

# What's the Matter With Metadata?

by Charles F. Luce, Jr.

*I never metadata I didn't like.*

—Will Rodgers<sup>1</sup>

**W**hat's the matter with metadata? Metadata—literally “data about data”—is great! By examining the metadata contained in a contract created using Microsoft® Word (MS Word), you can learn who originally created the document, the names of the last ten editors, and the names of the computer and network drives the document has been stored on. You also can view all changes made to the document, read comments the author *thought* had been deleted, tell how many revisions have been made and how long it took to make them, and much more.<sup>2</sup> Incidentally, so can your client, opposing counsel, and even the most amateur computer forensics expert. What's not to like?

The “metadata mess,” as some writers with a penchant for alliteration refer to the unintentional transmission of documents containing metadata, is hardly new. Metadata has been a known feature of MS Word, and to lesser degrees other computer programs, since the late 1990s, when our clients' choice of computer software forced the mass migration of attorneys from WordPerfect to Word. This author has been lecturing and writing about metadata ethics and solutions for more than six years.

Far from flying below the high-tech radar, the debate over metadata has been public and, at times, downright heated. For example, at the 2001 Colorado Bar Association (CBA) Institute in Vail, a fist-fight nearly broke out among audience members when I innocently posed this question: “Does an attorney receiving a document from opposing counsel have a duty, in zealously representing a client, to examine the document for metadata, or to avert his or her eyes?”

Software solutions<sup>3</sup> for the “meta migraine” have been around considerably longer than Blackberrys and iPods. Most lawyers have mastered those technologies without much difficulty. So why all the angst over metadata in 2007?

## Metadata: The Short Course

In commissioning this article, my editor gave me these instructions: “Keep it short, simple, understandable, and practical.” Roger, that—KISSUP it is. No geek-speak this week. So, for those of you who don't have time to tuck your kids in at night, much less to plow through an entire article whose title sounds <yawn> like GlaxoSmithKline's answer to Lunesta,<sup>®</sup> fear not. I can tell you everything a lawyer needs to know about metadata in seven words:

### Buy a metadata scrubber and use it.

How's *that* for KISSUP? You'll find a handy sidebar to this article with the names and Web addresses of software manufacturers whose metadata marketing message seems to have fallen on a lot of deaf legal ears (*see* page 117). So select a metadata solution from the sidebar, add buying and installing it to your Crackberry's to-do list, and skip directly to the Lawyers' Announcements to see who's jumped firms in the last thirty days.

For those of you with a bit more time, and the geeks, ethicists, and grammarians hoping I'll unintentionally commit some major blunder or slip something politically incorrect by my editor, read on. You'll see that I can KISSUP with the best of them, and you'll learn a little bit more about why, like chunky shoes, metadata is in vogue again.

## Why You Should Care: Colorado Rule 1.6(a)

Rule 1.6(a) of the Colorado Rules of Professional Conduct (Colorado Rules) provides:

A lawyer shall not reveal *information relating to representation of a client* unless the client consents after consultation, except for disclosures that are impliedly authorized in order to carry out the representation. . . .<sup>4</sup>

The emphasized phrase is worth mulling over, even committing to memory. Rule 1.6 does not speak of “attorney-client privilege,”



### About the Author:

Charles F. Luce, Jr. is a partner with the Denver law firm of Moye/White LLP, and heads its Intellectual Property Practice Group. He has been lecturing and writing about metadata ethics for more than six years—(303) 292-2900, charles.luce@moyewhite.com.

This Department welcomes submissions of articles and article topics of a practical nature that do not advocate a position or promote a product. For more information about the Department guidelines or to submit an article or topic suggestion, please contact one of the following Department editors: Sue Borgos, (720) 334-0231, sborgos@ots-denver.com; Garry Appel, (303) 297-9800, appelg@appellucas.com; or Brock Wood, (303) 824-5392, bwood@cobar.org.

Articles that appear in this Department do not necessarily reflect the official position of *The Colorado Lawyer* or the Colorado Bar Association, and the publication of these articles does not constitute any recommendation or endorsement of the goods or services mentioned herein.

“work-product,” or “client confidences.” The operative phrase is “information relating to the representation of a client.” That means a lawyer may not discuss anything about a client matter, including the client’s very identity, without the client’s express or implied consent. It matters not that the information is a matter of public record,<sup>5</sup> is on the front page of every newspaper in the free world, and is the buzz at every cocktail party in town. The whole world may be abuzz, but if you represent the “buzzee,” Rule 1.6 requires that you smile and be dumb as a doorknob. Stated differently, without client consent, a lawyer may say only that he or she is a lawyer and represents clients. That’s it. *Finito*.

How is Rule 1.6 applicable to metadata? The answer, and ethical devil, lies in the detailed information metadata tracks. While an attorney engaged to negotiate a business deal unquestionably has client authority to communicate with opposing counsel, it is highly unlikely that any client would expressly or impliedly authorize the release of a document’s metadata “into the wild,” especially if such metadata, directly or indirectly, reveals negotiating strategy or provides other “information relating to the representation of a client” useful to the other side.

## Cautionary Tales

Examples of inadvertent digital indiscretions in which metadata was publicly released abound. Two widely publicized cases illustrate the value of keeping one’s metadata to one’s self.

### *British Intelligence Dossier*

Perhaps the most celebrated debacle involving the release of metadata was committed by ex-British Prime Minister Tony Blair’s administration in 2003, at the outset of the Iraq War. In an effort to garner support for military action, 10 Downing Street released a “classified dossier” entitled “Iraq—Its Infrastructure Of Concealment, Deception And Intimidation,” and posted it on the Internet in its native MS Word format. Former U.S. Secretary of State Colin Powell, speaking to the United Nations in support of broad authority to impose sanctions against Iraq, cited as authoritative the British Intelligence dossier.

Working separately, Dr. Glen Rangwala, a lecturer in politics at Cambridge University, and U.S. privacy expert Richard Smith were able to demonstrate that the document was largely plagiarized from publicly available and outdated sources.<sup>6</sup> Using the dossier’s metadata, Smith was able to follow the “e-paper trail” from each reviser at the Communications Information Centre, a unit of the British Government, and trace its path: from John Pratt, who provided the dossier on a floppy disk to Alison Blackshaw, who in turn gave it to Colin Powell for his presentation before the United Nations. As a result of this major metadata muff, the Blair government was exposed as unsavvy and uninformed, both about technology and about Iraq.

### *SCO Group*

A more pertinent cautionary tale for lawyers involves the foibles of counsel for SCO Group (a provider of a proprietary version of the popular, open-source operating system, Linux), who demonstrated a profound lack of techno-savvy by electronically filing the MS Word version of their client’s complaint against DaimlerChrysler and AutoZone, complete with metadata, thus disclosing part of their client’s litigation strategy.

SCO Group gained public notice and worldwide scorn from the open-source community by first threatening, and then suing, businesses using the Linux operating system, claiming that the popular operating system includes proprietary source code owned by SCO. “We are the new RIAA,”<sup>7</sup> Darl McBride, SCO’s Chief Executive Officer, boasted in a news conference. As a result of SCO’s unpopular actions and McBride’s distinctly “un-open-source” attitude, hackers made routine sport of rendering SCO’s website inaccessible, and Linux aficionados scrutinized every move and motive in SCO’s litigation journey.

You might think that legal counsel for a self-avowed high-tech industry leader, especially one constantly under the microscope of an angry and technologically savvy mob, would have thought to cleanse its complaint of metadata before filing it electronically—but you would be wrong. The filing of the original complaint with the metadata intact provided some interesting insight into SCO’s litigation strategy and potential next moves.

Among other things, examination of the SCO complaint’s “track changes” metadata disclosed the following information:<sup>8</sup>

- On February 13, 2004 at 2:27 p.m., one editor inserted the question: “Did BA receive one of the SCO letters sent to Fortune 1500?” This was an apparent reference to a cease and desist demand earlier sent by SCO to Bank of America.
- Five days later, at precisely 11:10 a.m. (assuming the editor’s PC clock was properly adjusted, of course), “Bank of America, a National Banking Association” was removed as a defendant and “DaimlerChrysler Corp.” was inserted.
- Precisely two minutes later, consistent with the dropping of Bank of America as a party, the comment “Are there any special jurisdiction or venue requirements for a NA bank?” was removed.

### *Nacchio Trial*

A third, more recent example of metadata exposure happened closer to home. Defending against charges that he engaged in insider trading, former Qwest Chief Executive Officer Joe Nacchio claimed he had issued instructions to sell stock prior to a downturn in the company’s financial condition. In rebuttal, the prosecution proffered two experts who it said would testify that Nacchio backdated instructions to sell stock based on their examination of Qwest’s metadata. The testimony was excluded for procedural reasons.<sup>9</sup>

## Rules Pique Lawyer Awareness

The moral of such cautionary tales is obvious: There is no good reason for an attorney to release a metadata-loaded document into the wild. Quite the opposite, there are 1.6<sup>10</sup> good reasons not to. Still, the question remains: with so many well-publicized meta-blunders, and software solutions approaching the decade mark, why the histrionics over metadata *now*? Two theories come to mind.

### *New Federal Rules Regarding Electronic Discovery*

First, new Federal Rules of Civil Procedure (Federal Rules) regarding electronic discovery became effective in December 2006.<sup>11</sup> Now, electronic discovery is hardly new. Those of us practicing technology law have been making requests for the production of e-mail messages and the examination of computer hard drives for almost two decades. What *is* new is that the Federal Rules now re-

quire attorneys to discuss how electronic discovery will be conducted as part of a Rule 26(f)<sup>12</sup> conference. The result is that those lawyers who studiously avoided high-tech discovery for the past twenty years no longer can. There it is in the Federal Rules—in black and white and accompanied by a court order and sanctions for noncompliance. One theory is that, because litigators are now forced to consider their client’s metadata, they’re finally beginning to take greater stock of their own metadata and the consequences of failing to cleanse it.

### *ABA Opinion 06-442*

The second event to raise lawyers’ metadata consciousness was the issuance of American Bar Association (ABA) Formal Opinion 06-442 (Aug. 5, 2006). As with ABA Formal Opinion 99-413 (March 10, 1999)—which, more than five years after Internet e-mail hit its commercial stride, held it was not unethical for attorneys to send confidential communications by electronic mail—Opinion 06-442 is not so much significant for its timing or its conclusion as it is for its weight, being the opinion of the authoring body of the ABA’s Model Rules of Professional Conduct (Model Rules).

While its opinion was preceded by several state and local bar ethics opinions on metadata, the ABA’s Standing Committee on Ethics and Professional Responsibility demonstrated a clearer grasp of the technological and ethical issues involved in reaching a better-reasoned result. Addressing head-on the question I posed at the 2001 CBA Institute, the ABA did not hedge, finding no “specific prohibition against a lawyer’s reviewing and using embedded

information in electronic documents.”<sup>13</sup> Eschewing a balancing test, and adopting instead a refreshing and necessary bright-line rule, the ABA placed the duty entirely on the transmitting lawyer to sanitize metadata before hitting “send.”

The ABA Standing Committee declined to pigeonhole the transmission of metadata-laden documents into the same category as misdirected faxes and errantly addressed e-mail, both deemed “inadvertent” acts subject to the requirements of Model Rule 4.4(b).<sup>14</sup> The Committee also refused to characterize the inspection and use of metadata by the receiving attorney as either “dishonest”<sup>15</sup> or “prejudicial to the administration of justice.”<sup>16</sup>

[T]he Committee does not believe that a lawyer, by acting within the circumstances assumed by the instant opinion, would violate either of those paragraphs of Rule 8.4.<sup>17</sup>

Because the Model Rules impose on the sender a duty to cleanse metadata, lawyers who fail to scrub their documents before transmitting them do so now at greatly increased professional peril. Two months following issuance of the ABA’s opinion, the Maryland Bar followed suit, observing that the electronic discovery amendments to the Federal Rules affect the obligations of lawyers, too.<sup>18</sup>

### *Metadata Mining: Duplicity or Diligence?*

The ABA’s position is not without detractors. New York, Florida, and Alabama each have found something sinister and unethical about metadata “mining.”

“I have no doubt that anyone who receives a document and mines it . . . is unethical, unprofessional, and un-everything else,”

Florida Bar Board of Governors member Jake Schickel publicly declared.<sup>19</sup> Farther north, the Committee on Professional Ethics for the New York State Bar Association in 2001 decreed, “[a] lawyer may not make use of computer software applications to surreptitiously ‘get behind’ visible documents. . . .”<sup>20</sup> More recent, and seemingly oblivious to ABA Opinion 06-442, Alabama followed the approach of both Florida Bar Opinion 06-02, and New York State Bar Opinions 749 and 782, requiring an attorney to “exercise reasonable care when transmitting electronic documents to ensure that he or she does not disclose his client’s confidences or secrets,” while simultaneously imposing a duty on “the receiving lawyer . . . to refrain from mining an electronic document.”<sup>21</sup>

The ABA’s approach to metadata management, however, places the duty under Rule 1.6 where it properly belongs: on the transmitting attorney. It reasons that the sender is in the best position to avoid disclosure of information relating to the representation through the simple expedient of cleansing documents of metadata before they are transmitted. Additionally, by not requiring receiving lawyers to ignore potential evidence contained in metadata, the ABA approach avoids creating a conflict, or at least significant tension, between the receiving lawyer and his or her client who, unburdened by the Model Rules, can examine every aspect of a document’s metadata with legal impunity, and has a legitimate expectation of receiving the assistance of hired counsel to do so.

## Colorado’s Position

The CBA Ethics Committee has not yet taken a formal position in the ongoing metadata-ethics debate.<sup>22</sup> Regardless of the position the Ethics Committee ultimately might take, even states imposing a duty on receiving lawyers to not examine metadata have held also that an attorney must “use reasonable care when transmitting documents by e-mail to prevent the disclosure of metadata containing client confidences or secrets.”<sup>23</sup> While these opinions fall short of mandating that attorneys adopt the obvious technological solution, the KISSUP solution remains the best *metacine*: Buy a metadata scrubber and use it.

## Scrubbing Attorney Metadata: No Conflict With Electronic Discovery Rules

Before examining the several ways metadata may be managed, let’s first dispose of a red herring: An attorney’s duty to *not* reveal information relating to the representation of a client does not create any conflict with electronic discovery rules. These rules, having their root in the policy against spoliation of evidence, do not require that metadata be created, much less preserved, especially in an attorney’s own work product, for the benefit of opposing counsel.

The duty to preserve electronic evidence does not even arise until there is a credible threat of litigation. Moreover, even when the duty to preserve electronic data is triggered, it is unlikely a request for production of electronic documents will survive a timely motion for protective order to exclude metadata that embodies attorney-client communications and work product.

## Metadata Quick-Fixes

For cash-strapped counsel, there are a few inexpensive solutions for quarantining metadata. One is to fax documents instead of

e-mailing them. This, however, makes it difficult to collaborate with clients or opposing counsel, and is bound to introduce error and cost as documents must be re-keyed again and again. This approach also may cause your clients to wonder if you are technologically challenged.

A second solution for those owning Adobe Acrobat Author or another PDF utility is to convert documents to PDF format before sending them. This approach is not foolproof, however, as lawyers representing AT&T in a lawsuit against the National Security Agency discovered in 2006. AT&T’s attorneys *thought* they had electronically expurgated sensitive portions of a document that posited innocuous, hypothetical reasons for the existence of a secret room to monitor Internet and telephone traffic, only to later learn that some PDF readers could see right through their digital “whiteout.”<sup>24</sup>

Other solutions, such as turning off “track changes” and “fast save” in MS Word, are mere bandages on gaping abdominal wounds. While these stop-gap steps should be taken, doing so is no substitute for enterprise-wide deployment of a real metadata management tool.

## Metadata Management Tools

Turning to comprehensive metadata software solutions, an October 2006 e-mail survey by the International Legal Technology Association found the top three choices by law firms were Workshare’s Protect, Payne Consulting’s Metadata Assistant, and Esquire Innovations’ iScrub—with a whopping combined 83 percent market share.<sup>25</sup>

Market share isn’t everything, however. Metadata cleaning, although important for lawyers, is not even *model* rocket science. Any metadata product from a reputable vendor will adequately do the job, so it behooves the frugal lawyer to shop around. The sidebar to this article includes the names and addresses of the three leaders in metadata management tools, as well as some less well-known providers.

## Choosing a Vendor

Most solution providers offer a free, limited-time trial download, either through their website or on request. So, surf the vendor sites listed in the sidebar to this article and conduct your own “shoot-out” between vendors. Here are some things to look for and questions to ask when selecting a metadata solution:

- ✓ **Foolproofness.** First and foremost, the object of metadata management is to keep the metadata inside your firm when documents are e-mailed to outsiders. If your chosen solution does not accomplish this fundamental goal in the hands of the least computer-literate user in your firm, it’s no solution. Fortunately, most vendors have this requirement down pat. You simply cannot send an e-mail attachment without a dialog box popping up and asking, “Do you want to clean the metadata?” and “To what level would you like it cleansed?” Enterprise-wide solutions distinguish between documents being sent internally and those being sent outside an organization, and skip the cleaning and pop-up box for documents staying within your firm.
- ✓ **Price.** Providers typically offer a discount for volume license purchases. Esquire, which also makes iCreate (a great MS Word add-on), has been known to offer discounts on iScrub

for its iCreate customers. Be sure to ask about annual “maintenance” fees, too, lest ye be seduced by a lowball initial license fee, only to be thrown a curve ball in the form of a high maintenance fee when it’s time to update the program.

- ✓ **Configurability.** There is a reason they don’t call them *im*personal computers. User interfaces among programs vary widely and appeal to different types of users. Payne’s Metadata Assistant appeals to geeks because it allows a greater level of control over both metadata analysis and cleaning. However, iScrub’s simpler enterprise interface, offering just a few levels of metadata cleaning, from “cooperator” to “adversary,” may better appeal to your IT crew and risk management consultant because, in offering fewer choices, it is less intimidating for the techno-averse and somewhat easier to use.
- ✓ **Ease of installation.** Installing any of the top products on a single client workstation is generally a painless affair. All integrate seamlessly with the programs they clean, including the four horsemen of Microsoft: Word, Outlook, Excel, and PowerPoint. Installation on an enterprise level, however—the route for a networked firm of any size—can cause your IT staff to mutter dark oaths and start updating their résumés, particularly when configuring the programs for use with virtual private networks such as CITRIX.® Ask vendors for local law firm references and talk with IT and office administrators who have experience administering a program before buying.
- ✓ **Ease of software administration.** For networked firms, make sure your enterprise-wide solution can be easily controlled, configured, and updated from a single point by your IT ad-

ministrator. Most of the top solutions offer these features. If they don’t, choose another vendor.

- ✓ **Ease and clarity of metadata analysis.** Most metadata programs will both clean and analyze metadata, but report it in different ways. Even for attorneys licensed in states that prohibit examining metadata, such restrictions do not apply to the examination of electronic documents received through discovery. With the advent of the federal electronic discovery rules, the ease of examining such documents in batches, and the clarity of the reports they generate, is a feature metadata vendors are being forced to give greater attention to.

## KISSUP: The Bottom Line

So is *anything* the matter with metadata? Or is all the *nouveau* attention to metadata much ado about very little—mere vendor hype to sell software?

The answer is that there is nothing wrong with metadata as long as it is managed. Whether you adhere to the view that the onus is on the sender to cleanse metadata, or on the recipient not to examine it, when it comes to *sending* documents, Colorado Rule 1.6(a) unambiguously establishes an ethical imperative for Colorado lawyers: Don’t become the next cautionary tale of metadata malpractice. Buy a metadata scrubber and use it, and you, too, will feel just like Will Rodgers.

## Notes

1. No, this is not a spelling error. Will *Rodgers* is the computer forensic expert hired by opposing counsel; not to be confused with Will Rogers,

## I Never Metadata Scrubber I Didn’t Like

Metadata software prices and features change regularly to meet new competition, rendering any description or comparison of programs of questionable lasting value. Here is a resource guide of the major and minor players in the digital data security horse race.

With a commanding 83 percent market share, the three largest metadata providers have demonstrated staying power.

- **iScrub** (Esquire Innovations, <http://www.esqinc.com>). With a name like “Esquire,” you know these folks are focused on the legal market. iScrub is one of a suite of lawyer-focused products that includes iCreate and iRedline.
- **Metadata Assistant** (Payne Group, <http://www.payneconsulting.com>). Payne Group is another law firm-focused company with a suite of products to make your secretary smile. Founded in 1994, Payne was perhaps the first firm to both appreciate and publicize the risk of transmitting documents without managing the metadata—and the first to offer a solid solution.
- **Workshare Protect** (Workshare, <http://www.workshare.com>). With a current advertised starting price of \$29.95 per seat, it’s no wonder that Workshare has captured large market share. However, a clean, user-friendly interface also has undoubtedly attracted customers to this non-legal-specific information security company’s product.

In terms of market share, the following companies may be harder to find than the “last 10 authors” metadata in an Excel file. For that very reason, you may find that some of them try harder.

- **ezClean** (Kraft Kennedy & Lesser, <http://www.kklsoftware.com>). This product isn’t fancy, but it has an advertised \$20 starting price. Metadata software currently is this company’s sole mission.
- **Metadata Scrubber** (BEC Legal Systems, <http://www.beclegal.com>). Tracing its company roots to the 1940s, BEC is probably best known for its Summation litigation support software. Metadata Scrubber is a relative newcomer to BEC’s software lineup.
- **Out-of-Sight** (Softwise, <http://www.softwise.net>). Softwise is a small new player whose website needs some serious upgrading.
- **Office 2003/XP Add-in: Remove Hidden Data** (Microsoft, <http://www.microsoft.com>). At the low, low price of “free,” one cannot ignore this gratis download from Bill Gates. However, many, including the author, are naturally leery of Microsoft’s ability to clean its own stable.

the celebrated American political humorist, who never met a *man* he didn't like.

2. To learn more about what kind of information metadata reveals, see Luce, Jr., "Legal Ethics on the Internet," 7 *J. of Internet Law* 1 (Oct. 2003). See also Zall, "Ethical Concerns Regarding Metadata in Word Processing Documents," *Boulder County Bar Newsletter* 1 (July 2007).

3. Software solutions, such as Payne Consulting's Metadata Assistant, have been targeting the legal market since 1998.

4. Colo. RPC 1.6(a) (emphasis added). The Colorado Rules of Professional Conduct generally adopt the Model Rules of Professional Conduct (Model Rules) of the American Bar Association (ABA). The Colorado Supreme Court has adopted extensive revisions to the Colorado Rules of Professional Conduct (New Rules), which are effective January 1, 2008; however, the emphasized language is retained in the New Rules. The Supreme Court's Order and the full text of the New Rules, as adopted by the Court, are available: (1) on the Court's website at <http://www.coloradosupremecourt.com/pdfs/Regulation/Colorado%20RPC%202007.pdf>; (2) on the Colorado Bar Association (CBA) website, <http://www.cobar.org>; and (3) in 36 *The Colorado Lawyer* 151 (Aug. 2007).

5. See, e.g., *Lawyer Disciplinary Bd. v. McGravw*, 461 S.E.2d 850 (W.Va. 1995) ("[t]he ethical duty of confidentiality is not nullified by the fact that the information is part of a public record or that someone else is privy to it."); Ariz. Ethics Op. 2000-11 (2000) ("the lawyer is required to maintain the confidentiality of information relating to the representation even if the information is a matter of public record"); *In re Anonymous*, 654 N.E.2d 1128 (Ind. 1995) (Rule 1.6 violated even though information disclosed "was readily available from public sources and not confidential in nature").

6. To read more about 10 Downing Street's metadata mismanagement, see Smith, "Microsoft Word bytes Tony Blair in the Butt" (June 30, 2003), available at <http://www.computerbytesman.com/privacy/blair.htm>; Rangwala, "Writing by Glen Rangwala" (June 16, 2003), available at <http://middleeastreference.org.uk/fac030616.html>; and "UK Accused Of Lifting Dossier Text," *CNN.com* (Feb. 7, 2003), available at <http://www.cnn.com/2003/WORLD/meast/02/07/sprj.irq.uk.dossier/index.html>.

7. A reference to the Recording Industry Association of America, which has attempted to stem the rising tide of illegally downloaded music through an aggressive, high-profile litigation strategy, which includes suing thousands of college students and the institutions they attend for copyright infringement.

8. For a full account of the SCO story, see Shankland and Ard, "Lawyers May Need Microsoft Word Lessons" (March 5, 2004), available at <http://www.silicon.com/software/os/0,39024651,39118916,00.htm>.

9. See Griffen, "Judge Excludes Two Witnesses," *The Denver Post* (March 23, 2007), available at [http://www.denverpost.com/ci\\_5497687](http://www.denverpost.com/ci_5497687).

10. Colo. RPC 1.6(a), that is.

11. See generally Anderson and Barkley, "The Brave New World of E-Discovery," 36 *The Colorado Lawyer* 83 (Aug. 2007).

12. See Fed. R. Civ. P. 26(f).

13. ABA Standing Committee on Ethics and Prof'l Responsibility Formal Op. 06-422 (2006).

14. Model Rule 4.4(b) provides:

[a] lawyer who receives a document relating to the representation of the lawyer's client and knows or reasonably should know that the document was inadvertently sent shall promptly notify the sender.

See also CBA Ethics Op. 108: Inadvertent Disclosure of Privileged or Confidential Documents (May 20, 2000), 29 *The Colorado Lawyer* 55 (Sept. 2000), available at <http://www.cobar.org/group/display.cfm?GenID=1830>.

15. See Model Rule 8.4(c).

16. See Model Rule 8.4(d).

17. ABA Standing Committee on Ethics and Prof'l Responsibility Formal Op. 06-422 (2006).

18. See Md. State Bar Association Committee on Ethics Op. 2007-09 (Oct. 16, 2006).

19. Blakenship, "What's in your document?" *The Florida Bar News* (Jan. 1, 2006), available at <http://www.floridabar.org/DIVCOM/JN/JNNews01.nsf/76d28aa8f2ee03e185256aa9005d8d9a/c3f75b4e10e94f78852570e50051b23e?OpenDocument>. Florida ultimately adopted an opinion that imposes duties on both the sending attorney to scrub the metadata, and the receiving lawyer not to mine it, treating the transmission of metadata as inadvertent disclosure. See Prof'l Ethics of the Bar of Fla. Op. 06-02 (Sept. 15, 2006), available at <http://www.floridabar.org/tfb/tfbetopin.nsf/SearchView/ETHICS,+OPINION+06-2?opendocument>.

20. N.Y. State Bar Op. 749 (Dec. 14, 2001). See also N.Y. State Bar Op. 782 (Dec. 8, 2004), concluding:

[I]awyers have a duty under DR 4-101 to use reasonable care when transmitting documents by e-mail to prevent the disclosure of metadata containing client confidences or secrets.

21. Ala. Ethics Op. 2007-02, Office of the General Counsel (March 14, 2007), available at <http://www.alabar.org/ogc/PDF/2007-02.pdf>. The Ala. opinion contains no mention of the earlier ABA metadata opinion, but does cite as authoritative N.Y. State Bar Ops. 749 and 782, as well as Wikipedia (<http://en.wikipedia.org>).

22. Although the CBA Ethics Committee has not issued a formal opinion on metadata management, its informal "Seamless Web" website has for years advised attorneys to cleanse metadata before it leaves the law office:

When an e-mail communication is directed to opposing counsel, it is important to consider and, if necessary, cleanse such communications, particularly attachments. The programming that supports the "track changes" feature of Microsoft's MS Word® word processing program is made possible by computer code called metadata. Unless properly purged, the Word® document you e-mail to opposing counsel and/or the opposing party (or which your client forwards to the opposing party) may contain not only your latest revisions, but also several generations of changes and comments, which may, directly or indirectly, disclose client communications and or strategy.

The Seamless Web: Lawyering on the Internet, "What precautions should an attorney use when communicating with clients by electronic mail?" available at <http://www.cobar.org/group/display.cfm?GenID=4821>.

23. N.Y. State Bar Op. 782 (Dec. 8, 2004). *Accord* Florida Op. 06-02 (Sept. 15, 2006); Ala. Ethics Op. 2007-02, Office of the General Counsel (March 14, 2007).

24. See McCullagh, "AT&T Leaks Sensitive Info in NSA Suit," *CNet News* (May 30, 2006), available at [http://news.com.com/AT38T+leaks+sensitive+info+in+NSA+suit/2100-1028\\_3-6077353.html](http://news.com.com/AT38T+leaks+sensitive+info+in+NSA+suit/2100-1028_3-6077353.html).

25. International Legal Technology Association, "ITLA's 2006 E-Mail Survey" 9 (Oct. 2006), available at [http://www.iltanet.org/files/tbl\\_s6Publications/PDF33/127/2006%20E-Mail%20Survey.pdf](http://www.iltanet.org/files/tbl_s6Publications/PDF33/127/2006%20E-Mail%20Survey.pdf). ■