TO SCRUB OR NOT TO SCRUB: THE ETHICAL IMPLICATIONS OF METADATA AND ELECTRONIC DATA CREATION, EXCHANGE, AND DISCOVERY

INTRODUCTION 469
I. METADATA—THE BASICS 472
II. TO SCRUB . . . METADATA, THE ATTORNEY–CLIENT PRIVILEGE, WORK PRODUCT, AND ETHICAL CONSIDERATIONS 475
A. Waiver of Attorney–Client Privilege and Work-Product Protection 476
1. Legal Standards of Waiver 476
2. Potential Waiver Through Inadvertent Disclosure of Metadata 481
B. Ethical Duties of Attorneys 483
1. Ethical Duties of the Sending Attorney 484
2. Ethical Duties of the Receiving Attorney 485
III. NOT TO SCRUB . . . METADATA AND CIVIL DISCOVERY 490
A. The Client's Duty to Preserve Metadata 491
B. The Client's Duty to Produce Metadata Under Rule 34 492
CONCLUSION 496

INTRODUCTION

The rise of electronic data creation, exchange, filing, and production in litigation has transformed the legal landscape and forced attorneys to reconceptualize their approach to issues such as attorney–client confidentiality and evidence spoliation. Deleting a sentence from the text of a pleading or altering data in the cells of spreadsheets does not mean that the corresponding data has completely disappeared. Long after an item is "deleted," metadata that contains the original sentences or data remains hidden in the document. Metadata can roughly be defined as data about data. For example, metadata often reports the author's name and initials; the name of the company or organization where the document was created; the name of the author's computer; the name of the server or network on which the document was saved; the names of previous document authors; the original text, along with any revisions to the original text; template information; any digital comments made on the document; document ver-

sions; and hidden text.[1] It is essentially information about the document's creation and about prior versions of that document. Often the rules that govern legal practice are ill-equipped to address the issues raised by such technological innovations, frequently leaving members of the legal profession questioning how standards developed decades earlier impact the e-practices of the present. Metadata raises two distinct issues that impact lawyers.

First, metadata raises significant issues concerning confidentiality for attorneys. Depending upon the law of the jurisdiction, an attorney who sends a document that she has created and edited without removing the metadata may be held to have waived the attorney–client privilege or work-product protection. When a document is transmitted to an adverse party, electronically filed with the court, or disclosed to the public with its metadata intact, a third party might attempt to "mine," or intentionally reveal and review, that metadata, potentially discovering confidential client information. For example, in February 2004 SCO Group, licensors of the UNIX operating system, filed a complaint in the circuit court for Oakland County, Michigan against DaimlerChrysler and AutoZone for violation of their software licensing agreements with SCO.[2] Attorneys for SCO failed to remove the hidden metadata within the pleading, which subsequently revealed that SCO had initially spent considerable time developing a case against Bank of America, to be filed in a California federal court.[3] The metadata further revealed the exact date and time at which the last-minute changes were made to the pleadings, reflecting SCO's decision to file against DaimlerChrysler and AutoZone in Michigan state court instead.[4] By failing to "scrub" the metadata from the pleading, SCO's attorneys may have waived their work-product protection with regard to the initial case against Bank of America. Additionally, SCO's attorneys may have potentially committed a violation of their ethical duty of confidentiality.

Lack of attention to metadata may also significantly embarrass a client. For example, in 2003, the British government was embarrassed by the exposure of metadata buried in a British report entitled *Iraq: Its Infrastructure of Concealment, Deception and Intimidation*, which they claimed was current[5] and "based on high-level British intelligence and diplomatic

1. *See* Microsoft Help & Support, *How to Minimize Metadata in Word 2003*, July 27, 2006, http://support.microsoft.com/default.aspx?scid=kb;en-us;825576 (follow "Summary" hyperlink).

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

3. *Id.*

4. *Id.*

5. Sarah Lyall, *Threats and Responses: Intelligence Assessments; Britain Admits That Much of its Report on Iraq Came from Magazines*, N.Y. TIMES, Feb. 8, 2003, at A9.

sources."[6] However, the report's metadata revealed that large amounts of text had actually been copied and pasted from a 2002 article, the data for which was gathered more than a decade ago.[7]

Accidental disclosure is not the only problem. Often battles arise from an opponent's knowing request for metadata in civil discovery. Metadata has become the frequent target of discovery requests in litigation involving business entities.[8] However, the issue of whether, under Federal Rule of Civil Procedure 34(b)(2)(E)(i), producing documents as they are kept in the usual course of business includes the accompanying metadata has yet to be settled. One source noted that "more than 90% of all corporate information is electronic; North American businesses exchange over 2.5 trillion e-mails per year; today, less than 1% of all communications will ever appear in paper form; and, on average, a 1000-person corporation will generate nearly 2 million e-mails annually."[9] Therefore, attorneys must understand what requirements courts are likely to place on their clients with regard to preserving the massive amount of metadata they produce each year.[10] Otherwise, clients run the risk of sanctions for evidence spoliation, or possibly criminal charges arising from the destruction of evidence. Additionally, production of metadata in response to requests for electronically stored information may result in high legal bills for clients. The privilege review associated with producing metadata is likely tedious and time consuming, driving ever higher the cost of litigating in the era of e-discovery.

Although metadata does raise a myriad of concerns in various areas of business and law, this Note confines its discussion largely to the obstacles and issues raised by metadata in the context of civil litigation. This Note highlights the various pitfalls that metadata poses for attorneys and their clients, and advises attorneys of the best course of action to avoid such dangers. Ultimately, the goal of this Note is to equip attorneys to answer the question: "To Scrub or Not to Scrub." Part I discusses the basics of metadata: what it is, how it is created, what information it stores, and how it can be removed. Part II discusses ethical issues regarding inadvertent production of metadata. First, Part II explores attorneys' ethical obligations to remove metadata in order to preserve the attorney–client privilege or work-product protection. Next, Part II discusses the ethical dilemmas

6. Barry Rubin, *British Government Plagiarizes MERIA Journal: Our Response*, MIDDLE E. REV. INT'L AFF., http://meria.idc.ac.il/british-govt-plagiarizes-meria.html.

7. *Id.* For the plagiarized article, *see* Ibrahim al-Marashi, *Iraq's Security and Intelligence Network: A Guide and Analysis*, 6 MIDDLE E. REV. INT'L AFF., Sept. 2002, at 1, *available at* http://meria.idc.ac.il/journal/2002/issue3/al-marashi.pdf.

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

9. Harvey L. Kaplan, *Electronic Discovery in the 21st Century: Is Help on the Way?*, *in* ELECTRONIC DISCOVERY AND RETENTION GUIDANCE FOR CORPORATE COUNSEL 2005, at 65, 67 (PLI Litig. & Admin. Practice, Course Handbook Series No. 733, 2005) (citations omitted).

10. *See* discussion *infra* Part III.

faced by attorneys who receive documents containing valuable metadata. Finally, Part III discusses metadata as a subject of civil discovery. It examines attorneys' duties to preserve relevant metadata, and the potential burdens of producing metadata pursuant to a discovery request.

I. METADATA—THE BASICS

Metadata has been defined as "definitional data that provides information about or documentation of other data managed within an application or environment."[11] In other words, metadata is "a set of data that describes and gives information about other data."[12] Metadata is essentially the history of a document. Every comment, every edit, every iteration of a document is hidden within that document, chronicling its life.[13] Metadata is important for efficient "editing, viewing, filing, and retrieval" of documents.[14] For example, if one were to type a single page of text within a Microsoft Word document, one could hit the "undo" button repeatedly until the document was "unwritten" and then hit the "redo" button until the document was entirely re-written. This is possible because the text that was initially input into the document was also stored as metadata within the document.[15]

Metadata was originally developed "by software programmers accustomed to working in collaborative environments where sharing information is commonplace."[16] As in the working environments of software programmers, collaboration is a common, arguably necessary, element of law firm productivity. Thus, metadata is a helpful component of software that enables partners and associates to refine their work product. In a 2001 press release, Microsoft revealed that it solicited the opinions of attorneys in developing Word 2002 because "the legal profession must have an efficient way to compare documents and incorporate text and formatting changes."[17]

The metadata of a typical Microsoft Word document may include: the author's name and initials; the name of the company or organization where

11. Brian D. Zall, *Metadata: Hidden Information in Microsoft Word Documents and Its Ethical Implications*, 33 COLO. LAW., Oct. 2004, at 53, 53 (quoting definition of metadata then found at Webopedia.com, http://isp.webopedia.com/TERM/M/metadata.html).

12. THE NEW OXFORD AMERICAN DICTIONARY 1065 (2d ed. 2005).

13. *See generally* Zall, *supra* note 11, at 54 ("Metadata operates like a diary or log in tracking the development of documents.").

14. Microsoft Help & Support, *supra* note 1.

15. *See generally* J. Brian Beckham, *Production, Preservation, and Disclosure of Metadata*, 7 COLUM. SCI. & TECH. L. REV. 1, 3–4 (2006), *available at* http://www.stlr.org/html/volume7/beckham.pdf.

16. Zall, *supra* note 11, at 54.

17. Press Release, Microsoft, The Jury's In: New Office XP and Word 2002 Features Create a Premier Solution for Legal Professionals (Mar. 19, 2001), *available at* http://www.microsoft.com/presspass/features/2001/mar01/03-19officexplegal.mspx.

the document was created; the name of the author's computer; the name of the server or network on which the document was saved; the names of previous document authors; the original text, along with any revisions to the original text; template information; any digital comments made on the document; document versions; and hidden text.[18] Metadata is also produced by Corel WordPerfect and other popular word processing software,[19] Microsoft Excel and PowerPoint, and other similar programs.[20] Furthermore, e-mails also contain metadata.[21] One commentator noted that e-mail metadata "can be used to settle disputes over when information was exchanged, the fabrication of documents by interested parties, and the policies and practices of a company."[22]

Despite its potential benefits, however, inadvertent disclosure of metadata containing confidential information could be catastrophic for inattentive attorneys. However, there are several ways to reduce or remove the amount of metadata a document contains, thus minimizing its potentially harmful effects. First, simply converting a document from its original editable Word or WordPerfect format to a PDF[23] will reduce some of the more sensitive metadata. However, many legal professionals mistakenly believe that converting documents into PDF files *alone* will completely solve their metadata woes. Unfortunately, PDF files also contain a healthy amount of metadata.[24] According to Donna Payne of the Payne Consulting Group, a legal consulting firm specializing in metadata removal, PDF files may contain information regarding: Authors, Create Data, Filename, PDF Version, Page Count, Encryption Status, Permanent ID, Changing ID, Producer, Creator, Custom Fields, Title, Subject, Keywords, Modification

18. *See* Microsoft Help & Support, *supra* note 1; *see also* Beckham, *supra* note 15, at 4; Zall, *supra* note 11, at 54.

19. *See* Beckham, *supra* note 15, at 4.

20. *See, e.g.*, Microsoft Office Online Help & How-to, *Find and Remove Metadata (Hidden Information) in Your Legal Documents*, http://office.microsoft.com/en-us/help/HA010776461033.aspx (last visited Dec. 12, 2008).

21. *See* Beckham, *supra* note 15, at 4–5.

22. *Id.* at 5.

23. PDF (portable document format) files, most often created using Adobe Acrobat, "provide[] an electronic image of text or text and graphics that looks like a printed document." THE NEW OXFORD AMERICAN DICTIONARY 1250 (2d ed.). PDF files are "essentially a photocopy of an electronic document viewed as a picture on a users [sic] screen." Beckham, *supra* note 15, at 5.

24. *See* DONNA PAYNE, METADATA—ARE YOU PROTECTED? 1–2 (2004), http://www.payneconsulting.com/pub_books/articles/pdf/MidwestBarAssociationConferenceMetadataHandout.pdf. Payne quotes Sherry Kappel, Vice President of Development at Microsystems, noting that PDF files still contain metadata:

> Adobe's integration to Microsoft Office apps provides us *unparalleled* electronic publishing capabilities—but with those capabilities come heightened responsibilities: [A]re tracked revisions accepted? [C]omments suppressed? [D]ocument information up to date? [R]edaction techniques electronically savvy? Without checklisting these issues within your document workflow, QC processes and job configuration, *a PDF file is as much the "swimsuit competition" as sending the editable .doc file itself.*

Id. at 2 (second emphasis added).

Date, Bookmarks (Total number), Annotations (total number, type and total type amount), Page One Size, and Font Name, Type, and Embed Status.[25] Thus, "[t]he least revealing electronic paper, then, is also the least functional: printing the document to paper, then scan [sic] it into PDF."[26] According to Payne, however, "[t]here is at least one third-party utility to help eliminate the risk of PDF metadata."[27]

Additionally, there are a number of free metadata removal options available. Microsoft has posted several articles detailing step-by-step *do-it-yourself* metadata removal techniques.[28] These techniques include manually turning off fast saves, searching for and removing text that is formatted as hidden, and manually removing comments from a document, among other helpful methods.[29] Microsoft has also developed an add-in feature for newer versions of Microsoft Office that will remove unwanted metadata.[30] However, this add-in only removes metadata created by the track changes and comments features.[31] Commentators have noted "that the Microsoft updates and self-help solutions are not foolproof . . . the uninformed or typical computer user likely will overlook an issue and experience problems in implementing the solution."[32] Corel, the maker of WordPerfect, notes on its website that "WordPerfect handles metadata differently from Word. Features that might store hidden or attached data are readily available, so confidential or sensitive information can be removed from a file before it is shared electronically."[33] WordPerfect X3 contains a feature that allows users to save documents without metadata.[34] However, earlier versions of WordPerfect do not contain this feature, and require the manual clean-up of metadata.[35] Further, WordPerfect X3 does not automatically prompt users to save without metadata.[36] Therefore, users must be aware of the feature and save files without metadata on their

25. *Id.*
26. *Id.* (internal quotation marks omitted).
27. *Id.* at 4. Appligent offers downloadable software on its redaction page that attorneys may purchase to remove any residual metadata from Adobe Acrobat files. *See generally* Appligent, Products, http://www.appligent.com/products/products.php (last visited Feb. 13, 2009).
28. *See, e.g.*, Microsoft Help & Support, *supra* note 1.
29. *Id.*
30. *See* Microsoft Download Center, Office 2003/XP Add-in: Remove Hidden Data (July 8, 2008), http://www.microsoft.com/downloads/ (Search "All Downloads" for "Remove Hidden Data"; then follow "Office 2003/XP Add-in: Remove Hidden Data" hyperlink).
31. *See* Campbell C. Steele, Note, *Attorneys Beware: Metadata's Impact on Privilege, Work Product, and the Ethical Rules*, 35 U. MEM. L. REV. 911, 948 (2005).
32. Zall, *supra* note 11, at 58 ("Microsoft apparently agrees with [these noted limitations] because it posted a disclaimer on its website indicating that its proposed 'solutions' are for illustration only, without warranty as to their fitness for a particular purpose.").
33. Laura Acklen, *Saving WordPerfect Files Without Metadata*, http://www.corel.com/servlet/Satellite/us/en/Content/1153321341830 (last visited Dec. 12, 2008).
34. *Id.*
35. *Id.*
36. *See id.*

own initiative, creating the risk that user oversight will leave metadata intact.

Metadata scrubbers, on the other hand, are typically very effective, when used correctly, at removing the most important components of metadata. Scrubbers are programs developed by legal consulting companies that "claim [to] have the ability to identify and eliminate some of the more harmful forms of metadata from documents."[37] Generally, these programs prompt users to scrub or remove all or part of the metadata contained within a document before it is transmitted electronically, minimizing the problem of overlooking the existence of metadata. Additionally, scrubbers are relatively inexpensive. Metadata Assistant, offered by the Payne Consulting Group, which "[f]or Word, Excel and PowerPoint documents[] [is] one of the most widely used metadata scrubbers,"[38] costs $79 per workstation plus an annual maintenance fee which varies depending on the number of workstations.[39] The licensing fee is a one-time payment, and there is no minimum number of licenses that must be purchased.[40] Enterprise licenses, which offer the same protection as the individual licenses, are available for larger firms at $64 per license; however, there is a purchase requirement of at least twenty licenses.[41] Those critical of scrubbers argue that "some metadata scrubbers may not integrate with documents forwarded electronically and often are subject to user error because of the level of user interaction required to initiate a metadata scan."[42] While there may be minor problems associated with metadata scrubbers, considering the potential for oversight or user error associated with the self-help solutions provided by Microsoft and Corel, generally they are the wisest investment to minimize the potential consequences posed by inadvertent disclosure of metadata containing confidential client information.[43]

II. TO SCRUB . . . METADATA, THE ATTORNEY–CLIENT PRIVILEGE, WORK PRODUCT, AND ETHICAL CONSIDERATIONS

Ignorance of the existence of metadata, or failure to adequately address its content, may result in the inadvertent waiver of the attorney–client privilege or work-product protection. Such inadvertent disclosure of confidential client information may expose the attorney to disciplinary

37. Zall, *supra* note 11, at 58.

38. LAWYER'S PROFESSIONAL INDEMNITY CO., MANAGING THE SECURITY AND PRIVACY OF ELECTRONIC DATA IN A LAW OFFICE 27 (2005), *available at* http://www.practicepro.ca/practice/pdf/ManagingSecurityPrivacy.pdf.

39. Telephone Interview with Dawn Thompson, Associate, Payne Consulting Group, in Seattle, Wash. (Feb. 28, 2008).

40. *Id.*

41. *Id.*

42. Zall, *supra* note 11, at 58.

43. *See* discussion *infra* Part II.

action by the relevant state bar association as well as constitute grounds for a future legal malpractice claim. On the other hand, attorneys who receive documents containing metadata may violate their ethical responsibilities by affirmatively "mining" such metadata.

A. Waiver of Attorney–Client Privilege and Work-Product Protection

The attorney–client privilege is among the oldest and most vital protections in the Anglo-American system of justice.[44] It protects communications between clients and their attorneys in order to "encourage full and frank communication between attorneys and their clients and thereby promote broader public interests in the observance of law and administration of justice."[45] It is well settled that the privilege resides with the client;[46] and therefore only the client may waive the protection provided by the privilege.[47] However, courts also acknowledge the inherent limitation that "the attorney's conduct [may] bind[] the client even in the absence of his express consent."[48]

1. Legal Standards of Waiver

The various jurisdictions have tended to adopt one of three approaches regarding when and to what extent the attorney–client privilege may be deemed to have been waived by an inadvertent disclosure of otherwise privileged information.[49] On one extreme, courts have found that any breach of the confidentiality necessary for the privilege to exist, by either

44. *See* 8 JOHN HENRY WIGMORE, WIGMORE ON EVIDENCE § 2290, at 542 (John T. McNaughton ed., Little, Brown & Co. 1961) (1904) (noting that the attorney–client privilege "already appear[ed] as unquestioned" at the time of the reign of Elizabeth I). *But see* Carol Rice Andrews, *Standards of Conduct for Lawyers: An 800-Year Evolution*, 57 S.M.U. L. Rev. 1385, 1405 (2004) ("Wigmore's historical account and purported justification for the privilege are subject to question . . . .").

45. Upjohn Co. v. United States, 449 U.S. 383, 389 (1981).

46. *See, e.g.*, *In re* Grand Jury Proceedings, Thursday Special Grand Jury, Sept. Term 1991, 33 F.3d 342, 348 (4th Cir. 1994) ("The client is the holder of the privilege."); *In re* von Bulow, 828 F.2d 94, 100 (2d Cir. 1987) ("Of course, the privilege belongs solely to the client . . . ."); Maloney v. Sisters of Charity Hosp. of Buffalo, N.Y., 165 F.R.D. 26, 29 (W.D.N.Y. 1995) (noting that "the privilege belongs to the client").

47. *See, e.g.*, Republic Gear Co. v. Borg–Warner Corp., 381 F.2d 551, 556 (2d Cir. 1967) ("[A]n attorney can neither invoke the privilege for his own benefit when his client desires to waive it nor *waive the privilege without his client's consent to the waiver*." (emphasis added)).

48. 2 PAUL R. RICE, ATTORNEY–CLIENT PRIVILEGE IN THE UNITED STATES § 9:10, at 9-28 (2d ed. 1999).

49. For a student note discussing the three approaches to waiver of the attorney–client privilege through inadvertent disclosure, see Steele, *supra* note 31, at 918–23. For additional discussions on the approaches, see also Gray v. Bicknell, 86 F.3d 1472, 1483 (8th Cir. 1996); Heidi McNeil Staudenmaier & Sara Vrotos, *The Inadvertenet Disclosure of Privileged Documents: Current State of the Law*, THE BRIEF, Spring 2003, at 30.

the client or the attorney, for whatever reason, results in waiver of the privilege (the strict-liability approach).[50] Wigmore noted:

> All *involuntary* disclosures, in particular, through the loss or theft of documents from the attorney's possession, are not protected by the privilege, on the principle . . . that, since the law has granted secrecy so far as its own process goes, it leaves to the client and attorney to take measures of caution sufficient to prevent being overheard by third persons. The risk of insufficient precautions is upon the client. *This principle applies equally to documents*.[51]

Proponents of the Wigmorian approach to attorney–client privilege emphasize that such a strict rule provides an added incentive for attorneys to take great care of such a fragile privilege for fear that the slightest of missteps may lead to waiver.[52] Critics of the strict-liability approach, however, argue that it "seems too harsh in light of the vast volume of documents disclosed in modern litigation."[53] Under the liberal modern discovery practices, where parties "may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense,"[54] which often results in voluminous document production, such a strict rule would place a virtually unmanageable burden on attorneys.

On the other end of the waiver spectrum, some courts have reasoned that since waiver is often defined as "[t]he voluntary relinquishment or abandonment—express or implied—of a legal right or advantage"[55] it is not possible to waive the privilege inadvertently (the intent-based approach).[56] Proponents of this approach reason that because the client is the privilege holder any disclosure of privileged information by the client's attorney, other than those disclosures authorized by the client, cannot result in a waiver.[57] Thus, because inadvertent disclosures are, by definition, unintentional or involuntary they cannot destroy a privilege, which may

50. *See, e.g.*, Hamilton v. Hamilton Steel Corp., 409 So. 2d 1111, 1114 (Fla. Dist. Ct. App. 1982).

51. WIGMORE, *supra* note 44, § 2325, at 633 (second emphasis added).

52. *See* Matthew J. Boettcher & Eric G. Tucciarone, *Concerns over Attorney–Client Communication Through E-mail: Is the Sky Really Falling?*, 2002 L. Rev. M.S.U.-D.C.L. 127, 136 (2002).

53. Fed. Deposit Ins. Corp. v. Marine Midland Realty Credit Corp., 138 F.R.D. 479, 481 (E.D. Va. 1991).

54. FED. R. CIV. P. 26(b)(1).

55. BLACK'S LAW DICTIONARY 1611 (8th ed. 2004).

56. *See, e.g.*, Trilogy Commc'ns, Inc. v. Excom Realty, Inc., 652 A.2d 1273, 1275 (N.J. Super. Ct. Law Div. 1994).

57. *See, e.g.*, Stratagem Dev. Corp. v. Heron Int'l N.V., 153 F.R.D. 535, 543 (S.D.N.Y 1994) ("A waiver must be intentional, however, to be effective. Where the disclosure is inadvertent, the privilege is not waived.") (citations omitted).

only be voluntarily waived.[58] Advocates of the intent-based approach argue that such a rule more adequately protects clients from their attorneys' negligence.[59]

Critics, however, argue that such an approach provides no incentive for attorneys to fervently guard their client's confidences.[60] Moreover, some critics urge that the intent-based approach is erroneously premised on an inapplicable standard.[61] Paul Rice notes in his treatise *Attorney–Client Privilege in the United States*, that "intentional relinquishment of a known right" is the standard for waiver of *constitutional rights*.[62] Rice argues that the attorney–client privilege is not a constitutional right, but rather is an evidentiary privilege, and thus the "intentional relinquishment" standard should not apply.[63]

A plurality of the jurisdictions have adopted an approach somewhere in between these two extremes, examining factors such as "the precautions taken to prevent the disclosure, the frequency of such incidents, the extent of the disclosure which has resulted, any aspects of compulsion surrounding the disclosure, the promptness of efforts to correct the disclosure, the interests of justice, and who the discloser was" (the middle-of-the-road approach).[64] Proponents of this approach note that it provides clients the most protection from "minor mistake[s] made by otherwise competent counsel"[65] that would otherwise result in waiver, while still forcing attorneys to be cognizant of the fragile nature of confidential attorney–client communications.[66]

Critics, however, point out that this approach fails to provide any meaningful guidance to attorneys regarding whether their actions will or will not waive the privilege, especially in light of ever-evolving technological capabilities.[67] Furthermore, one court noted that "court[s] applying

58. *See id.*

59. *See, e.g.*, Mendenhall v. Barber–Greene Co., 531 F. Supp. 951, 955 (N.D. Ill. 1982) ("[I]f we are serious about the attorney–client privilege and its relation to the *client's* welfare, we should require more than such negligence by *counsel* before the client can be deemed to have given up the privilege.") (emphasis added).

60. *See, e.g.*, Gray v. Bicknell, 86 F.3d 1472, 1483 (8th Cir. 1996).

61. *See* RICE, *supra* note 48, § 9:10, at 9-29.

62. *Id.* § 9:20, at 9-53; *see also* Johnson v. Zerbst, 304 U.S. 458, 464 (1938) (criminal defendant's right to counsel).

63. *See* RICE, *supra* note 48, § 9:20, at 9-53.

64. John T. Hundley, Annotation, *Waiver of Evidentiary Privilege by Inadvertent Disclosure—State Law*, 51 A.L.R. 5th 603, 634 (1997).

65. Patricia M. Worthy, *The Impact of New and Emerging Telecommunications Technologies: A Call to the Rescue of the Attorney–Client Privilege*, 39 HOW. L.J. 437, 461 (1996).

66. *See* Alldread v. City of Grenada, 988 F.2d 1425, 1434 (5th Cir. 1993) (noting that the middle-of-the-road approach "serves the purpose of the attorney client privilege, the protection of communications which the client fully intended would remain confidential, yet at the same time will not relieve those claiming the privilege of the consequences of their carelessness if the circumstances . . . do not clearly demonstrate that continued protection is warranted").

67. *Cf.* Natalie A. Kanellis, Comment, *Applicability of the Attorney–Client Privilege to Communications Intercepted by Third Parties*, 69 IOWA L. REV. 263, 274 (1983) ("Obviously, it is difficult to

th[is] doctrine to [inadvertent disclosures] come[] quite close to applying a *per se* rule or something akin to the doctrine of *res ipsa loquitur*."[68] The court argued that often courts evaluating the reasonableness of the precautions taken by the attorney tautologically reason that "the precautions were inadequate because they were not effective in preventing the disclosure of privileged documents. If the precautions had been adequate, the disclosure would not have occurred."[69]

Likewise, as with the attorney–client privilege, an attorney may waive work-product protection through inadvertently disclosing such material.[70] The treatment of the issue of waiver of work-product protection, however, has not varied as much as that of waiver of the attorney–client privilege.[71] Courts have tended to apply a balancing test similar to the middle-of-the-road approach to questions of waiver of the work-product protection by inadvertent disclosure.[72] Generally, courts have weighed the following five factors in determining whether waiver has occurred: (1) reasonableness of precautions taken to prevent disclosure, (2) time taken to rectify error, (3) scope of discovery, (4) extent of disclosure, and (5) overriding issues of fairness.[73]

On September 19, 2008, President Bush signed a bill amending the Federal Rules of Evidence to include a new rule of evidence specifically designed to address many of the problems associated with waiver of the attorney–client privilege and work-product protection—Federal Rule of Evidence 502.[74] Section (b) of Rule 502 specifically addresses waiver of the attorney–client privilege and work-product protection through inadvertent disclosure of privileged or protected material:

> When made in a Federal proceeding or to a Federal office or agency, the disclosure does not operate as a waiver in a Federal or State proceeding if:
>
> (1) the disclosure is inadvertent;

define 'reasonable' in concrete terms.").

68. Int'l Digital Sys. Corp. v. Digital Equip. Corp., 120 F.R.D. 445, 449 (D. Mass. 1988).

69. *Id.*

70. *See* United States v. Nobles, 422 U.S. 225, 239 (1975) ("The privilege derived from the work-product doctrine is not absolute. . . . [I]t may be waived.").

71. *See generally* 2 CHRISTOPHER B. MUELLER & LAIRD C. KIRKPATRICK, FEDERAL EVIDENCE § 5:38, at 727 (3d ed. 2007) ("Most courts consider the degree of fault on the part of the disclosing party and whether unfairness would result from upholding immunity under the circumstances.").

72. *See* 6 JAMES WM. MOORE ET AL., MOORE'S FEDERAL PRACTICE § 26.70[6][c] (3d ed. 2008).

73. *See id.*; *see also* Employer's Reinsurance Corp. v. Clarendon Nat'l Ins. Co., 213 F.R.D. 422, 428 (D. Kan. 2003); Sanner v. Bd. of Trade, 181 F.R.D. 374, 379 (N.D. Ill. 1998); Fleet Nat'l Bank v. Tonneson & Co., 150 F.R.D. 10, 15–16 (D. Mass. 1993); City of Worcester v. HCA Mgmt. Co., 839 F. Supp. 86, 89 (D. Mass. 1993).

74. Pub. L. No. 110-322, 122 Stat. 3537 (2008).

> (2) the holder of the privilege or protection took reasonable steps to prevent disclosure; and
>
> (3) the holder promptly took reasonable steps to rectify the error, including (if applicable) following Federal Rule of Civil Procedure 26(b)(5)(B).[75]

Rule 502 is designed to adopt the middle-of-the-road approach that a plurality of the courts have adopted.[76] However, the advisory committee decided not to codify the five factor test that most courts adopting the middle-of-the-road approach have applied. Rather, the committee states that the rule "is really a set of non-determinative guidelines that vary from case to case" and it is "flexible enough to accommodate any of those [five] listed factors."[77] Additionally, in cases where a disclosure is made at the state level, if the communication that is the subject of the state disclosure is offered in a subsequent federal proceeding, and the state and federal law governing waiver differ, section (c) instructs the federal courts to use either the state or the federal rule, whichever is more protective of the attorney–client privilege or work-product protection.[78]

Section (d) allows courts to enter orders—which are enforceable against both parties and nonparties in all subsequent state and federal proceedings—that govern whether and under what circumstances waiver has or will occur.[79] Section (e) allows the parties to enter into agreements, such as "clawback" and "quick peek" agreements,[80] governing the effect of disclosures made during the course of the pending litigation.[81] However, unlike section (d), agreements under section (e) are only enforceable for purposes of the current litigation, unless included in a court order under section (d).[82]

While Congress attempted to remedy many of the issues that waiver by inadvertent disclosure raises, it should be noted that there is disagreement as to the constitutionality of Rule 502.[83] Thus, while Rule 502 has received wide support from both the plaintiff and defense bars due to the stated goal of decreasing litigation costs, it is unclear whether Rule 502

75. FED. R. EVID. 502(b).
76. *See* FED. R. EVID. 502 advisory committee's note.
77. *Id.*
78. FED. R. EVID. 502(c).
79. FED. R. EVID. 502(d).
80. *See infra* notes 92–95 and accompanying text.
81. FED. R. EVID. 502(e).
82. *Id.*
83. For an excellent discussion of the myriad of constitutional issues raised by the enactment of Federal Rule of Evidence 502, see Henry S. Noyes, *Federal Rule of Evidence 502: Stirring the State Law of Privilege and Professional Responsibility with a Federal Stick*, 66 Wash. & Lee L. Rev. (forthcoming 2009), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1273325.

will withstand constitutional challenges. Additionally, Rule 502 is not the final pronouncement on the effect of inadvertent disclosures because virtually no state has adopted any rule of evidence based on Rule 502. Instead state courts continue to follow one of the three main approaches to waiver.

2. Potential Waiver Through Inadvertent Disclosure of Metadata

Virtually all documents attorneys create in the course of representing a client (whether in litigation or in a transaction) are created in digital form. With attorneys relying heavily on the use of e-mail to serve documents on opposing parties under Federal Rule of Civil Procedure 5,[84] and the advent of electronic filing in federal and state courts,[85] the dangers of inadvertent disclosure of privileged or protected information are heightened. Because metadata "is not immediately apparent when one opens a document, metadata can easily be missed in a privilege review."[86] Thus, an attorney's treatment of metadata will likely depend on which of the approaches to waiver that her particular jurisdiction follows.

An attorney practicing in a jurisdiction following the strict-liability approach must take all possible precautions to protect against an inadvertent disclosure of metadata. Failure to exercise such extraordinary care would likely result in a waiver of any privilege because the confidential nature of the information would have been destroyed, thus opening the disclosing attorney up to possible liability for legal malpractice. Furthermore, the disclosing attorney—depending on the jurisdiction—may have committed an ethical violation, resulting in possible disciplinary action by the appropriate bar association.[87] Given the fact that many attorneys are unsure as to what steps to take to adequately remove metadata, or are simply ignorant of the existence of metadata altogether, the result of inadvertent disclosure of metadata under the strict-liability approach seems too harsh an outcome for both attorneys and their clients alike. Such an approach—requiring

84. *See* FED. R. CIV. P. 5(b)(2)(E) (providing that a document is considered to have been properly served by "sending it by electronic means if the person consented in writing").

85. *See generally* Zall, *supra* note 11, at 55. Zall highlights the dangers that the electronic filing service in Colorado poses to attorneys ignorant of the disastrous consequences of metadata, noting:

> Counsel may file a document in Colorado state court with the LexisNexis File & Serve service, which is the statewide electronic filing system. When an MS Word document is uploaded to the website for conversion to Adobe Portable Document Format ("PDF") format, the original MS Word document—metadata included—is available and accessible to anyone with an account with the LexisNexis File & Serve service.

Id.

86. Dale M. Cendali, et al., *Potential Ethical Pitfalls in Electronic Discovery*, *in* ETHICS IN CONTEXT 2007: ETHICS AND ELECTRONIC DISCOVERY; ETHICS AND CORPORATE COMPLIANCE; ETHICS FOR COMMERCIAL LITIGATORS 105, 120 (PLI N.Y. Practice Skills, Course Handbook Series No. 171, 2007).

87. *See* discussion *infra* Part II.B.

absolute certainty in an inherently uncertain and complex technological environment—would likely have a chilling effect on electronic communication in the legal community.[88]

On the other hand, attorneys in jurisdictions that have adopted the intent-based approach may mistakenly give short shrift to the potentially disastrous effects of disclosure of the information in metadata, thinking that such a disclosure will not result in the waiver of the attorney–client privilege. To be certain, this approach would level the playing field between the more tech-savvy attorneys and the technologically illiterate by eliminating the threat that inadvertent disclosure of metadata would harm their client. However, the intent-based approach hardly seems adequate in dealing with disclosures of metadata because it fails to take into account the effects of any public disclosures. For example, it was media sources, and not the opposing party, that mined and published the contents of the metadata from the complaint in the SCO litigation.[89] If confidential information contained in the metadata of a legal document is made public, the rationale behind the intent-based approach would likely lose its relevance. Once confidential information is made public, asking attorneys and potential jurors (depending on how widely publicized the disclosure is) to essentially stick their heads in the sand and ignore the disclosed information is nearly impossible. Therefore, it only seems logical in such a case to find waiver.

The middle-of-the-road approach, however, seems to be the most appropriate approach to dealing with the inadvertent disclosure of sensitive information resulting from an attorney's failure to scrub metadata. This approach, which requires attorneys to adopt "reasonable precautions" to prevent disclosure,[90] does not completely absolve the attorney of any duty to scrub, thereby forcing attorneys to analyze the likely effect of their safety measures. While the concept of "reasonable precautions" is inherently subjective—often inviting courts to tautologically infer that when inadvertent disclosures occur the precautions were not reasonable—it seems to be the most appropriate inquiry when dealing with the evolving nature of electronic document creation, storage, and production. The reasonableness prong allows courts to examine a number of factors—including current state of technology, and the relative costs of safety measures—in their determination of whether privilege has been waived, rather than applying a hard and fast rule that does not take into account advances in technology and the problems associated with such advances.

88. *Cf.* Worthy, *supra* note 65, at 462 ("Such an approach increases substantially the threat to privileged communications, because courts would be forced to confront and resolve the issues of confidentiality based on the complexities of an ever-changing telecommunications environment.").

89. *See supra* notes 2–4 and accompanying text.

90. MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 16 (2002).

Additionally, the reasonable precautions standard of the middle-of-the-road approach is likely roughly equivalent to Model Rule of Professional Conduct 1.6's standard requiring that "method[s] of communication afford[] a reasonable expectation of privacy."[91] By aligning such standards, the analysis of whether waiver has occurred and whether an ethical violation has occurred would be more consistent. If a court finds that an attorney did not take reasonable precautions to prevent inadvertent disclosure, then it is also likely that the attorney neglected her duty to competently safeguard her client's confidences.

Additionally, one commentator has suggested the possibility of "clawback" or "quick peek" agreements among the parties to litigation that would address the effect of inadvertent disclosures that occur specifically within that litigation.[92] In a "clawback" agreement, the parties simply agree ahead of time that any inadvertent disclosure of privileged or protected information will not result in a waiver.[93] In a "quick peek" agreement, the parties agree ahead of time that a party requesting discovery may "preliminarily review materials without that review constituting a waiver of any privileged information therein."[94] Rule 16(b) of the Federal Rules of Civil Procedure allows courts to include agreements such as "clawbacks" and "quick peeks" in their scheduling orders, thus decreasing the likelihood that inadvertent disclosure will result in waiver.[95] However, whether such agreements are enforceable outside of the federal system is unclear, especially in jurisdictions that have adopted the strict-liability approach, which find waiver whenever the confidentiality of the communication is breached. Thus, it seems that while the interplay between the various approaches to waiver and most of the self-help prophylactic measures may soften the sting of accidental metadata disclosure, there is no substitute for scrubbing.

B. Ethical Duties of Attorneys

In addition to the possibility of waiver of the attorney–client privilege and work-product protection, attorneys who inadvertently disclose client

91. *See id.* For a more detailed discussion of Model Rule 1.6's requirements, see *infra* Part II.B.1.

92. *See* Cendali et al., *supra* note 86, at 121.

93. *See id.*

94. *Id.*

95. *See* FED. R. CIV. P. 16(b)(3)(B)(iv); *see also* FED. R. CIV. P. 26(b)(5)(B) advisory committee's note on 2006 amendments ("[S]uch agreements . . . may be considered when a court determines whether a waiver has occurred."); Hopson v. Mayor & City Council of Balt., 232 F.R.D. 228, 233–34 (D. Md. 2005) (noting that such agreements are one of several methods devised to "address the burdens of privilege review associated with production of electronically stored information . . . but at the price of risking waiver or forfeiture of privilege/work-product protection, depending on the substantive law of the jurisdiction in which the litigation was pending").

information contained in metadata may also run afoul of state ethical rules, subjecting them to possible disciplinary action. Moreover, attorneys choosing to affirmatively mine communications received from opposing parties for confidential information contained in the metadata may also subject themselves to sanctions for violating state ethical rules.

1. Ethical Duties of the Sending Attorney

All states impose an affirmative duty of confidentiality on lawyers, greater than the attorney–client privilege or the work-product protection. Most states have adopted some form of the American Bar Association's (ABA) Model Rules of Professional Conduct (Model Rules), while fewer than ten states have elected to retain its predecessor, the Model Code of Professional Responsibility (Model Code).[96] Rule 1.6 of the Model Rules states: "A lawyer shall not reveal information relating to the representation of a client."[97] While the Model Rules allow for disclosure of client confidences in very limited circumstances[98]—which are not applicable to the scenario at hand—the comments make it very clear that "[a] fundamental principle in the client-lawyer relationship is that, in the absence of the client's informed consent, the lawyer must not reveal information relating to the representation."[99]

The Model Rules require that an attorney act competently in safeguarding client confidences, which includes taking reasonable steps to ensure that confidentiality is maintained when transmitting a document.[100] Generally, lawyers are not required to take special security measures when transmitting a document that might contain confidential client information, provided that the method of transmission provides a "reasonable expectation of privacy."[101] However, determining whether technological advances in communication offer a reasonable expectation of privacy has historically proven difficult for state bar associations.[102] For example, bar associations were initially hesitant as to the reasonableness of the security offered by fax machines, noting that the increase in usage of fax machines made it "'ever more likely that through inadvertence, privileged or confidential

96. ABA Comm. on Evaluation of the Rules of Prof'l Conduct, Chair's Introduction (2002), *available at* http://www.abanet.org/cpr/mrpc/e2k_chair_intro.html (noting that forty-two jurisdictions, including the District of Columbia, have adopted some version of the Model Rules of Professional Conduct, while "[a] few states had elected to retain some version of the 1969 Model Code of Professional Responsibility, and California remained committed to an entirely separate system of lawyer regulation").

97. MODEL RULES OF PROF'L CONDUCT R. 1.6(a) (2002).

98. *See* MODEL RULES OF PROF'L CONDUCT R. 1.6(b).

99. MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 2.

100. MODEL RULES OF PROF'L CONDUCT R. 1.6 cmts. 16–17.

101. MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 16.

102. *See* Steele, *supra* note 31, at 929.

materials [would] be produced to opposing counsel by no more than the pushing of the wrong speed dial number on a facsimile machine.'"[103] Similarly, with the rise of e-mail in the 1990s, attorneys were concerned as to whether sending client documents via unencrypted e-mail afforded them a reasonable expectation of privacy.[104] Eventually the ABA noted that fax machines and unencrypted e-mails provide the same reasonable expectation of privacy as did the U.S. mail and telephone lines.[105]

2. Ethical Duties of the Receiving Attorney

While questions regarding the reasonableness of certain specific media of communication may have been answered for sending attorneys, attorneys receiving communications containing confidential information from an adverse party found themselves in an ethical quagmire. Model Rule 1.3 requires that "[a] lawyer shall act with reasonable diligence and promptness in representing a client."[106] As the comments note, this duty requires an attorney to "act with commitment and dedication to the interests of the client and with zeal in advocacy upon the client's behalf."[107] Thus, commentators have speculated that attorneys may not only be free, but may be duty bound to review and use confidential client information inadvertently produced by an adverse party.[108] However, it is professional misconduct for an attorney to "engage in conduct involving dishonesty, fraud, deceit or misrepresentation"[109] or "that is prejudicial to the administration of justice."[110] Thus, it was difficult for attorneys who had received information of a confidential nature from an adverse party to know what the ethical rules required of them.

In 1992, the ABA attempted to clear up this ethical quandary for attorneys who had received information of a confidential nature from an adverse party. The Committee on Ethics and Professional Responsibility opined that a receiving attorney must "avoid reviewing the materials, notify sending counsel if sending counsel remains ignorant of the problem and abide sending counsel's direction as to how to treat the disposition of the confidential materials."[111] However, the ABA withdrew this ethical opi-

103. *Id.* (alteration in original) (quoting ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 92-368 (1992)).
104. *Id.* at 930.
105. *See* ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 99-413 (1999) (unencrypted e-mails); ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 92-368 (1992) (fax machines).
106. MODEL RULES OF PROF'L CONDUCT R. 1.3 (2002).
107. MODEL RULES OF PROF'L CONDUCT R. 1.3 cmt. 1.
108. *See* Beckham, *supra* note 15, at 14.
109. MODEL RULES OF PROF'L CONDUCT R. 8.4(c) (2002).
110. MODEL RULES OF PROF'L CONDUCT R. 8.4(d).
111. ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 92-368 (1992) (finding that imposing such an obligation on receiving attorneys "not only fosters the important principle of confidentiality, avoids punishing the innocent client and conforms to the law of bailment, but also achieves

nion in 2005 after the ABA House of Delegates adopted amended Model Rule 4.4 in 2002.[112] Model Rule 4.4(b) simply 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."[113] The comments to Model Rule 4.4 note that "[w]hether the lawyer is required to take additional steps, such as returning the original document, is a matter of law beyond the scope of these Rules, as is the question of whether the privileged status of a document has been waived."[114]

Thus, it is unclear whether under the ABA's approach, an attorney who sends an adverse party an electronic document containing metadata relating to confidential client information has breached his or her duty of confidentiality. If rule 1.6(a) is strictly construed, it appears likely that a breach of the duty of confidentiality has occurred, thus subjecting the sending attorney to possible disciplinary action. However, considering the ABA's leniency regarding inadvertent disclosures through other media,[115] it is unclear whether it would in fact find a violation. Likewise, until recently, it was even more unclear what the ABA deemed the ethical responsibilities of an attorney who receives an electronic document containing metadata relating to confidential information of an adverse party. Under Model Rule 4.4(b), it is clear that the receiving attorney must notify the adverse party of the disclosure.[116] However, until 2006, neither Model Rule 4.4(b), nor any formal opinion issued by the ABA addressed to what extent the receiving attorney could, or should, affirmatively "mine" the metadata for such information.

Attempting to clarify its position, the ABA issued Formal Opinion 06-442 in 2006, which deals with the review and use of metadata. The ABA did not address whether an attorney who sends an adverse party an electronic document containing metadata relating to confidential client information has breached his or her duty of confidentiality, merely stating that "[a] lawyer who is concerned about the possibility of sending . . . a document that contains or might contain metadata . . . may be able to limit the likelihood of its transmission by 'scrubbing' metadata from documents."[117] However, it did expressly state that it did not consider a receiving attor-

---

a level of professionalism which can only redound to the lawyer's benefit").

112. *See* ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 05-437 (2005) (noting that Model Rule 4.4(b) imposed a lesser duty than Formal Opinion 92-368 had required).

113. MODEL RULES OF PROF'L CONDUCT R. 4.4(b) (2002).

114. MODEL RULES OF PROF'L CONDUCT R. 4.4 cmt. 2.

115. *See* ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 99-413 (1999) (opining that unencrypted e-mails provide a reasonable expectation of privacy); ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 92-368 (1992) (opining that fax machines provide a reasonable expectation of privacy).

116. *See* MODEL RULES OF PROF'L CONDUCT R. 4.4(b) (2002).

117. ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 06-442 (2006).

ney's mining of metadata to be an ethical violation, thus placing the onus of preserving the confidentiality solely on the sending attorney.[118]

While virtually every jurisdiction to have addressed the metadata dilemma has placed an ethical responsibility on sending attorneys to scrub, the ABA approach regarding the ethical obligations of receiving attorneys has not been met with universal acceptance.[119] In fact, the authorities are evenly split on the issue, with three of the eight jurisdictions to have directly addressed the scope of the duties of receiving attorneys adopting an approach similar to the ABA's.[120] For example, the District of Columbia Bar Association's approach prohibits attorneys having actual knowledge that the metadata was inadvertently included in a document received from an adverse party from reviewing such metadata.[121] While the D.C. approach does acknowledge that "actual knowledge may also exist where a receiving lawyer immediately notices upon review of the metadata that it is clear that protected information was unintentionally included,"[122] generally under the D.C. approach a receiving attorney lacking actual knowledge that metadata has been inadvertently included in an electronic document is free to review the contents of the metadata.[123] In 2008, the Colorado State Bar Association went one step further, noting that "where the Receiving Lawyer has no prior notice from the sender, the Receiving Lawyer's only duty upon viewing confidential metadata is to notify the Sending Lawyer."[124] Therefore, under the Colorado approach, a receiving attorney may review all metadata regardless of whether he or she has actual knowledge that it was inadvertently included in the electronic document, unless the

118. *Id.*

119. *See* Colo. Bar Ass'n Ethics Comm., Formal Op. 119 (2008); Ala. State Bar Office of the Gen. Counsel, Formal Op. RO-2007-02 (2007); State Bar of Ariz. Comm. on the R. of Prof'l Conduct, Formal Op. 07-03 (2007); D.C. Bar Legal Ethics Comm., Formal Op. 341 (2007); Md. State Bar Ass'n Comm. on Ethics, Formal Op. 2007-09 (2007); Fla. Bar Prof'l Ethics Comm., Formal Op. 06-2 (2006); N.Y. State Bar Ass'n Comm. on Prof'l Ethics, Formal Op. 782 (2004). Addressing to what extent an attorney is ethically obligated to release electronic documents to clients upon termination of employment, the California Bar Association noted that prior to releasing such documents the attorney must "take reasonable steps to strip any metadata reflecting confidential information belonging to other clients from any of the electronic items prior to releasing them." State Bar of Cal. Standing Comm. on Prof'l Responsibility and Conduct, Formal Op. 2007-174 (2007).

120. *See* Colo. Bar Ass'n Ethics Comm., Formal Op. 119 (2008); D.C. Bar Legal Ethics Comm., Formal Op. 341 (2007); Md. State Bar Ass'n Comm. on Ethics, Formal Op. 2007-09 (2007). It should be noted that the Pennsylvania Bar Association has also addressed the issue, but refused to adopt either the ABA approach or the New York approach, both discussed *infra*. Instead, Pennsylvania has adopted a framework of case-by-case analysis in lieu of establishing a bright line rule. *See* Pa. Bar Ass'n Comm. on Legal Ethics and Prof'l Responsibility, Formal Op. 2007-500 (2007).

121. D.C. Bar Legal Ethics Comm., Formal Op. 341 (2007).

122. *Id.*

123. *Id.* ("Given the ubiquitous exchange of electronic documents and the sending lawyers' obligation to avoid inadvertent productions of metadata, we believe that mere uncertainty by the receiving lawyer as to the inadvertence of the sender does not trigger an ethical obligation by the receiving lawyer to refrain from reviewing the metadata.").

124. Colo. Bar Ass'n Ethics Comm., Formal Op. 119 (2008).

sending attorney has specifically notified the receiving attorney prior to his or her review of the metadata.[125] The Maryland State Bar Association has adopted a similar approach placing the ethical duty to remove metadata on the sending attorney.[126] The Maryland State Bar Association, however, goes one step further than either the D.C. or Colorado bar associations, noting that since Maryland has not adopted any version of Model Rule of Professional Conduct 4.4, "there is no ethical violation if the recipient attorney (or those working under the attorney's direction) reviews or makes use of the metadata without first ascertaining whether the sender intended to include such metadata."[127]

In Opinion 782, the New York State Bar Association Committee on Professional Ethics found that sending attorneys must use reasonable care to ensure that confidential client information is not disclosed through metadata contained in documents exchanged with adverse parties.[128] However, the New York State Bar Association additionally prohibits receiving attorneys from mining metadata, noting that receiving attorneys "may not ethically use available technology to surreptitiously examine" metadata.[129] Following New York's lead, the Alabama, Arizona, and Florida State Bar Associations have also placed an ethical responsibility on both the sending attorney to remove all confidential client information from an electronic document's metadata before sending, and also on the receiving attorney to refrain from reviewing metadata containing such information.[130] Some commentators have opined that even in states that have not explicitly addressed the ethical issues presented by metadata, most state's ethical rules would likely impose requirements similar to those in Alabama, Arizona, Florida, and New York.[131]

Like the middle-of-the-road approach to waiver of the attorney client privilege and the work-product protection, the New York ethical model provides both an incentive to attorneys to exercise reasonable caution re-

125. *Id.* ("[W]here the Receiving Lawyer has prior notice from the sender of the inadvertent transmission of confidential metadata, Rule 4.4(c) does prohibit the Receiving Lawyer from reviewing the electronic document or file.").

126. *See* Md. State Bar Ass'n Comm. on Ethics, Formal Op. 2007-09 (2007).

127. *Id.*

128. *See* N.Y. State Bar Ass'n Comm. on Prof'l Ethics, Formal Op. 782 (2004) ("What constitutes reasonable care will vary with the circumstances, including the subject matter of the document, whether the document was based on a 'template' used in another matter for another client, whether there have been multiple drafts of the document with comments from multiple sources, whether the client has commented on the document, and the identity of the intended recipients of the document.").

129. *See* N.Y. State Bar Ass'n Comm. on Prof'l Ethics, Formal Op. 749 (2001).

130. *See* Ala. State Bar Office of the Gen. Counsel, Formal Op. 2007-02 (2007); State Bar of Ariz. Comm. on the R. of Prof'l Conduct, Formal Op. 07-03 (2007); Fla. Bar Prof'l Ethics Comm., Formal Op. 06-2 (2006). The New York County Lawyers Association also recently opined that "[a] lawyer who receives from an adversary electronic documents that appear to contain inadvertently produced metadata is ethically obligated to avoid searching the metadata in those documents." NYCLA Comm. on Prof'l Ethics, Formal Op. 738 (2008).

131. *See, e.g.*, Zall, *supra* note 11, at 56–58.

garding the presence of sensitive metadata before sending electronic documents and also protects the interests of clients whose attorneys have failed to scrub sensitive metadata out of documents before sending them to opposing counsel. Some courts have agreed, sanctioning attorneys for reviewing and using inadvertently produced documents that the attorneys knew or should have known to be privileged or protected as attorney work product.[132] As one court noted, "'[A]n attorney has an obligation not only to protect his client's interests but also to respect the legitimate interests of fellow members of the bar, the judiciary, and the administration of justice.'"[133] The court went on to note an opposing argument:

> Even apart from the inadvertent disclosure problem, the party responding to a request for mass production must engage in a laborious, time-consuming process. If the document producer is confronted with the additional prospect that any privileged documents inadvertently produced will become fair game for the opposition, the minute screening and re-screening that inevitably would follow not only would add enormously to that burden but would slow the pace of discovery to a degree sharply at odds with the general goal of expediting litigation.[134]

Unlike the case of inadvertently produced documents in which it is often difficult to determine if the documents were legitimately intended for opposing counsel without first reviewing them to some extent, inadvertently produced metadata presents a stronger case for requiring attorneys to refrain from reviewing such information. Presumably, an attorney does not mean for an opposing attorney to see the contents of the metadata of a document. If such contents were intended to be shared, an attorney would either call attention to the presence of such information, or more likely would simply include such data in the actual visible text itself.

By condoning metadata mining, the ABA and similar approaches not only fail to provide adequate protection to clients whose attorneys have overlooked the presence of metadata in the documents they have exchanged and contribute to the added expense and burden of litigation, but also contribute to an increasingly unprofessional and contentious environment by incentivizing the search for otherwise confidential information that was not intended to be shared. The New York approach, by also placing ethical obligations on receiving attorneys, renders metadata mining

132. *See, e.g.*, Am. Express v. Accu-Weather, Inc., No. 91 CIV. 6485 (RWS), 92 CIV. 705 (RWS), 1996 WL 346388 (S.D.N.Y. June 25, 1996); Rico v. Mitsubishi Motors Corp., 171 P.3d 1092 (Cal. 2007).

133. *Rico*, 171 P.3d at 1099 (quoting Kirsch v. Duryea, 578 P.2d 935, 939 (Cal. 1978)).

134. *Id.*

more risky and less likely, thus protecting the integrity of the adversarial system and the interests of clients against innocent mistakes made by their attorneys.

The Federal Rules of Civil Procedure were also amended in 2006 in an attempt to deal with some of the issues created by large amounts of electronic discovery.[135] Rule 26(b)(5)(B) was added to address the increased risk of inadvertent disclosure of privileged or protected material implicated by large amounts of electronic discovery.[136] Rule 26(b)(5)(B) is essentially a codified version of a "clawback" agreement, allowing a party who has inadvertently produced a privileged or protected document to notify the adverse party who then may not use the document in any way until the status of the privilege or protection is resolved.[137] However, it is important to note that Rule 26(b)(5)(B) simply governs discovery procedure in civil litigation. Thus, as the advisory committee has noted, "Rule 26(b)(5)(B) does not address whether the privilege or protection that is asserted after production was waived by the production. The courts have developed principles to determine whether, and under what circumstances, waiver results from inadvertent production of privileged or protected information."[138] Moreover, an attorney may still be held to have violated his or her Model Rule 1.6 duty of confidentiality regardless of the outcome of a Rule 26(b)(5)(B) hearing.

III. NOT TO SCRUB . . . METADATA AND CIVIL DISCOVERY

Metadata also presents another distinct, yet equally crucial, issue within the context of discovery. "'Electronic data has become the crucial source of discoverable evidence in corporate litigation and regulation.'"[139]

135. *See* FED. R. CIV. P. 26 advisory committee's note on 2006 amendments.

136. *See* FED. R. CIV. P. 26(b)(5)(B). In the advisory committee's notes for the 2006 amendments to the Federal Rules of Civil Procedure, the committee stated:

> The Committee has repeatedly been advised that the risk of privilege waiver, and the work necessary to avoid it, add to the costs and delay of discovery. When the review is of electronically stored information, the risk of waiver, and the time and effort required to avoid it, can increase substantially because of the volume of electronically stored information and the difficulty in ensuring that all information to be produced has in fact been reviewed.

FED. R. CIV. P. 26 advisory committee's note on 2006 amendments.

137. FED. R. CIV. P. 26(b)(5)(B) ("If information produced in discovery is subject to a claim of privilege or of protection as trial-preparation material, the party making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has; must not use or disclose the information until the claim is resolved; must take reasonable steps to retrieve the information if the party disclosed it before being notified; and may promptly present the information to the court under seal for a determination of the claim. The producing party must preserve the information until the claim is resolved.").

138. FED. R. CIV. P. 26 advisory committee's note on 2006 amendments.

139. Beckham, *supra* note 15, at 2 (quoting Evidence Exchange, Electronic Discovery of Data and Documents with Evidence Exchange, http://www.evidenceexchange.com (last visited Feb. 13, 2009)).

While attorneys should generally scrub all metadata from documents that they have generated in the course of representing a client before exchanging them with anyone, clients are generally under a duty to preserve all metadata that is produced in the course of business once they have received notice of an impending lawsuit.[140] Failure to preserve metadata may result in court-imposed sanctions for spoliation of evidence,[141] or at the extreme, criminal penalties for the destruction of evidence.[142] Metadata preservation and production also has the potential to impose a significant financial burden on clients.

A. The Client's Duty to Preserve Metadata

Corporations commonly destroy or delete documents as part of regular document retention plans. However, once a party "reasonably anticipates litigation" it is under a duty to preserve evidence.[143] While the filing of a complaint certainly gives rise to a reasonable anticipation of litigation, the duty to preserve may very well arise long before a complaint is ever filed.[144] A party is not required to preserve *all* of its documents and electronic information; rather, it must preserve "evidence [that] may be relevant to future litigation."[145] Determining what is likely to be relevant, however, may be difficult at the time that the duty to preserve arises, thus necessitating a broad litigation hold.

This duty should also include the preservation of metadata, as it may be relevant to a claim or defense.[146] Spoliation of relevant metadata may result in harsh sanctions by the court, including adverse jury instructions, default judgment, or dismissal.[147] Federal Rule of Civil Procedure 37(e) provides a safe harbor for clients, preventing the courts from imposing spoliation sanctions for electronic data that is disposed of as part of "rou-

140. *See generally* Cendali et al., *supra* note 86, at 113–16.

141. *See generally* Daniel Renwick Hodgman, Comment, *A Port in the Storm?: The Problematic and Shallow Safe Harbor for Electronic Discovery*, 101 NW. U. L. REV. 259, 267 (2007) ("The power vested in courts under their inherent authority includes the ability to sanction a party for spoliation of evidence.").

142. *See, e.g.*, 18 U.S.C. § 1512(c)(1) (Supp. 2005) (providing that "corruptly . . . alter[ing], destroy[ing], mutilat[ing], or conceal[ing] a record, document, or other object, or attempt[ing] to do so, with the intent to impair the object's integrity or availability for use in an official proceeding" is punishable by a fine and/or imprisonment of up to twenty years).

143. *See* Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 218 (S.D.N.Y. 2003).

144. *Id.* at 217 ("Merely because one or two employees contemplate the possibility [of a lawsuit] does not generally impose a firm-wide duty to preserve."). However, parties are under a duty to institute a litigation hold when they believe that the information that they have may be part of a lawsuit, whether or not it has been instituted yet. *See id.*

145. Broccoli v. Echostar Commc'ns Corp., 229 F.R.D. 506, 510 (D. Md. 2005).

146. *Cf.* Beckham, *supra* note 15, at 13 ("[M]etadata may reveal the date a certain fact was known, which is crucial in tort and product liability actions. Metadata may also serve to protect a party where forging of documents could be proven through metadata.").

147. *See* Clayton L. Barker & Philip W. Goodin, *Discovery of Electronically Stored Information*, 64 J. MO. B., Jan.–Feb. 2008, at 12, 19–20 (2008).

tine, good-faith operation of an electronic information system."[148] Therefore, business entities with electronic document retention programs in place will not be punished if an electronic file "slips through the cracks" of the litigation hold, so long as the retention program was being operated in good faith.[149] However, most states have not incorporated this safe harbor provision into their rules. Clients may also be held criminally liable for obstruction of justice if, having knowledge of a pending official proceeding, they destroy relevant metadata.[150] Generally, however, a client's destruction of, or failure to preserve, evidence only subjects him or her to criminal liability if he or she intended to impair the use of such evidence in an official proceeding.[151]

B. The Client's Duty to Produce Metadata Under Rule 34

The question of when production of metadata is required is significantly less clear. Rule 34(a) clearly allows discovery of "designated documents or *electronically stored information*."[152] Rule 34(b) allows parties to specify the form in which electronically stored information is to be produced.[153] Thus, if a party specifically requests electronically stored documents to be produced with metadata intact, the responding party is obligated to provide the metadata unless the responding party has a legitimate objection under the rules governing discovery to the discoverability of the metadata. The problem arises when the request for electronically stored documents does not address whether the associated metadata is to be produced. Rule 34(b) further requires a party, in response to a discovery request under Rule 34, to produce electronically stored information "in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms" unless another form is specified in the request.[154] Although Rule 26(f) of the Federal Rules of Civil Procedure requires parties to address "any issues about disclosure or discovery of electronically stored information, including the form or forms in which it should be produced" in their proposed discovery plan,[155] and Rule 16(b) allows the court to "provide for disclosure or discovery of electronically stored in-

148. FED. R. CIV. P. 37(e) ("Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system.").
149. Tantivy Commc'ns, Inc. v. Lucent Techs. Inc., No. Civ.A.2:04CV79 (TJW), 2005 WL 2860976, at *3–4 (E.D. Tex. Nov. 1, 2005).
150. *See, e.g.*, 18 U.S.C. § 1512(c)(1) (Supp. 2005).
151. *See, e.g.*, *id.*
152. FED. R. CIV. P. 34(a)(1)(A) (emphasis added).
153. FED. R. CIV. P. 34(b)(1)(C).
154. FED. R. CIV. P. 34(b)(2)(E)(ii).
155. FED. R. CIV. P. 26(f)(3)(C).

formation" in its scheduling order,[156] oversights are likely and controversies are inevitable. Unfortunately, the advisory committee comments do not specifically address the issue of whether producing electronically stored information in the form in which is it ordinarily maintained also requires the production of the metadata associated with such information. However, the comments do state that a party may not "convert electronically stored information from the form in which it is ordinarily maintained to a different form that makes it more difficult or burdensome for the requesting party to use the information efficiently in the litigation."[157]

In an effort to fill in the gaps regarding electronic discovery that were not addressed by the 2006 amendments to the Federal Rules of Civil Procedure, the Sedona Conference has developed a number of guiding principles aimed at balancing the burdens of electronic discovery. The Sedona Conference is a group of "leading jurists, lawyers, experts, academics and others," whose mission is "to come together—in conferences and mini-think tanks (Working Groups)—and engage in true dialogue, not debate, all in an effort to move the law forward in a reasoned and just way."[158] In its first edition of the *Best Practices Recommendations & Principles for Addressing Electronic Document Production*, released in 2005, the Sedona Conference stated, "Unless it is material to resolving the resolution of a dispute, there is no obligation to preserve and produce metadata absent agreement of the parties or order of the court."[159] Because it believed that "most . . . metadata has no evidentiary value, and any time (and money) spent reviewing it is a waste of resources," the Conference found that "the producing party should have the option of producing all, some or none of the metadata."[160] However, in its second edition of the *Best Practices Recommendations & Principles for Addressing Electronic Document Production*, released in 2007, the Conference significantly tempered its stance regarding metadata production.[161] The steering committee significantly

156. FED. R. CIV. P. 16(b)(3)(B)(iii).

157. FED. R. CIV. P. 34(b) advisory committee's note on 2006 amendments.

158. The Sedona Conference, TSC Mission, http://www.thesedonaconference.org/content/tsc_mission/show_page_html (last visited Feb. 15, 2009). The Sedona Conference's official website states:

> Our hallmark is our unique use of the dialogue process to reach levels of understanding and insight not otherwise achievable. Our Working Group Series is designed to focus the dialogue on forward-looking principles, best practices and guidelines in specific areas of the law that may have a dearth of guidance or are otherwise at a "tipping point." The goal is that our Working Groups, the open Working Group Membership Program, and our peer review process, will produce output that is balanced, authoritative, and of immediate benefit to the Bench, Bar and general public.

159. THE SEDONA CONFERENCE WORKING GROUP ON BEST PRACTICES FOR ELECTRONIC DOCUMENT RETENTION & PRODUCTION, THE SEDONA PRINCIPLES: BEST PRACTICES RECOMMENDATIONS & PRINCIPLES FOR ADDRESSING ELECTRONIC DOCUMENT PRODUCTION 46 (2005), *available at* http://www.thesedonaconference.org/content/miscFiles/7_05TSP.pdf.

160. *Id.* at 46–47.

161. *See* THE SEDONA CONFERENCE WORKING GROUP ON BEST PRACTICES FOR ELECTRONIC

revised Principle 12 (governing metadata) "to both reflect the emphasis on 'form or forms' of production in the 2006 Amendments [to Rule 34] and to provide a more neutral view of the need for metadata."[162] The current version of Principle 12 states:

> Absent party agreement or court order specifying the form or forms of production, production should be made in the form or forms in which the information is ordinarily maintained or in a reasonably usable form, taking into account the need to produce reasonably accessible metadata that will enable the receiving party to have the same ability to access, search, and display the information as the producing party where appropriate or necessary in light of the nature of the information and the needs of the case.[163]

Thus, the second edition of Principle 12 suggests that the Conference is urging that a presumption of production of metadata should exist under the 2006 Amendments to the Federal Rules of Civil Procedure.

Ultimately, determining whether such a presumption does in fact exist is difficult. Relatively few courts have addressed whether a discovery request for electronically stored information that is silent on the issue of metadata requires the production of associated metadata.[164] In *Williams v. Sprint/United Management Co.*,[165] the first case to provide a detailed analysis of the discoverability of metadata, the court issued a show cause order as to why the defendant should not be sanctioned for removing metadata from certain relevant Excel spreadsheets before producing them.[166] This was in violation of what the judge stated was "what at least I understood my Order to be, which was that electronic data be produced in the manner in which it was maintained, and to me that did not allow for the scrubbing of metadata because when I talk about electronic data, that includes the metadata."[167] Relying heavily on the first edition of the Sedona Principles,

---

DOCUMENT RETENTION & PRODUCTION, THE SEDONA PRINCIPLES (SECOND EDITION): BEST PRACTICES RECOMMENDATIONS & PRINCIPLES FOR ADDRESSING ELECTRONIC DOCUMENT PRODUCTION 60–61 (2007), *available at* http://www.thesedonaconference.org/content/ miscFiles/TSC_PRINCP_2nd_ed_607.pdf [hereinafter SEDONA PRINCIPLES (SECOND EDITION)].

162. THOMAS Y. ALLMAN, THE SEDONA PRINCIPLES AFTER THE FEDERAL AMENDMENTS: THE SECOND EDITION (2007) 7–8 (2007), *available at* http://www.thesedonaconference.org/content/ miscFiles/2007SummaryofSedonaPrinciples2ndEditionAug17assentforWG1.pdf.

163. SEDONA PRINCIPLES (SECOND EDITION), *supra* note 161, at 60.

164. *See* Lucia Cucu, Note, *The Requirement for Metadata Production Under* Williams v. Sprint/United Management Co.*: An Unnecessary Burden for Litigants Engaged in Electronic Discovery*, 93 CORNELL L. REV. 221, 225 (2007) ("A Westlaw search in the 'all federal cases' database for the word 'metadata' from January 2000 to September 2005 . . . yields only eighteen results, almost all of which are not related to electronic discovery.").

165. 230 F.R.D. 640 (D. Kan. 2005).

166. *Id.* at 644.

167. *Id.*

the court noted that "emerging standards of electronic discovery appear to articulate a general presumption against the production of metadata, but provide a clear caveat when the producing party is aware or should be reasonably aware that particular metadata is relevant to the dispute."[168] However, the court also stated:

> Based on these emerging standards, the Court holds that when a party is ordered to produce electronic documents as they are maintained in the ordinary course of business, the producing party should produce the electronic documents with their metadata intact, unless that party timely objects to production of metadata, the parties agree that the metadata should not be produced, or the producing party requests a protective order.[169]

A few courts have cited *Williams* while concluding that emerging standards establish a presumption against metadata production,[170] but have neglected to give credence to the court's subsequent statement that documents should be produced with metadata intact.[171] Considering the fact that the language in *Williams* to which courts have cited is based on the first Sedona Conference guidelines, it is difficult to know whether there is indeed an emerging presumption against producing metadata. Further, due to the interlocutory nature of discovery orders, there has been little appellate guidance on the subject.

The production of documents with metadata intact poses interesting cost-shifting issues as well. The actual *production* of documents with metadata intact likely imposes little if any additional cost on the responding party. Rather, the responding party would simply produce the responsive items as they would normally, without scrubbing the metadata. The requesting party would then be responsible for mining the metadata from the responsive items. Thus, the cost of obtaining the metadata naturally shifts to the requesting party. The cost of mining the metadata is also relatively low.[172] However, considering the vast amount of electronically stored data

168. *Id.* at 652.

169. *Id.* (footnote omitted).

170. *See* Autotech Tech. Ltd. P'ship v. Automationdirect.com, Inc., 248 F.R.D. 556, 560 (N.D. Ill. 2008); D'Onofrio v. SFX Sports Group, Inc., 247 F.R.D. 43, 46–47 (D.D.C. 2008); Wyeth v. Impax Labs., Inc., 248 F.R.D. 169, 171 (D. Del. 2006).

171. *See, e.g.*, Mich. First Credit Union v. Cumis Ins. Soc'y, Inc., Civ. No. 05-74423, 2007 WL 4098213 (E.D. Mich. Nov. 16, 2007); *Wyeth*, 248 F.R.D. 169.

172. *See* Beckham, *supra* note 15, at 4 ("[W]ith some basic tools that are available online, more deeply hidden metadata may be uncovered."); *see also* Zall, *supra* note 11, at 54 ("Additional, detailed information about metadata in MS Word documents is available by downloading from the Internet a metadata viewer. Depending on how a document is created and saved, metadata viewers may reveal intricate details of a particular document. Freeware metadata viewers are designed typically to compile information regarding the last ten authors of a document, where a document was saved on the hard drive or network, who a document was routed to via e-mail, how many prior document versions

that is often requested, and because "metadata can easily be missed in a privilege review,"[173] the hours logged reviewing metadata for privileged or protected information will likely be extremely costly.

The 2006 amendments to Federal Rule of Civil Procedure 26 provide a cost-shifting scheme for electronically stored information that the responding party identifies as "not reasonably accessible."[174] Because metadata is usually reasonably accessible, Rule 26(b)(2)(B) does not appear on the surface to apply cost-shifting to cases where the privilege review of metadata would be extremely costly. However, the 2006 advisory committee comments state that a source may not be reasonably accessible "in light of the burdens and costs required to search for, retrieve, and produce whatever responsive information may be found."[175] In addition, the committee notes that "the producing party's burdens in reviewing the information for relevance and privilege may weigh against permitting the requested discovery."[176] Additionally, Principle 13 of the second edition of the Sedona Conference's *Best Practices Recommendations & Principles for Addressing Electronic Document Production* notes that "the 'total cost of production' includes the estimated costs of reviewing retrieved documents for privilege, confidentiality, and privacy purposes."[177]

Thus, while the actual production of electronically stored documents with metadata intact is not costly, the accompanying privilege review is likely to impose a high cost on clients. The cost of privilege review is likely a factor courts will take into consideration when determining whether the information is not reasonably available due to cost. Attorneys must remember, however, that if they are required to produce the metadata, Rule 26(b)(2)(B) permits the court to split or completely shift the high cost to the requesting party.

CONCLUSION

Metadata poses significant issues of confidentiality for attorneys and of spoliation for clients. While there may be varying approaches to whether the inadvertent disclosure of metadata containing privileged or protected information results in waiver, it is clear that the possibility exists. Additionally, inadvertent disclosure of metadata may also subject an attorney to disciplinary action for violating his or her duty of confidentiality to the

exist, what changes were made to the text, who made the changes, and when the changes were made. Such metadata viewers also reveal hidden text, comments, and other potentially sensitive information.").

173. Cendali et al., *supra* note 86, at 120.

174. FED. R. CIV. P. 26(b)(2)(B).

175. FED. R. CIV. P. 26(b)(2) advisory committee's note on 2006 amendments.

176. *Id.*

177. SEDONA PRINCIPLES (SECOND EDITION), *supra* note 161, at 67.

client. In an attempt to soften the blow of inadvertent disclosure of confidential metadata, some jurisdictions have made mining metadata an ethical violation. Additionally, both the Federal Rules of Civil Procedure and the Federal Rules of Evidence have developed methods by which a disclosing attorney may be able to "clawback" inadvertently produced metadata, making waiver significantly more difficult. However, there is no way to tell whether a document's metadata has been viewed and neither the Federal Rules of Civil Procedure nor the Model Rules of Professional Conduct actually address when waiver has occurred. Thus, the most efficient method to protect oneself is by systematically scrubbing the metadata from every document that the attorney creates and transmits to an adverse party. While there are additional costs involved, the potential costs of inadvertent disclosure significantly outweigh the minimal cost of purchasing scrubbing software.

When advising a client, however, attorneys must be sure to caution their clients to refrain from destroying possibly relevant metadata. Once a reasonable anticipation of litigation arises, clients generally must preserve all data that is or may be relevant to future litigation. This includes metadata. While it is still unclear as to whether there is a presumption that producing documents as they are kept in the ordinary course of business includes metadata, it is clear that metadata is discoverable. In order to guard against the possibility of spoliation of evidence and the accompanying adverse inference instruction, clients must ensure that all metadata remains intact once the reasonable anticipation of litigation arises.

The potential pitfalls of metadata raise significant issues that attorneys must face. Adequately addressing the confidentiality concerns that attorneys face, and competently advising their client of the potential issues metadata raises for them will significantly decrease the professional hazards that metadata poses for attorneys today.

Adam K. Israel[*]

* B.A. 2006, Birmingham-Southern College; J.D. Expected 2009, The University of Alabama School of Law. The author graciously thanks Professor Carol Rice Andrews, Professor of Law at the University of Alabama School of Law, for her invaluable guidance and insight in the writing of this Note. The author would also like to thank Emily D. Israel for her constant support and encouragement during the writing of this Note.