Coping With Metadata: Ten Key Steps

by Steven C. Bennett* and Jeremy Cloud**

Nearly every electronic document contains "metadata," information that typically does not appear in the paper form of the document but that can be retrieved from electronic files. Metadata is often harmless and irrelevant, but in some cases, it can reveal much about the creation, alteration, and transmission of a document. Metadata, moreover, may contain privileged and confidential information. In some instances, electronic documents cannot be reviewed or used efficiently without metadata. Because modern businesses and law firms depend heavily on electronic communication, data management,

The views expressed in this Article are solely those of the Authors and should not be attributed to Jones Day or its clients.

- 3. See id.
- 4. *Id*.

^{*} Partner in the firm of Jones Day, New York, New York. Macalester College (B.A., 1979); New York University (J.D., 1984).

^{**} Associate in the firm of Jones Day, Atlanta, Georgia. Florida State University (B.S., 2005; J.D., 2008).

^{1.} Definitions of *metadata* vary. *See* Autotech Techs. Ltd. P'ship v. AutomationDirect .com, Inc., 248 F.R.D. 556, 557 n.1 (N.D. Ill. 2008) (defining *metadata* as "all of the contextual, processing, and use information" associated with an electronic document). Such information may include "substantive," "system," and "embedded" metadata. Aguilar v. Immigration & Customs Enforcement Div. of the U.S. Dep't of Homeland Sec., 255 F.R.D. 350, 354–55 (S.D.N.Y. 2008); *see* John Wesley Hall, Jr., Professional Responsibility in Criminal Defense Practice § 28:45.50 (3d ed. 2008) (defining *metadata* in part as "descriptive," "structural," and "administrative" information).

^{2.} H. Craig Hall, Jr., *Dealing with Metadata in the Non-Discovery Context*, 21 UTAH B.J. 24, 24 (2008) ("Most metadata is irrelevant to legal transactions or proceedings.").

 $^{5.~}See\, Dennis Kennedy. com\, Blog, http://www.denniskennedy.com/archives/000891.html (Oct. 24, 2005, 08:40\, CST)$ ("Metadata is not inherently bad. It depends on the context we find it and who is viewing or using it.").

and word processing, lawyers must learn to cope with metadata and its legal implications.⁶

This Article outlines some of the most important practical steps lawyers can take to familiarize themselves with metadata, to recognize the potential risks involved, and to implement procedures aimed at minimizing such risks.

I. EDUCATE YOURSELF

Lawyers must act competently and diligently when representing clients. Most lawyers, however, are not computer experts, and even relatively tech-savvy lawyers may not have heard of metadata until recently. Stories abound of embarrassing revelations that have occurred because of metadata. Lawyers should not fall into the "it can't happen to me" trap. It can, quite easily.

^{6.} See generally Steven C. Bennett & Thomas M. Niccum, Two Views from the Data Mountain, 36 CREIGHTON L. REV. 607 (2003) (summarizing trend toward increasing volume of information and its legal consequences).

^{7.} American Bar Association (ABA) Model Rule of Professional Conduct 1.1 provides, "A lawyer shall provide competent representation to a client." MODEL RULES OF PROF'L CONDUCT R. 1.1 (2009). Model Rule 1.3 provides, "A lawyer shall act with reasonable diligence . . . in representing a client." MODEL RULES OF PROF'L CONDUCT R. 1.3 (2009). The ABA Center for Professional Responsibility website provides access to the text of the Model Rules and Comments, a database of ABA formal ethics opinions, and links to state bar and other resources on ethics issues. See American Bar Association, Center for Professional Responsibility, http://www.abanet.org/cpr/home.html (last visited Feb. 15, 2010). The ABA Legal Technology Resource Center maintains a listing of many recent ethics opinions on questions surrounding metadata. See American Bar Association, Metadata Ethics Opinions Around the U.S., http://www.abanet.org/tech/ltrc/fyidocs/metadatachart.html (last visited Feb. 15, 2010).

^{8.} See Joseph Howie, No Excuses, Law Tech. News, Mar. 2009, http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202435495495&No_Excuses(noting"wide-spread anecdotal support for the proposition that many lawyers are technologically incompetent"); David Hricik, I Can Tell When You're Telling Lies: Ethics and Embedded Confidential Information, 30 J. Legal Prof. 79, 92 (2006) (suggesting that it will become increasingly difficult for lawyers to claim no knowledge of metadata); Campbell C. Steele, Attorneys Beware: Metadata's Impact on Privilege, Work Product, and the Ethical Rules, 35 U. Mem. L. Rev. 911, 950 (2005) (same).

^{9.} See, e.g., Symposium, Ethics and Professionalism in the Digital Age, 60 MERCER L. REV. 863, 960–63 (2009) (discussing several real and hypothetical problems caused by the accidental disclosure of metadata); Brian Bergstein, Bigger Efforts Made Against Embarrassing "Metadata," USA TODAY, Feb. 3, 2006, available at http://www.usatoday.com/tech/news/internetprivacy/2006-02-03-metadata-woes_x.htm (noting a "long line of organizations bitten by information lurking in electronic files"); Ralph Losey, Metadata Spy Blooper, http://www.floridalawfirm.com/bloopers.html (last visited Jan. 22, 2010) (describing "horror stories" within the legal profession regarding lawyers "accidentally producing documents to opposing counsel that contain embarrassing metadata").

As one useful illustration, take a few documents created outside your firm—the more innocuous the better—and turn on the "track changes" feature or other document property listings, which can show much of the information hidden in such documents. Pay attention to just how much information may be conveyed in the metadata contained in a document, and consider whether you might be embarrassed to send out documents with similar kinds of information available to the recipient.

Now, open one of your own word processing documents; check the properties listed and note what you find. Inquire about the software tools your firm uses or may be considering for use in "scrubbing" metadata from documents. Locate and read your firm's policies regarding transmission of electronic documents. Begin to develop a more cautious approach to electronic information in metadata. This cautious approach should include awareness of the standard activities of secretaries and word-processing staff regarding creation of documents.¹⁰

II. RECOGNIZE POTENTIAL PRIVILEGE PROBLEMS IN DISTRIBUTING METADATA

The American Bar Association (ABA) Model Rule of Professional Conduct 1.6¹¹ prohibits lawyers from "reveal[ing] information relating to the representation of a client," including confidential communications and client secrets. ¹² Rule 1.6 requires that attorneys take affirmative steps to ensure that they do not inadvertently transmit such information to third parties without consent from their clients. ¹³ The precise degree of effort at privilege protection required by Rule 1.6 may vary, depending on the importance of the matter and the instructions of the client. ¹⁴ What should not vary, however, is the lawyer's attention to the issue of

^{10.} See Bradley H. Leiber, Applying Ethics Rules to Rapidly Changing Technology, 21 GEO. J. LEGAL ETHICS 893, 897 (2008) (noting that a lawyer may be unaware that staff members have enabled software features that save metadata).

^{11.} Model Rules of Prof'l Conduct R. 1.6 (2009).

^{12.} Id.

^{13.} *Id.* cmt. 17. Significantly, Rule 1.6 applies "not only to matters communicated in confidence by the client but also to all information relating to the representation, whatever its source." *Id.* cmt. 3. Thus, work product, attorney–client privileged information, and client secrets are all subject to protection obligations for the attorney. *See id.* cmt. 2 ("The client is thereby encouraged to seek legal assistance and to communicate fully and frankly with the lawyer even as to embarrassing or legally damaging subject matter.").

^{14.} Id. cmt. 17.

metadata.¹⁵ Several recent ethics opinions make clear that lawyers transmitting electronic information have a duty to use "reasonable care" to prevent the disclosure of metadata that may contain client confidences and secrets.¹⁶

Metadata may reveal privileged or confidential information in various ways. In transactions, it could compromise a negotiating position by showing client or lawyer comments on a draft proposal or deletions of proposed terms in a standard document.¹⁷ In litigation, metadata could reveal trial strategies and views of counsel regarding the viability of legal claims or the strength of evidence.¹⁸

Various techniques may help restrict the distribution of potentially embarrassing—and perhaps quite damaging—metadata:¹⁹

- The simplest method is to reduce the creation and distribution of electronically stored information. A prudent document management program, aimed at eliminating duplicative, outdated, and unnecessary materials, may help law firms and their clients reduce the possibility of distributing private information.²⁰
- Word processing features may be turned off for certain documents. Thus, for example, a document may be created without the "track changes" feature; and the comments field used creating a document may be deleted when the document is finalized.

^{15.} See Leiber, supra note 10, at 909 ("[A]] states are in agreement that an attorney who sends a document containing metadata must act competently."); see also Jason Krause, Metadata Minefield: Opinions Disagree on Whether It's Ethical to Look at Hidden Electronic Information, A.B.A. J., Apr. 2007, at 32, available at http://abajournal.com/magazine/me tadata_minefield (noting that attorneys may run "afoul" of other rules by disclosing client confidences and secrets)

^{16.} N.Y. State Bar Ass'n Comm. on Prof'l Ethics, Op. 782, at 2 (2004); see also Prof'l Ethics of the Fla. Bar, Op. 06-2, at 3 (2006) ("It is the . . . lawyer's obligation to take reasonable steps to safeguard the confidentiality of all communications sent by electronic means to other lawyers and third parties and to protect from other lawyers and third parties all confidential information, including information contained in metadata").

^{17.} See Thomas J. Watson, Avoiding the Dangers of Metadata, 81 Wis. Law. 21, 21 (2008).

^{18.} See David Hricik & Chase Edward Scott, Metadata: The Ghosts Haunting e-Documents, 13 GA. B.J. 16, 16 (Feb. 2008), available at http://www.gabar.org/public/pdf/gbj/feb08.pdf.

^{19.} See generally id. at 20 (summarizing methods to avoid disclosing confidential information in metadata); Boris Reznikov, To Mine or Not to Mine: Recent Developments in the Legal Ethics Debate Regarding Metadata, 4 SHIDLER J.L. COM. & TECH. 13 (2008), available at http://www.lctjournal.washington.edu/Vol4/a13Reznikov.html (same).

^{20.} See generally Steven C. Bennett, Records Management: The Next Frontier in E-Discovery?, 41 Tex. Tech L. Rev. 519 (2009).

- In sending materials to adversaries, send hard copies, transmit images of the materials via facsimile, or send Portable Document Format (PDF) images of paper copies. These steps will ensure that metadata cannot be transmitted.
- If a document must be sent in electronic form, consider the use of PDF or rich text format (RTF). Note, however, that PDF and RTF image conversion from an electronic file will retain and transmit at least some minimum bits of metadata.²¹
- "Scrubbing" software is available for routine transmissions of information. ²² Such software often can be programmed to restrict transmission of specific fields of information. ²³ Similarly, "tracing" software may help ensure that confidential information is not distributed beyond its intended recipients. ²⁴

None of these steps are foolproof. Most significantly, even the lawyer who is well-attuned to metadata privilege problems may encounter cocounsel or staff who lack such awareness. Thus, it becomes essential to implement a regular system to train lawyers and staff and confirm the use of good document management practices within a lawyer's office. In some instances, even outside of litigation, counsel may wish to enter into "unintended disclosure agreements" with adversaries, which confirm arrangements for return or deletion of confidential information that is unintentionally sent outside the firm. ²⁶

^{21.} See Hricik & Scott, supra at note 18, at 24.

^{22.} See Catherine Sanders Reach, Dir., ABA Legal Tech. Res. Ctr., Dangerous Curves Ahead: The Crossroads of Ethics and Technology, Presentation at the Arkansas Bar Mid-Year Meeting (Jan. 25, 2008), available at http://www.abanet.org/tech/ltrc/presentations/arkbarethicstech.pdf (summarizing "what to look for in metadata removal software").

^{23.} Note, however, that "redaction" of documents in native format is a particularly difficult process and is not always effective. See generally Robert B. Brownstone & Dennis P. Duffy, Metadata and Embedded Data: Concerns for Litigators & Transactional Attorneys, Presentation to the Santa Clara County Bar Association (Sept. 20, 2007), available at http://www.sccba.com/docs/cs_pub103.pdf (mentioning that redactions are sometimes ineffective).

^{24.} Philip J. Favro, *A New Frontier in Electronic Discovery*, 13 B.U. J. Sci. & Tech. L. 1, 12 (2007) (noting that "metadata can . . . function as a security device that companies may employ to protect privileged communications").

^{25.} Daniel J. Siegel, *Mind the Metadata*, 44 TRIAL 62, 63 (2008) (suggesting use of a "policy" and "procedure" that addresses the fact that metadata may be a concern "whenever you send out electronic documents").

^{26.} Hricik & Scott, supra note 18, at 25.

III. BE PREPARED FOR INADVERTENT TRANSMISSION

Even if a lawyer's own state ethics rule interpretations prohibit the receiving lawyer from examining confidential information in metadata, it is entirely possible that the recipient of the information operates under the professional responsibility regime of another state, which may permit such examination.²⁷ Further, the recipient lawyer may not realize, until after examining the document, that it contains privileged information. In that event, the producing lawyer cannot "unring the bell" and take the privileged information out of the receiving lawyer's mind.²⁸

In addition to using techniques to reduce the risks of inadvertent transmission outlined above, ²⁹ lawyers should consider steps to reduce damage from inadvertent transmission of private information when it occurs. Such steps may include:

- Lawyers may use a notice statement in the text of e-mail transmissions, which says that the transmission may contain confidential information and that such information, if sent in error, should not be reviewed. The notice may request that the recipient notify the sender and return or destroy all copies of the information.
- In litigation, parties may enter into a "claw-back" agreement or order, providing that inadvertently disclosed information will be returned or destroyed, and not used.
- When inadvertent disclosure of privileged information occurs, counsel should notify opposing counsel promptly and demand reasonable steps to remedy the disclosure. Such steps may include return or destruction of the information and a promise not to use the information for any purpose.

^{27.} See Norman C. Simon, Coming to Terms with Metadata, N.Y.L.J., Oct. 27, 2008, available on Westlaw at 10/27/2008 NYLJ S2.

^{28.} In some serious cases, metadata—such as comments on negotiating strategy (in a transactions context) or trial strategy (in a litigation context)—could affect the outcome of the representation even if the recipient lawyer complies with a request to discard or return the privileged document.

^{29.} See generally Jim Calloway, Metadata—What Is It and What Are My Ethical Duties?, 79 OKLA. B.J. 2529, 2534 (2008), available at http://www.okbar.org/obj/articles08/110808calloway1.htm ("The best rule is for law firms to develop best practices internally to keep metadata from 'escaping' in the first place.").

IV. RECOGNIZE POTENTIAL ETHICAL PROBLEMS IN RECEIVING METADATA

For the lawyer who receives a document containing arguably private metadata, the ethical practice rules are more complicated. Model Rule of Professional Conduct 8.4(c)³0 provides, "It is professional misconduct for a lawyer to . . . engage in conduct involving dishonesty, fraud, deceit or misrepresentation."³¹ Model Rule of Professional Conduct 4.4(b)³² more specifically provides that a "lawyer who receives a document relating to the representation of the lawyer's client and knows or reasonably should know that the document was inadvertently sent shall promptly notify the sender."³³ Rule 4.4(b) does not suggest a means by which a lawyer "reasonably should know" that a document was inadvertently sent; nor does it state whether the lawyer must do (or refrain from doing) anything with the document after notifying the adversary.³⁴ Instead, the comments to Rule 4.4 state that it is "a matter of professional judgment" whether lawyers may read such documents once they know the documents were inadvertently sent.³⁵

In a 2006 formal opinion, the ABA Committee on Ethics and Professional Responsibility determined that, because Rule 4.4(b) specifies that the only ethical obligation of the receiving lawyer is to notify the sending lawyer that private information might have been inadvertently sent, the Model Rules do not preclude receiving lawyers from reading such

^{30.} Model Rules of Prof'l Conduct R. 8.4(c) (2009).

^{31.} *Id*.

^{32.} Model Rules of Prof'l Conduct R. 4.4(b) (2009).

^{33.} Id.

^{34.} See id. cmt. 2 ("Whether 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.").

^{35.} Id. cmt. 3. Comment 3 states:

Some lawyers may choose to return a document unread . . . when the lawyer learns before receiving the document that it was inadvertently sent to the wrong address. Where a lawyer is not required by applicable law to do so, the decision to voluntarily return such a document is a matter of professional judgment ordinarily reserved to the lawyer.

Id. The Pennsylvania Bar Association Committee on Legal Ethics and Professional Responsibility, in a formal opinion, similarly concluded 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." Pa. Bar Assoc. Comm. on Legal Ethics and Prof1 Responsibility, Formal Op. 2007-500 (2007) (suggesting a "common sense" approach), reprinted in Ethics Digest, PA. LAW., Jan.-Feb. 2008, at 46.

information and exploiting it for any lawful purpose.³⁶ However, a number of contrary state ethics opinions have been issued.³⁷

With an absence of clear controlling authority or a majority rule, a lawyer who receives potentially confidential metadata should proceed with caution. Because a lawyer's reputation for ethical and professional conduct is key to professional success, when in doubt about whether confidential information has been inadvertently produced, and whether the lawyer has an ethical obligation to refrain from exploiting the information, the better practice is to provide notice to opposing counsel and seek a dialogue on how best to handle the situation. In the context of litigation under the newly revised Federal Rules of Civil Procedure, that practice is suggested but not specifically required.³⁸

36. See ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 06-442 (2006) ("Even if transmission of 'metadata' were to be regarded as inadvertent, Rule 4.4(b) is silent as to the ethical propriety of a lawyer's review or use of such information."); see also Ethics Comm. of the Colo. Bar Ass'n, Formal Op. 119 (2008) (finding there is "nothing inherently deceitful" about searching through metadata); D.C. Bar Ass'n, Ethics Op. 341 (2007) (concluding that lawyers are prohibited from reviewing metadata only when they have "actual knowledge that the metadata was inadvertently sent"; but "[i]n all other circumstances, a receiving lawyer is free to review the metadata contained within the electronic files provided by an adversary"); Md. State Bar Ass'n Comm. on Ethics, Ethics Dkt. No. 2007-09 (2007) ("[T]here 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.").

37. See, e.g., Ala. State Bar Office of Gen. Counsel, Formal Op. 2007-02 (2007) (finding that "mining of metadata" is prohibited because it could permit the recipient attorney to "acquire confidential and privileged information in order to obtain an unfair advantage against an opposing party"); State Bar of Ariz. Ethics Comm., Ethics Op. 07-03 (2007) (concluding that lawyers should "refrain from conduct that amounts to an unjustified intrusion into the client-lawyer relationship"); Fla. Bar Ethics Dep't, Ethics Op. 06-2 (2006) (finding that a recipient lawyer has an obligation "not to try to obtain from metadata information relating to the representation of the sender's client"); Me. Bd. of Overseers of the Bar Prof'l Ethics Comm'n, Op. 196 (2008) (finding that a lawyer may not "take steps to uncover metadata, embedded in an electronic document sent by counsel for another party, in an effort to detect information that is legally confidential"); N.Y. County Lawyers Ass'n Comm. on Prof'l Ethics, Op. 738 (2008) (concluding that "there is a presumption that disclosure of metadata is inadvertent and would be unethical to view"); N.Y. State Bar Ass'n Comm. on Prof'l Ethics, Op. 749 (2001) (finding that the "use of technology to surreptitiously obtain information that may be protected by the attorney-client privilege, the work product doctrine or that may otherwise constitute a 'secret' of another lawyer's client would violate the letter and spirit of [the New York] Disciplinary Rules").

38. See FED. R. CIV. P. 26(b)(5)(B). Rule 26 provides that a party who produces privileged information may notify the recipient of a claim of privilege; and after being notified, the recipient "must promptly return, sequester, or destroy the specified information and . . . must not use or disclose the information until the claim is resolved." *Id.* Rule 26, however, does not itself impose an obligation on the recipient to notify the producing party of the possibility of an inadvertent production of information. See id.

V. RECOGNIZE THE POTENTIAL VALUE OF METADATA AS EVIDENCE

Much metadata may be entirely innocuous, such as formatting instructions that determine margins, type size, line spacing, and other features in a document. Yet, in some cases, metadata can provide crucial evidence, not available from a paper version of the document.³⁹ For example, metadata could help show who created a document, who edited it, what was changed, who received the document, and when these various events occurred.⁴⁰ Perhaps most significantly, metadata might provide such information even though the face of the document (or a paper copy) would not provide the same information—or might actually suggest different answers. In some instances, metadata might reveal that a document has been backdated or fabricated. Metadata may also provide a means to avoid problems of hearsay in conventional documents.⁴¹

Moreover, in some instances metadata may be an important means to search for and analyze electronic information.⁴² When such information appears in a database, for example, the ability to search the database and extract data of relevance to the lawsuit may affect the outcome of the dispute.⁴³

Despite these potential uses of metadata in litigation, courts also recognize that "[m]ost metadata is of limited evidentiary value, and

^{39.} See Craig Ball, When Out-of-Box Means Out-of-Luck, LAW TECH. NEWS, May 29, 2008, http://www.law.com/jsp/article.jsp?id=1202421750040 ("Don't confuse hardworking system metadata with its troublemaker cousin, application metadata. The latter is that occasionally embarrassing marginalia embedded in documents, holding user comments and tracked changes."); Craig Ball, Make Friends With Metadata, LAW TECH. NEWS, Jan. 26, 2006, http://www.law.com/jsp/PubArticle.jsp?id=900005446137 (noting that metadata can be "the electronic equivalent of DNA, ballistics and fingerprint evidence, with a comparable power to exonerate and incriminate").

^{40.} See, e.g., J. Brian Beckham, Production, Preservation, and Disclosure of Metadata, 7 COLUM. SCI. & TECH. L. REV. 1, 13 (2006) (stating that metadata "may reveal the date a certain fact was known," often "crucial" in tort cases); Ralph C. Losey, Hash: The New Bates Stamp, 12 J. TECH. L. & POL'Y 1, 12 (2007) (noting that metadata provides a type of digital fingerprint, called a "hash value").

^{41.} See United States v. Hamilton, 413 F.3d 1138, 1142 (10th Cir. 2005) (holding that header information in pornographic images was not hearsay because it was not the product of a human "declarant").

^{42.} See Nova Measuring Instruments, Ltd. v. Nanometrics, Inc., 417 F. Supp. 2d 1121, 1122 (N.D. Cal. 2006) (concluding that native file production was necessary).

^{43.} See Lee H. Rosenthal, A Few Thoughts on Electronic Discovery After December 1, 2006, 116 YALE L.J. POCKET PT. 167, 186–87 (2006), http://thepocketpart.org/images/pdfs/82.pdf (noting that metadata may permit effective database review).

reviewing it can waste litigation resources."⁴⁴ And courts "have yet to take a uniform approach" to the production of metadata.⁴⁵ Accordingly, the best practice for parties considering a request for metadata production is to make such a request promptly and to specify the need for such information.⁴⁶

VI. BE SPECIFIC ABOUT METADATA REQUESTS

Requesting counsel should be prepared to explain why metadata production is necessary in a particular case.⁴⁷ "[B]lanket requests" for production of all system metadata will not succeed in most cases.⁴⁸ Nor is there a "routine right of direct access to a party's electronic information system."⁴⁹ Accordingly, the party considering a request for metadata should be specific about what it needs and why it needs such information.

Often, when metadata may be important, the preferred format may be native file production. As noted below, however, native file production may be particularly burdensome. Accordingly, requesting counsel should also consider whether something less than native file production may suffice. The alternatives include the following:

- Production of converted, searchable PDF files;
- Production of tagged image file format (TIFF) files with separate metadata load files;⁵¹ or
 - 44. Wyeth v. Impax Labs., Inc., 248 F.R.D. 169, 171 (D. Del. 2006).
- 45. See Lisa Ann T. Ruggiero & Elissa J. Glasband, Metadata: What Can You Tell Your Clients, N.J.L.J., Aug. 27, 2008, http://www.law.com/jsp/nj/PubArticleNJ.jsp?id=120242 4073607 (noting that courts have not clarified "when and under what circumstances metadata should be produced").
- 46. See generally JAY E. Grenig et al., ediscovery & Digital Evidence § 1:5 (2008) (reviewing cases in which courts have ordered production of metadata).
- 47. See Adam J. Levitt & Scott J. Farrell, *Taming the Metadata Beast*, N.Y.L.J., May 16, 2008, available on Westlaw at 5/16/2008 NYLJ 4 (suggesting that the requesting party must make a "cogent argument" for production of metadata).
- 48. See Nolan M. Goldberg & Scott M. Cohen, Turning Obscure Bits of Data into Hard Evidence, METRO. CORP. COUNSEL, Sept. 2008, at 8, available at http://www.metrocorp.counsel.com/pdf/2008/September/08.pdf.
 - 49. FED. R. CIV. P. 34(a) advisory committee note.
- 50. See Erin E. Wright, Metadata Mining During E-Discovery: The Potential for Finding a Diamond in the Rough, 21 D.C.B.A. BRIEF 26, 29 (Mar. 2009), available at http://www.dcbabrief.org/vol210309art3.html (suggesting that a party seeking discovery should request "native-format metadata in a form that is searchable").
- 51. See Lexbe, e-Discovery Documents Production Formats: Native, TIFF and PDF, http://www.lexbe.com/hp/e-Discovery-production-formats-native-PDF-TIFF.aspx (last visited Jan. 22, 2010) (comparing advantages and disadvantages of various formats).

ullet Native file review by the responding party, coupled with production in TIFF or PDF format. 52

Moreover, when unsure about the value of requesting metadata, counsel might agree upon a sampling system.⁵³ Further, even after production of documents in standard formats, it may become apparent that one or more specific documents are critical in the case. In those circumstances, counsel might request access to metadata for those particular documents, to obtain the "distinctive" information available only through metadata.⁵⁴

VII. RAISE METADATA ISSUES EARLY IN LITIGATION

The recently amended Federal Rules of Civil Procedure generally call for early consultation between parties regarding "any issues about disclosure or discovery of electronically stored information, including the form or forms in which it should be produced."⁵⁵ The new rules address metadata only in the context of pretrial Federal Rule of Civil Procedure 26(f)⁵⁶ conferences, suggesting in the advisory committee note that metadata may be among the topics for such a conference.⁵⁷

At least one recent decision suggests that parties requesting metadata in litigation will have an "uphill battle" when they fail to request such information early in the pretrial process.⁵⁸ Such failure may impose

^{52.} See Kroll, Native File Review: Defining the Future of Document Review (2006), http://www.ontrackinview.com/whitepaper/native2006.pdf (outlining systems for native file review); Mary Mack, Native File Review: Simplifying Electronic Discovery?, JLN'S LEGAL TECH NEWSL., May 2005, available at http://www.fiosinc.com/e-discovery-knowledge-center/electronic-discovery-article.aspx?id=306 (noting advantages and disadvantages of native file review).

^{53.} See Experian Info. Solutions, Inc. v. I-Centrix, L.L.C., No. 04 C 4437, 2005 U.S. Dist. LEXIS 42868, at *6–7 (N.D. Ill. July 21, 2005) (requiring an independent expert to review mirror images of hard drives and report on metadata content).

^{54.} See Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 547-48 (D. Md. 2007).

^{55.} FED. R. CIV. P. 26(f)(3)(C); see Geoff Howard, What Every Lawyer Should Know About the New E-Discovery Rules, CAL. LAW., Jan. 2007, available at http://www.callawyer.com/common/print.cfm?eid=883194&EVID=1 (suggesting that early discussion should include issues surrounding preservation and production of metadata).

^{56.} FED. R. CIV. P. 26(f).

^{57.} See FED. R. CIV. P. 26 advisory committee note ("Whether [metadata] should be produced may be among the topics discussed in the Rule 26(f) conference."). The advisory committee identified the issue of metadata production in discovery but apparently "decided that the best course of action was to remain silent and leave the issue to individual case law development." Thomas Y. Allman, *The Impact of the Proposed Federal E-Discovery Rules*, 12 RICH. J.L. & TECH. 13, ¶ 21 (2006), http://jolt.richmond.edu/v12i4/article13.pdf.

^{58.} Aguilar v. Immigration & Customs Enforcement Div. of the U.S. Dep't of Homeland Sec., 255 F.R.D. 350, 359 (S.D.N.Y. 2008). One commentator suggests that there is a

significant cost on a responding party to recreate a document production that has been substantially completed—a situation that courts may take particular care to avoid.⁵⁹

Under the Federal Rules of Civil Procedure, after the discovery process begins, a party requesting electronic information should specify the form in which requested information is to be produced, 60 and the responding party must state whether it objects to the requested form of production. If there is no agreement between the parties, then the responding party must "produce documents as they are kept in the usual course of business or must organize and label them to correspond to the categories in the request." If the discovery request does not specify a form, the responding party must produce documents "in a form or forms in which [the information] is ordinarily maintained or in a reasonably usable form or forms."

The cases diverge on whether metadata must be produced whenever it is requested. ⁶⁴ In many cases, a resolution of the question whether

- 60. FED. R. CIV. P. 34(b)(1)(C).
- 61. FED. R. CIV. P. 34(b)(2)(D).
- 62. FED. R. CIV. P. 34(b)(2)(E)(i).

[&]quot;pattern" in the cases to the effect that "'when a party requests metadata early on in the e-discovery process, they're usually going to get it.'" Tresa Baldas, *Untangling the DNA of a Document: Metadata Grows in Legal Importance in Cases Throughout the Country*, 35 CONN. LAW TRIB. 5, Feb. 23, 2009, *available at* http://www.ctlawtribune.com/getarticle.aspx?ID=32883 (quoting Wayne Matus).

^{59.} See In re Payment Card Interchange Fee & Merch. Disc. Antitrust Litig., No. MD 05-1720(JG)(JO), 2007 WL 121426, at *4 (E.D.N.Y. Jan. 12, 2007) (holding that, although the requesting party was entitled to a searchable form of electronic documents, the order would apply only prospectively because the other party had already produced a substantial volume of material without objection).

^{63.} FED. R. CIV. P. 34(b)(2)(E)(ii). At least one commentator, noting the disjunctive "or" in Rule 34, suggests that the rule does not necessarily mean that electronic data must always be produced in an electronic format. See W. Lawrence Wescott II, The Increasing Importance of Metadata in Electronic Discovery, 14 RICH. J.L. & TECH. 10, ¶ 11 (2008), http://jolt.richmond.edu/v14i3/article10.pdf (citing Scotts Co. v. Liberty Mut. Ins. Co., No. 2:06-CV-899, 2007 WL 1723509, at *4 (S.D. Ohio June 12, 2007) (rejecting the assertion that hard copy production of electronic information does not satisfy discovery obligations "as a matter of law")).

^{64.} Compare In re Seroquel Prods. Liab. Litig., No. 6:06-md-1769-Orl-22DAB, 2008 WL 1995058, at *8–9 (M.D. Fla. May 7, 2008) (ordering production of specific metadata fields), and Williams v. Sprint/United Mgmt. Co., 230 F.R.D. 640, 656 (D. Kan. 2005) (requiring production of metadata for purposes of discovery regarding database) with Autotech Techs. Ltd. v. AutomationDirect.com, Inc., 248 F.R.D. 556, 559 (N.D. Ill. 2008) (finding insufficient justification for metadata production), and Ky. Speedway, LLC v. NASCAR, Inc., No. 05-138-WOB, 2006 U.S. Dist. LEXIS 92028, at *22–23 (E.D. Ky. Dec. 18, 2006) (suggesting a presumption against production of metadata). One recent commentary suggests an "emerging standard [that] requires metadata production when requested and not objected

metadata must be produced requires development of facts (and even expert opinion), all at the expense of efficiency in the litigation process. As a result, both sides in a litigation should have an incentive to discuss metadata early. The requesting party may be more likely to obtain an agreement or court order when it raises the issue at the outset of the proceedings. And the responding party may avoid the risk and uncertainty regarding its obligations to produce metadata by promptly negotiating a solution with the requesting party that most appropriately balances the burdens and benefits of metadata. Courts prefer such agreements, whenever possible, in lieu of distracting disputes concerning forms and methods for production of electronically stored information.

to, but at the same time emphasizes the need for early, clear requests, and prompt objections if the metadata is not provided." RALPH C. LOSEY, E-DISCOVERY: CURRENT TRENDS AND CASES 166 (2008).

65. The factual issues may include the degree of burden associated with producing metadata. See In re Verisign, Inc. Sec. Litig., No. C 02-02270 JW, 2004 WL 2445243, at *3 (N.D. Cal. Mar. 10, 2004) (degree of burden presented question of fact). Weighed against such a burden, the court may consider the relevance and weight of metadata. Ky. Speedway, 2006 U.S. Dist. LEXIS 92028, at *23 (declining to order production of metadata because requesting party failed to "identify any specific document or documents for which such [metadata] information would be relevant and is not obtainable through other means"). If the requesting party insists that metadata is required to aid in searching the documents produced, the court would have to consider whether production without metadata "significantly degrades" a searchability function that is otherwise available. See FED. R. CIV. P. 34 advisory committee note ("If the responding party ordinarily maintains the information it is producing in a way that makes it searchable by electronic means, the information should not be produced in a form that removes or significantly degrades this feature.").

66. Judye Carter Reynolds, *Practice Tip: Managing Your Metadata*, JLN's LEGAL TECH. NEWSL., Apr. 2007, http://esqinc.com/Content/Articles/metadata.php (suggesting that counsel should gain a "full understanding" of their client's "infrastructure, technology routines, retention policies, and the cost of searching and reviewing data" to be prepared for initial conference with adversary).

67. One agreement, for example, might be to provide metadata for documents with no potential issues of privilege, or for documents (such as databases) that may be particularly difficult to use without metadata. The circumstances of the individual case, and the creativity of the parties and their lawyers, will dictate the final forms of deals that may be struck on metadata.

68. See generally Covad Commc'ns Co. v. Revonet, Inc., 254 F.R.D. 147, 151 (D.D.C. 2008) ("[C]ourts have reached the limits of their patience with having to resolve electronic discovery controversies that are expensive, time consuming and so easily avoided by the lawyers' conferring with each other"). One recent opinion offered a "wake-up call" to the bar about the need for "cooperation between opposing counsel and transparency in all aspects of preservation and production" of electronically stored information. See William A. Gross Constr. Assocs. v. Am. Mfrs. Mut. Ins. Co., 256 F.R.D. 134, 136 (S.D.N.Y. 2009).

VIII. BE PREPARED TO PRESERVE METADATA

If there is an obligation to produce metadata in some circumstances in litigation, then, *a fortiori*, there may be an obligation to preserve metadata, in some cases, or risk later claims of "spoliation." Recently, the Sedona Conference revised its "best practice" principles for ediscovery to address circumstances in which metadata may be essential to understand and use certain electronic materials. Principle 12 now reads:

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.⁷¹

Comment 12a to this new statement of principles endorses the concept of fairness, stating:

Aside from its potential relation to the facts of the case, metadata may also play a functional role in the usability of electronically stored information. For example, system metadata may allow for the quick and efficient sorting of a multitude of files by virtue of the dates or other information captured in metadata. In addition, application metadata may be critical to allow the functioning of routines within the file, such as cell formulae in spreadsheets.

. . . .

^{69.} Spoliation generally involves "destruction or significant alteration of evidence, or the failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation." West v. Goodyear Tire & Rubber Co., 167 F.3d 776, 779 (2d Cir. 1999) (citing BLACK'S LAW DICTIONARY 1401 (6th ed. 1990)). The precise definition of spoliation varies among jurisdictions.

^{70.} The January 2004 edition of THE SEDONA PRINCIPLES took the position that "[u]nless it is material to resolving the dispute, there is no obligation to preserve and produce metadata absent agreement of the parties or order of the court." THE SEDONA CONFERENCE, THE SEDONA PRINCIPLES: BEST PRACTICES RECOMMENDATIONS & PRINCIPLES FOR ADDRESSING ELECTRONIC DOCUMENT PRODUCTION, at i (2004), available at http://www.thesedonaconference.org/dltForm?did=SedonaPrinciples200401.pdf.

^{71.} THE SEDONA CONFERENCE, THE SEDONA PRINCIPLES: BEST PRACTICES RECOMMENDATIONS & PRINCIPLES FOR ADDRESSING ELECTRONIC DOCUMENT PRODUCTION, at ii (2d ed. 2007), available at http://www.thesedonaconference.org/dltForm?did=TSC_PRINCP_2nd_ed_607.pdf.

The extent to which metadata should be preserved and produced in a particular case will depend on the needs of the case. Parties and counsel should consider: (a) what metadata is ordinarily maintained; (b) the potential relevance of the metadata to the dispute (e.g., is the metadata needed to prove a claim or defense, such as the transmittal of an incriminating statement); and (c) the importance of reasonably accessible metadata to facilitating the parties' review, production, and use of the information. In assessing preservation, it should be noted that the failure to preserve and produce metadata may deprive the producing party of the opportunity later to contest the authenticity of the document if the metadata is material to that determination. Organizations should evaluate the potential benefits of retaining native files and metadata (whether or not it is produced) to ensure that documents are authentic and to preclude the fraudulent creation of evidence.⁷²

Compliance with the potential duty to preserve metadata may require special planning. Metadata is fragile: it can be altered even by simply copying or viewing a file. Most such alterations hold little significance, but counsel must be alert to cases when dates of creation or receipt of documents—or other issues that may require metadata evidence—prominently appear. One solution in such cases may be to "image" hard drives, preserving pristine electronic copies of documents and the metadata they contain. The data produced from such copies may be provided either in native form, in TIFF (with some metadata), or in some other less complete form.

If such solutions are undertaken, the ordinary forms of litigation-hold notices may not suffice. Not only may counsel need to ensure that employees are aware of general preservation duties, but they may also need to take account of the fact that metadata preservation is important in the particular case. Counsel must be alert to the technical capabilities of those responsible for collecting and preserving potential evidence. Information technology or forensic assistance may be necessary to take

^{72.} Id. at 60–61. As the Sedona Conference authors explained, this new statement of principles now takes a more "neutral view of the need for metadata." THOMAS Y. ALLMAN, THE SEDONA PRINCIPLES AFTER THE FEDERAL AMENDMENTS: THE SECOND EDITION, at 8 (2007), http://www.thesedonaconference.org/dltForm?did=2007SummaryofSedonaPrinciples2ndEditionAug17assentforWG1.pdf.

^{73.} Mirror imaging of hard drives (for preservation purposes only) may avoid some of the burdens that can arise when a party requests direct access to the computer systems of an adversary. See Calyon v. Mizuho Sec. USA Inc., No. 07 Civ 02241 RODF, 2007 WL 1468889, at *1 , *6 (S.D.N.Y. May 18, 2007) (declining to permit direct access).

^{74.} See In re Genetically Modified Rice Litig., No. 4:06 MD 1811CDP, 2007 WL 1655757, at *5 (E.D. Mo. June 5, 2007) (ordering production of documents as TIFF images, plus separate load files containing metadata).

technical steps to preserve metadata that are beyond the normal experiences of workers.⁷⁵

Metadata, moreover, may reveal privileged or confidential information. The process of retrieving and reviewing metadata in documents to identify and redact privileged and confidential information may be quite burdensome. ⁷⁶

Because of the potential burdens in preserving metadata, early engagement with an adversary in litigation to discuss metadata may be particularly important. In this regard, the receipt of a litigation-hold letter may be a blessing in disguise. Upon such receipt, counsel or the client may wish to take up questions of special burdens in document preservation. One potential challenge to the adversary, if well founded, is to insist that metadata is not important in the particular case and to request that the adversary pay the cost of preserving metadata if it truly wishes to retain all such information.⁷⁷

If all else fails, counsel must be prepared to argue that any losses of metadata were the result of "routine, good-faith" operation of computer systems. When a client has put a litigation hold in place and has taken reasonable steps to identify and preserve particularly relevant metadata, counsel may argue that the inadvertent loss of metadata is not subject to sanction (at least under the Federal Rules of Civil Procedure). The key under these rules may be the "good faith" of the party. The key under these rules may be the "good faith" of the party.

IX. BE PREPARED TO OBJECT TO PRODUCTION OF METADATA

A party resisting the discovery of metadata or the production of files in native form with metadata intact must be prepared to make specific,

^{75.} See Paul Shread, Metadata Ruling Impacts E-Discovery, ENTERPRISE IT PLANET, Jan. 14, 2009, http://www.enterpriseitplanet.com/storage/news/article.php/3796236 (suggesting that the recent decision in Aguilar v. Immigration & Customs Enforcement Div. of the U.S. Dep't of Homeland Sec., 255 F.R.D. 350 (S.D.N.Y. 2008), "could mean more business for e-discovery vendors").

^{76.} See CP Solutions PTE, Ltd. v. Gen. Elec. Co., No. 3:04 cv 2150 (JBA)(WIG), 2006 WL 1272615, at *4 (D. Conn. Feb. 6, 2006) (declining to order production of metadata due to large volume of information at issue when redaction of metadata for privilege would be burdensome).

^{77.} See Steven C. Bennett, Practical Responses to Pre-Litigation Preservation Letters, 8-4 Digital Discovery & E-Evidence Rep. (BNA) 81, 82–83 (Apr. 1, 2008).

^{78.} See FED. R. CIV. P. 37(e) (containing a "safe harbor" exception to sanctions). The advisory committee's note to Rule 37 suggests that "[t]he 'routine operation' of computer systems includes the alteration and overwriting of information, often without the operator's specific direction or awareness." *Id.* advisory committee notes.

^{79.} FED. R. CIV. P. 37(e).

reasonable objections to such discovery.⁸⁰ Blanket objections to metadata production may not suffice, at least when the requesting party can show some specific need for metadata.⁸¹

Specific objections to metadata production may take many forms. Potential objections to metadata production include:

- Native file production may alter or destroy metadata;
- Metadata production may be useless and a waste of time to review;
- Native files with metadata may be difficult to Bates stamp or identify (other than through the use of "hash" values);⁸²
- Redaction of privileged and confidential documents may be difficult in native form;
 - · Not all metadata formats are searchable; and
- $\bullet\,$ Native file documents may be more easily altered or manipulated by users. 83

In the context of metadata production, concerns about privilege review costs and the dangers of inadvertent production of privileged information may be particularly heightened. "The possibility of inadvertent disclosures of privileged information has always been part of the

80. Production of information in "native" form—with metadata intact—may present particular problems of burden and risk. See Robert B. Wiggins, From Boxes of Documents to Gigabytes and Meta Data, METRO. CORP. COUNSEL, Jan. 2004, at 21, available at http://www.metrocorpcounsel.com/pdf/2004/January/21.pdf (noting lack of "standardized" formats for search, review, and production in native form, and risk of alteration of data); Kroll Ontrack, Talking Technology: Objecting to Native File Production Requests (Oct. 2006), http://www.krollontrack.com/newsletters/clu_1006.html#2 ("[C]ounsel should not agree to a native production without being informed about the implications it will have on the effort, including the time and the expense [of discovery].").

81. See generally Craig Ball, Beyond Data About Data: The Litigator's Guide to Metadata 6 (2005), http://www.craigball.com/metadata.pdf (suggesting a "continuum of reasonableness" regarding requests for metadata, such that relevance is a "crucial factor" in determining whether production is required) (emphasis omitted).

82. See e-Discovery Team Blog, Objections to Requests for Native Format Production, http://ralphlosey.wordpress.com/2007/05/21/objections-to-requests-for-native-format-production/ (May 21, 2007, 14:28 EST) (summarizing potential objections and responses).

83. See Mich. First Credit Union v. Cumis Ins. Soc'y, Inc., No. 05-74423, 2007 WL 4098213, at *3 (E.D. Mich. Nov. 16, 2007) (rejecting production of metadata that "would consume substantial resources" and be of limited value); Bolton v. Sprint/United Mgmt. Co., No. 05-2361-JWL, 2007 WL 756644, at *10-11 (D. Kan. Mar. 8, 2007) (denying in part a motion to compel production of metadata, noting burdens). See generally Linda Kish, Production, Metadata and Privilege Trends, 2006-4 DATABASED ADVISOR 25, available at http://my.advisor.com/doc/18137 (summarizing potential objections to metadata production).

discovery process."⁸⁴ But production of metadata in e-discovery increases that risk in at least two ways: (1) the volume and complexity of materials may make a "record-by-record" review burdensome, ⁸⁵ and (2) privilege review may become more difficult and complicated with metadata because some or all of the privileged information may be hidden from plain view by counsel. In some instances, such problems may be at least partially mitigated if counsel enter into some form of confidentiality agreement or order to preserve claims of privilege in the event of inadvertent production. ⁸⁶

A court must balance burden concerns, including issues regarding privilege protection, against the relevance of metadata in the particular case. The following are some factors that may determine whether metadata must be produced in litigation:

- Whether the metadata is "highly relevant to the matters at issue in the lawsuit";
- Whether production of metadata may "assist in authenticating documents":
- Whether "metadata may make it easier for the parties to search, retrieve and use" information;
- Whether production can "avoid any additional costs associated with the removal of metadata"; and
- Whether such data may be useful in showing "who received the document and when, who authored or altered it, and from where it was sent."87

The party resisting production of metadata should be prepared to comment on these kinds of issues. Ultimately, some form of expert

^{84.} David G. Keyko, *Unique Ethical Dilemmas Facing Corporate Counsel*, in E-DISCOVERY FOR CORPORATE COUNSEL § 26:9 (Carole Basri & Mary Mack eds., 2008) (noting that when large quantities of electronic information must be reviewed, the risk of "mistaken disclosure is great").

^{85.} Hopson v. Mayor & City Council of Baltimore, 232 F.R.D. 228, 244 (D. Md. 2005) (finding that the burden of review may "bear no proportionality to what is at stake in the litigation").

^{86.} Rule 502 of the Federal Rules of Evidence, enacted in 2008, endorses such agreements and orders. See FED. R. EVID. 502(d)—(e). See generally Stacy O'Neil Jackson, FRE 502 - Attorney—Client Privilege and Work Product; Limitations on Waiver (Oct. 15, 2008), http://www.iediscovery.com/files/articles/FRE_502_Article.pdf (suggesting that new rule may "standardize" procedures regarding protection against waiver of privilege claims).

^{87. 3} BUSINESS AND COMMERCIAL LITIGATION IN FEDERAL COURTS \S 22:22 (Robert L. Haig ed., 2d ed. 2005 & Supp. 2007).

analysis of the burdens and benefits of metadata production may be required.⁸⁸

X. MONITOR DEVELOPMENTS

Law and best practices regarding metadata are changing rapidly, even as the technologies that produce metadata and permit search and production of such information also change. As we have seen, ethical rules regarding metadata vary between jurisdictions. And additional ethics opinions almost certainly will issue in this area. In the litigation context, absent the unlikely event of a new set of civil procedure rules specific to metadata, trends in the law regarding metadata will evolve on a case-by-case basis.

In this environment, the only sure prescription for a practitioner is to monitor legal and technical developments closely. The stakes are high, and the uncertainties great. Well-informed and savvy practitioners, armed with the latest information on metadata law and technology, can provide their clients with the most effective advice and representation, and can protect themselves from charges of unprofessional conduct.

88. See Elliot Paul Anderson, What Lies Beneath: Native Format Production and Discovery of Metadata in Federal Court, 78 OKLA. B.J. 999, 1002–03 (2007), available at http://www.okbar.org/obj/articles07/041407anderson.htm (concluding that metadata production "depends heavily on the facts of the case: the severity of the requesting party's need, the strength of the producing party's interest, and the availability of reasonable alternatives"). In many instances, it may be possible to demonstrate that metadata production does not produce "bang for the buck." See generally JAMES M. WRIGHT, ESTIMATING THE COST BURDEN OF E-DISCOVERY 11 (2008), http://pdfserver.amlaw.com/legaltechnology/EDiscBurdenEst.WhitePaper.pdf (noting "potential for staggeringly increased costs unless means to limit the [electronically stored information] in discovery are employed").

^{89.} See Marcia Coyle, Metadata Mining Vexes Lawyers, Bars: Invisible Document Data a Big Problem, NAT'L L.J., Feb. 20, 2008, available on Westlaw at 2/19/2008 NLJ 1 (noting that legal ethics expert expects to see "an explosion of opinions" on the ethics of metadata).

^{90.} See e-Discovery Team Blog, Should You "Go Native"?, http://ralphlosey.wordpress.com/2009/02/17/should-you-go-native/ (Feb. 17, 2009, 18:39 EST) (noting that the volume of cases addressing metadata "suggests that the conflict is escalating" on the issue).

^{91.} See Stephen M. Prignano, Modern Discovery Practice: The Hidden World of Metadata in Electronic Discovery, 3-10 Mealey's Litig. Rep.: Discovery (LexisNexis) 23, 27 (July 2006) (noting that "substantial and costly pitfalls . . . await unwary practitioners in this area").