsel another avenue for espionage.[20] As a final example, Word's "versions" feature creates a new version of the document on every save, thereby allowing the user to compare versions against each other.[21] Unfortunately for some, all versions are saved in the same final document, so a savvy opponent would also be able to view every version of that document.[22]

B. Real-life Metadata Disclosure Debacles

Inadvertent metadata disclosure is not simply a hypothetical phenomenon. In 2004, the SCO Group—a self proclaimed "leading provider of software technology" for, among other things, embedded systems[23]—sued DaimlerChrysler and Autozone. But a revision in a SCO attorney's document sent to the opposition revealed that the original target of the lawsuit was actually Bank of America.[24]

A 2008 employment discrimination suit against GE provided the setting for a far more public disclosure. Portions of that case's filings were redacted by court order before they were sent to PACER, an online database that allows public access to all federal court filings.[25] Unfortunately for GE, by simply copying the redacted lines and pasting them into a fresh Word document, "[i]nformation about the inner-workings of GE's white, male-dominated management and their alleged discriminatory practices against women . . . appear[ed] with little technical

[18] *Id.*

[19] *See id.* at 18–20; Microsoft Office Online, *Help and How-to: About Tracked Changes and Comments*, http://office.microsoft.com/en-us/help/HP052416341033.aspx?mode=print (last visited Oct. 31, 2009).

[20] *See* Hricik & Scott, *supra* note 6, at 19.

[21] *Id.*

[22] *Id.*

[23] SCO Group, Inc., Home Page, http://www.sco.com/company/profile.html (last visited Oct. 31, 2009).

[24] Stephen Shankland & Scott Ard, *Hidden Text Shows SCO Prepped Lawsuit Against BofA*, CNET NEWS, Mar. 4, 2004, *available at* http://news.cnet.com/2100-7344_3-5170073.html.

[25] Douglas S. Malan, *A Major Redaction Gaffe*, CONN. L. TRIB., May 26, 2008, *available at* http://www.ctlawtribune.com/getarticle.aspx?ID=30411.

savvy required."[26]

Nor are metadata disclosure problems confined to legal matters. When then-Judge Samuel A. Alito, Jr. was nominated to fill Justice Sandra Day O'Connor's seat on the U.S. Supreme Court, the metadata in an anonymous and highly controversial anti-Alito memo revealed that its authors were actually Chris Prendergast and Devorah Adler—both members of the Democratic National Committee.[27]

A final example of an inadvertent metadata disclosure demonstrates that high ranking government officials are not immune. In 2005, Charles Clarke, the U.K.'s Home Secretary, sent a Word document via email to the opposing Conservative Party voicing his support for a plan to hold terror suspects for up to three months without trial.[28] A quick look at the document's "tracked changes," however, revealed Clarke's discord with this measure—his earlier draft stated, "I believe there is room for debate as to whether we should go as far as three months. I'm still in discussion with the police on this point."[29]

III. THE ABA AND NYCLA ISSUED CONFLICTING OPINIONS ON "MINING FOR METADATA"

The American Bar Association's Model Rules of Professional Conduct ("ABA Model Rules") is the common starting point for any legal ethics issue. To date, the vast majority of states—including, as of April 2009, New York—have adopted professional conduct rules that closely follow the ABA Model Rules.

A. The ABA Finds Nothing Unethical About "Mining for Metadata"

On August 5, 2006, the ABA Standing Committee on Ethics and Professional Responsibility ("ABA Committee") issued an opinion entitled "Review and Use of Metadata" ("ABA opinion"),

[26] *Id*.

[27] Tom Zeller, Jr., *LINK BY LINK; Beware Your Trail of Digital Fingerprints*, N.Y. TIMES, Nov. 7, 2005, *available at* http://query.nytimes.com/gst/fullpage.html?res=9C07E3DA143EF934A35752C1A9639C8B63&scp=1&sq=%22track%20changes%22%20lebanese%20prime%20minister%20names&st=cse.

[28] *See* Will Sturgeon, *Word Blunder Exposes U.K. Split on Terrorism*, CNET NEWS, Sept. 16, 2005, *available at* http://news.cnet.com/Word-blunder-exposes-U.K.-split-on-terrorism/2110-1029_3-5869260.html?part=rss&tag=5869260&subj=news.

[29] *Id.*

which held that "the ABA Model Rules of Professional Conduct permit a lawyer to review and use embedded information contained in e-mail and other electronic documents, whether received from opposing counsel, an adverse party or an agent of an adverse party."[30] The Model Rules thus do not prohibit a lawyer from "mining for metadata" and taking full advantage of any discoveries. The ABA Committee noted that the most closely applicable provision is Model Rule 4.4(b), which deals with a lawyer's receipt of inadvertently disclosed information, but declined to address whether metadata disclosure should be considered inadvertent.[31]

Instead, the ABA's rationale for allowing "mining" focused primarily on the sending lawyer's duty to maintain client confidentiality by properly "scrubbing" the data to avoid disclosing client confidences.[32] "Scrubbing" means eliminating certain embedded information in an electronic document before sending it to others.[33] The ABA Committee found support for this approach in its Comment to Model Rule 1.6, which states, "[a] lawyer 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 of the client or who are subject to the lawyer's supervision."[34] The ABA opinion went as far as offering computer tips for sending attorneys, and even suggested avoiding electronic document transmission altogether with an ancient solution: send hard copies![35]

Roy Simon summed up the ABA opinion's application to New York lawyers in the following way:

> Given that lawyers in most jurisdictions in the United States have adopted the ABA Model Rules, a [New York] lawyer sending a digital attachment to an out-of-state lawyer should assume that the receiving lawyer may ethically study the metadata embedded in the document as long as the lawyer notifies the sending lawyer that the metadata has been received. Indeed, if a receiving lawyer

---

30 ABA, *supra* note 1, at 1.

31 *Id*. at 3–4 (citing MODEL RULES OF PROF'L CONDUCT R. 4.4(b) (2004) ("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.")).

32 ABA, *supra* note 1, at 4–5.

33 *Id.* at 5.

34 MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. (2004).

35 ABA, *supra* note 1, at 5.

> believes that the metadata was sent deliberately rather than inadvertently – often a plausible conclusion, given the ease of removing metadata – then the lawyer need not even notify the sender that the metadata has been received and even in New York may freely exploit it.[36]

B. New York Deems "Mining for Metadata" Unethical

New York's legal ethics committees take an alternate approach to metadata. Rather than focusing solely on the sending attorney's duty to maintain client confidentiality, they acknowledge that some amount of inadvertent metadata disclosure is inevitable. Accordingly, they advise that there must be an ethical obligation on the receiving attorney not to take advantage.

In 2001, New York became the first state to address an attorney's ethical obligations with regard to "mining for metadata."[37] An opinion by the New York State Bar Association's Committee on Professional Ethics drew the line at using "available technology to surreptitiously examine and trace e-mail and other electronic documents."[38]

The NYCLA Committee reaffirmed New York's position in a March 24, 2008 opinion ("NYCLA opinion") that is squarely at odds with the ABA's.[39] The NYCLA opinion held that "when a lawyer sends opposing counsel correspondence or other material with metadata, the receiving attorney may not ethically search the metadata in those electronic documents with the intent to find privileged material . . . ."[40] Every lawyer still has an obligation to "scrub" electronic documents to avoid disclosing client confidences and secrets, but clearly not all documents will always be properly "scrubbed" because mistakes do happen.[41] In such situations, the NYCLA opinion instructs New York lawyers not to take advantage of the sending attorney's oversight by

---

[36] ROY SIMON, SIMON'S NEW YORK CODE OF PROFESSIONAL RESPONSIBILITY ANNOTATED 589–90 (2007).

[37] *See* Norman C. Simon, *Coming to Terms on Metadata*, N.Y.L.J. (Oct. 28, 2008), *available at* http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1202425583826.

[38] NYS Bar Ass'n Comm. on Prof'l Ethics, Op. 749 (2001), *available at* http://www.nysba.org/AM/Template.cfm?Section=Ethics_Opinions&TEMPLATE=/CM/ContentDisplay.cfm&CONTENTID=6533.

[39] NYCLA, *supra* note 2.

[40] *Id.*

[41] *Id*.

"mining for metadata."[42]

The NYCLA Committee found support for this position in the New York Code of Professional Responsibility ("Code").[43] Under the Code, a lawyer may not engage in conduct that involves "dishonesty, fraud, deceit, or misrepresentation" or that is "prejudicial to the administration of justice."[44] And while lawyers are ethically bound to zealously represent their clients,[45] any such zealous representation must remain "within the bounds of the law, which includes Disciplinary Rules and enforceable professional regulations."[46]

To further support its view, the NYCLA Committee drew an analogy to the more general issue of "inadvertently disclosed privileged information."[47] In an earlier ethics opinion on that topic, the NYCLA Committee recommended immediately reporting any inadvertent disclosure to opposing counsel and ceasing to review the inadvertently disclosed document.[48] Ironically, support for that opinion came directly from the ABA's Model Rule 4.4(b)—the same rule that the ABA Committee found inapplicable to metadata because of the difficulty in determining whether metadata disclosure is inadvertent.[49] The NYCLA

---

[42] *Id.*

[43] *Id.* ("While the New York Code of Professional Responsibility . . . does not directly address this issue, several disciplinary rules and ethical considerations in the Code relate to the topic."). The Code served as New York's ethical guidelines until April 1, 2009, when New York adopted its Rules of Professional Conduct. Press Release, N.Y. Unified Ct. Sys., New Attorney Rules of Professional Conduct Announced (Dec. 16, 2008), *available at* http://www.courts.state.ny.us/press/pr2008_7.shtml. Despite the new rules' firm grounding in the ABA's Model Rules, this author questions the timing of the change—is April Fool's Day the appropriate occasion to adopt a new set of ethical guidelines?

[44] N.Y. CODE OF PROF'L RESPONSIBILITY DR 1-102(A)(4)-(5) (2003).

[45] N.Y. CODE OF PROF'L RESPONSIBILITY DR 7-101 (2003) ("Representing a Client Zealously").

[46] N.Y. CODE OF PROF'L RESPONSIBILITY EC 7-1 (2003).

[47] NYCLA, *supra* note 2, at 2.

[48] NYCLA Comm. on Prof'l Ethics, Formal Op. 730 (2002), *available at* http://www.nyclamail.org/siteFiles/Publications/Publications266_0.pdf ("If a lawyer receives information which the lawyer knows or believes was not intended for the lawyer and contains secrets, confidences or other privileged matter, the lawyer, upon recognition of same, shall, without further review or other use thereof, notify the sender and (insofar as it shall have been in written or other tangible form) abide by sender's instructions regarding return or destruction of the information.").

[49] ABA, *supra* note 1, at 3–4 n.9 (citing MODEL RULES OF PROF'L CONDUCT R. 4.4(b) (2004)); MODEL RULES OF PROF'L CONDUCT R. 4.4(b) (2004) ("A lawyer who receives a document relating to the representation of the lawyer's client and

Committee reasoned that actively "mining for metadata" could only mean using the guise of zealous representation to search for either attorney work product or privileged client information, neither of which the sending attorney would have intended to disclose.[50] "Mining for metadata," it follows, is essentially an intentional attempt to find information that was never intended for the receiving attorney's eyes. New York thus deems a receiving attorney's active search for that type of information unethical.

But New York does carve out two exceptions—situations where viewing metadata would not be unethical. First, if the sending attorney sends a document with "tracked changes" showing, and the receiving attorney reasonably believes that the disclosure is intentional, perhaps because it has been part of a normal course of business, the receiving attorney may view the "tracked changes."[51] Second, if a lawyer is facing a *pro se* litigant and suspects that another lawyer is actually drafting that *pro se* litigant's filings, the receiving lawyer may "mine for metadata" to determine whether her suspicions are well-founded.[52] This makes sense because a *pro se* litigant does not enjoy the privilege that surrounds an attorney-client relationship.

The NYCLA opinion did not shy away from its conflict with the ABA, but rather confronted it head-on. After recognizing the ABA's conflicting viewpoint and underlying rationale, the NYCLA Committee bluntly stated, "the NYSBA rule is a better interpretation of the Code's disciplinary rules and ethical considerations and New York precedents than the ABA's opinion on this issue."[53]

To sum up New York's position, sending attorneys must take due care to "scrub" electronic documents before sending them to opposing counsel, but receiving attorneys that believe a document includes inadvertently sent metadata may not ethically "mine."[54]

knows or reasonably should know that the document was inadvertently sent shall promptly notify the sender."); s*ee also* NYCLA, *supra* note 2, at 5 (stating that the committee's guidance is modeled by, *inter alia*, the ABA Model Rule 4.4(b)).

[50] NYCLA, *supra* note 2.

[51] *Id*.

[52] *Id*.

[53] *Id*. (emphasis added).

[54] *Id*.

C. Resolving the Conflict With Help From Other Jurisdictions

The problem of conflicting opinions between the ABA and a state's ethics committee is not unique to New York. The bars of Alabama, Arizona, and Florida are firmly in New York's camp with regard to "mining for metadata," and thus at odds with the ABA. Of those three, Alabama takes the strongest position by stating that "[t]he 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."[55] Likewise, Arizona declined to follow the ABA opinion because, under the ABA's view, "the sending lawyer would be at the mercy of the recipient lawyer . . . . [T]he sending lawyer might conclude that the only ethically safe course of action is to forego the use of electronic document transmission entirely. We do not think that is realistic or necessary."[56] Florida, in turn, advises against "mining for metadata" and requires notifying the sending attorney in the event that metadata is uncovered.[57] All three opinions cite to previous New York State ethics opinions.[58] The only states squarely in the ABA's camp appear to be Maryland and Colorado, whose bar associations both held that it is not unethical to "mine for metadata."[59]

Without suggesting that New York lawyers violate their duty to follow ethical rules, approaches used by several other jurisdictions—those whose opinions on "mining for metadata" fall between the two extreme positions laid out by the ABA and NYCLA—may help New Yorkers navigate any gray area.

[55] Ala. St. B. Off. Gen. Couns., Formal Op. 2007-02 (2007), *available at* http://www.alabar.org/ogc/fopDisplay.cfm?oneId=412.

[56] St. B. Ariz. Ethics Comm., Formal Op. 07-03 (2007), *available at* http://www.myazbar.org/ethics/printop.cfm?id=695.

[57] Fla. Prof'l Ethics Comm., Op. 06-2 (2006), *available at* https://www.floridabar.org/tfb/tfbetopin.nsf/SearchView/ETHICS,+OPINION+06-2?opendocument.

[58] *Id.* at n.3; Ala. St. B. Off. Gen. Couns., *supra* note 55; St. B. Ariz. Ethics Comm., *supra* note 56.

[59] *See* Md. St. B. Ass'n Comm. on Ethics, Op. 2007-09 (2006), *available at* http://www.msba.org/events/soloconference/08/materials/pdfs/04iwpypRaschkeMDEthicsOp2007-09.pdf ("[T]his Committee believes that there is no ethical violation if the recipient attorney (or those working under the attorney's discretion) reviews or makes use of the metadata without first ascertaining whether the sender intended to include such metadata."); Colo. B. Ass'n Ethics Comm., Formal Op. 119 (2008), *available at* http://www.cobar.org/index.cfm/ID/386/subID/23789/CETH// ("[A] Receiving Lawyer generally may ethically search for and review metadata embedded in an electronic document that the Receiving Lawyer receives from opposing counsel or other third party.").

Pennsylvania is one such state. The Pennsylvania Bar refused to apply a bright-line rule to metadata issues, stating that "each attorney must . . . determine for himself or herself whether to utilize the metadata contained in documents and other electronic files based upon the lawyer's judgment and the particular factual situation."[60] The following factors inform a Pennsylvania receiving attorney's decision on whether to "mine": the attorney's view of his or her obligations to the client; the nature of the information received; how and from whom the information was received; and common sense, reciprocity, and professional courtesy.[61]

The District of Columbia Bar takes a unique approach. Recognizing that the exchange of metadata is usually harmless, it suggests asking first whether the receiving lawyer has actual knowledge that the metadata was sent inadvertently.[62] If not, "a receiving lawyer is free to review the metadata contained within the electronic files provided by an adversary."[63]

IV. PRACTICAL TIPS TO AVOID INADVERTENT METADATA DISCLOSURE

For the twenty-first century New York lawyer who cannot simply avoid metadata problems by reverting to "snail mail" and facsimile, ways to avoid metadata disclosure problems abound, and range from the simple to the highly technological.

First, since metadata disclosure problems arise as soon as metadata is created, lawyers must take steps to avoid creating metadata in the first place by using Microsoft Word[64] in the following ways:

- First and foremost, know when the "track changes" feature is turned on. Microsoft Office's website offers instructions entitled "Get rid of tracked changes and comments, once and for all" at http://office.microsoft.com/en-us/word/HA010983881033.aspx. This website will allow a previously unsavvy lawyer to take control of

60 Pa. B. Ass'n, Formal Op. 2007-500 (2008) (not available online, but at 30-FEB Pa. Law. 46).

61 *Id.*

62 *See* D.C. B. Legal Ethics Comm., Op. 341 (2007), *available at* http://www.dcbar.org/for_lawyers/ethics/legal_ethics/opinions/opinion341.cfm.

63 *Id*.

64 For tips on avoiding the creation of metadata in Microsoft Excel and Microsoft Power Point, *see* Hricik & Scott, *supra* note 6, at 21–22.

this highly useful (but potentially disastrous) feature.[65]

- Rather than sending documents that are saved to your hard drive, use "Save As" to save them separately to a flash drive, then send that copy to the opposition. This avoids revealing information about the user's computer or network.[66]
- Under "Tools," "Options," "Security," check the box entitled "Remove personal information from file properties on save." This also prevents sensitive information about your computer or network from attaching to the document.[67]
- An author that wishes to remove his own name or other information about the document itself should go to "File," "Properties," "Summary," delete any unwanted text, and click "OK."[68]
- Avoid leaving hidden data on your document by turning off the aforementioned "fast saves" feature. Go to "Tools," "Options," "Save," and uncheck the box next to "allow fast saves."[69]
- Avoid saving multiple versions of a document by going to "File," "Versions," and deleting any unwanted versions from the list.[70]

Second, there are steps that lawyers can take to remove embedded data before transmitting a document:

- "Scrubbers" (which are alluded to above as recommendations of both the ABA and NYCLA Committees) are the most comprehensive and efficient way to prevent metadata disclosure. "Scrubbing" programs scan and eliminate metadata from a document before it is sent as an email attachment.[71]

---

[65] For a comprehensive look at the problems that the "track changes" feature can create, advice on how to solve them, and links to websites that offer tips on using Microsoft Word's most recent versions, *see* Mighell & Kennedy, *supra* note 14.

[66] *See* Microsoft Support, *How to Minimize Metadata in Word 2003*, http://support.microsoft.com/kb/825576/ (last visited Dec. 20, 2009) (suggesting use of a floppy disk for such purposes, although a flash drive may serve as a substitute).

[67] Hricik & Scott, *supra* note 6, at 21.

[68] *Id*.

[69] *Id*.

[70] *Id*.

[71] *See* ABA, *supra* note 1, at 5 (stating that embedded information can be eliminated or "scrubbed" before sharing that document with others); *see also*

- Save Word files in PDF or RTF form before transmitting. Both of these formats cut down on the amount of metadata stored, but have drawbacks as well: PDF files are much larger and RTF files often sacrifice formatting.[72]
- Install the add-in that Microsoft created for Word users concerned about metadata disclosure. The add-in, downloadable from Microsoft's web site, creates an option under "File" called "Remove Hidden Data." This will eliminate much already-created metadata.[73]
- For smaller documents, consider scanning them and sending the scanned image of the document, rather than the document itself.[74]

Finally, where lawyers on both sides of a dispute or transaction recognize the potential for disaster that an inadvertent metadata disclosure poses, there are the following options:

- Negotiate a confidentiality agreement with opposing counsel stating that any metadata disclosures are unintentional and will be deleted immediately.[75]
- Litigators may negotiate a protective order whereby a party can prevent the introduction of any evidence based on either a document that contains embedded information or the embedded information itself.[76]

V. A FEW SIMPLE WAYS TO "MINE FOR METADATA"

Maybe you do not practice law in New York State. Maybe New York will one day relax its view toward "mining for metadata." Or maybe you would just like to know whether your son started

BEC Legal Systems, Document Management Software, http://www.beclegal.com/products.aspx?id=64 (last visited Dec. 20, 2009) (providing MetaReveal, a Microsoft Office add-in software application used to scrub embedded information). The specifics of these programs are beyond the scope of this paper, but numerous versions are readily available for purchase on the Internet.

[72] Toby Brown, *Special Handling: How Paper and Electronic Files Differ*, GPSOLO MAG., Sept. 2004, *available at* http://www.abanet.org/genpractice/magazine/2004/sep/practice2.html.

[73] *See* Hricik & Scott, *supra* note 6, at 22. To download this add-in, search for "remove hidden data" on http://www.microsoft.com/downloads.

[74] *See* ABA, *supra* note 1, at 5.

[75] Hricik & Scott, *supra* note 6, at 24.

[76] *See* ABA, *supra* note 1, at 5 ("Of course, if the embedded information is on a subject such as [a] client's willingness to settle at a particular price, then there might be no way to 'pull back' that information.").

writing that term paper when he said he did. In any case, it can be useful to know where to find a document's embedded information. This section offers four simple ways to "mine for metadata" in Microsoft Word documents.

First, the most basic metadata in Word is located under "File," "Properties." Those two mouse clicks reveal, among other things, the document's author, date of creation, number of times it has been opened and closed (which implies its level of revision), and word count.[77]

Second, examine whether any "tracked changes" have been made to the document. Go to "View," "Toolbars," and check the "Reviewing" tab. Then go to "Show" on the "Reviewing" toolbar (which should now be in plain view to the top-left of your document) and click on "Comments" or "Insertions and Deletions" to see if any comments or changes have been made.[78]

Third, take advantage of the glitch in Word's "fast saves" feature by opening a Word document with another program, such as Notepad. If the transmitting person was using "fast saves," this will reveal any deleted information from earlier versions of the document because "fast saves" stores that information at the end of that document.[79]

Finally, examine whether any prior versions of the document exist within the file, when they were created, and any accompanying comments, by simply clicking "File," "Versions."[80]

VI. CONCLUSION

Metadata poses a variety of ethical concerns for attorneys across jurisdictions. Sending attorneys always owe their clients a duty of confidentiality that includes "scrubbing" documents before transmitting to avoid inadvertent disclosures. However, a receiving attorney's ethical obligations vary. Attorneys practicing in states that have adopted the ABA Model Rules are free to "mine for metadata" in any document they receive. New York attorneys, however, may not ethically do so.

The best advice for attorneys near and far is to (1) know what computer features have the potential to create an inadvertent

---

77 Hricik & Scott, *supra* note 6, at 17–18.

78 Microsoft Office Online, *Get Rid of Tracked Changes and Comments, Once and For All*, http://office.microsoft.com/en-us/word/HA010983881033.aspx (last visited Dec. 20, 2009).

79 Brown, *supra* note 72.

80 Hricik & Scott, *supra* note 6, at 21.

disclosure; and (2) have a plan of attack for eliminating unwanted metadata before transmitting documents to opposing counsel. A comprehensive "scrubbing" program is best, but the more primitive measures mentioned above will suffice in a crunch. Remember, the time you take to safeguard your documents could save your client millions.