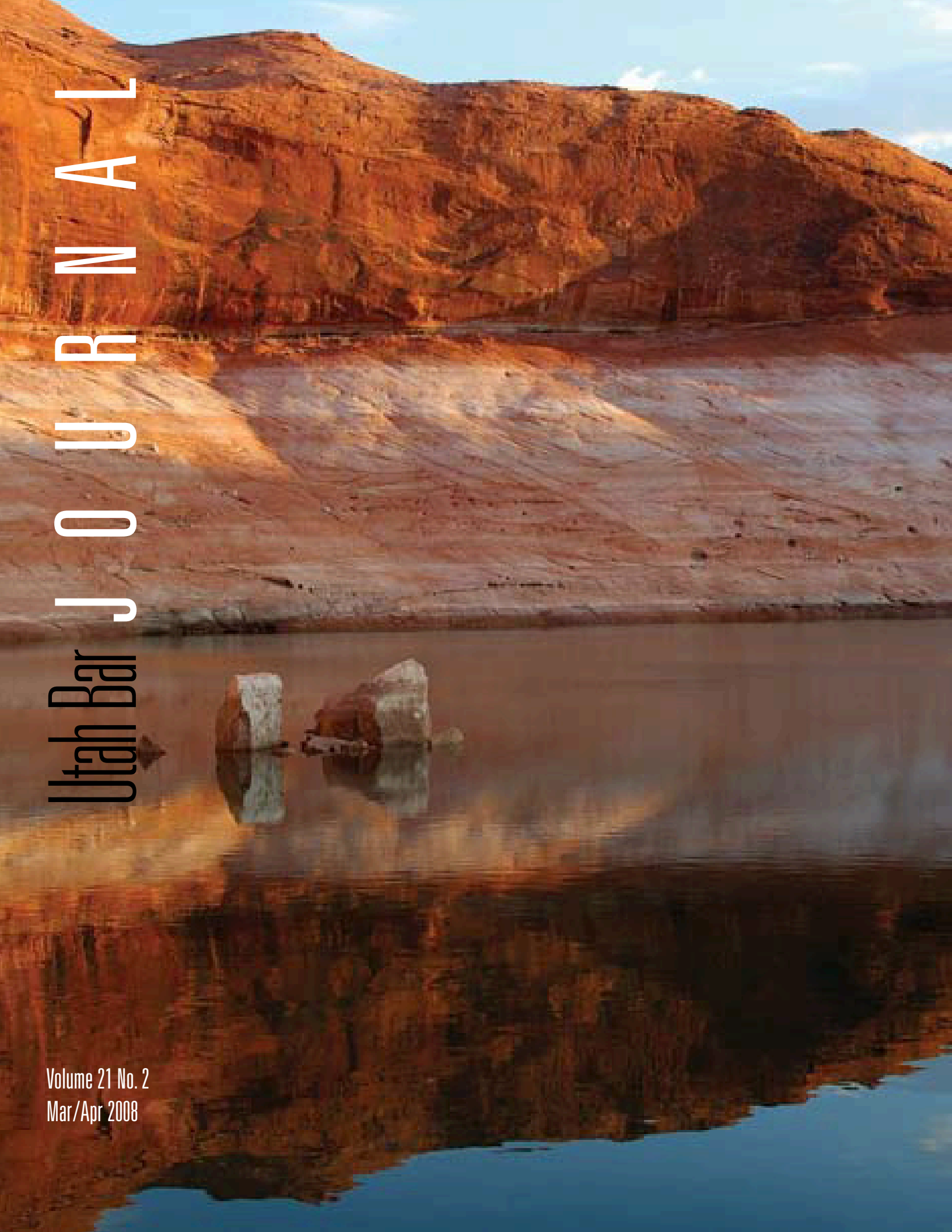

Utah Bar JOURNAL

Volume 21 No. 2
Mar/Apr 2008

Dealing with Metadata in the Non-Discovery Context

by H. Craig Hall, Jr.

I'm not exactly sure how this was done, but rumor has it that lawyers used to practice law without computers.

Word processing software, e-mail, spreadsheets, PowerPoint, and the like have become an almost essential part of the professional and personal lives of lawyers and their clients. Such technology can significantly enhance our communication capabilities and efficiency as lawyers. However, potential dangers abound for lawyers. Perhaps one of the most dangerous issues to be aware of is the existence of metadata in electronic documents.

The federal rules advisory committee has defined "metadata" as "[i]nformation describing the history, tracking, or management of an electronic file."[1] It is sometimes more generally described as "data that provides information about other data" or "data about data."[2] Metadata within electronic documents typically cannot be seen on the face of the document or when the document is printed, and generally is found only if specifically searched. As indicated in one ethics opinion, "[t]o the uninitiated, metadata is hidden and perhaps unknown, but to competent computer-users, the existence of metadata is well known and may be a simple 'click' away."[3]

Information that may be found within metadata includes:

- The time and date a document was last accessed and last saved.
- The identity of the computer that created the document, the date and time of the document's creation, and the identity of all those who revised the document.
- How much time was spent drafting and revising a document.
- How many times the document was revised.
- Where the document is saved on the author's computer.
- Hidden text.
- Redline changes. On the face of the document, as seen on the computer screen, redline changes may be easily viewable or discretely hidden. But even if hidden, the changes (and subsequently, prior versions of documents) can sometimes be easily retrieved and viewed by others.
- Prior versions of documents may also be viewed by others if the author uses the "Versions" feature of Microsoft Word which can automatically save a version of the document each time the document is closed.
- "Comments" by the author (or by others who reviewed the document) may be viewable and/or retrievable.
- Spreadsheets may include cells containing mathematical formulas not seen when printed but easily viewable in electronic form.
- E-mail normally includes the sender's I.P. address, which may reveal the identity of the computer, network, and geographical location from which one is sending the e-mail.[4]

Most metadata is irrelevant to legal transactions or proceedings. However, there may be times where metadata may lead to inadvertent disclosure of confidential information, waiver of a privilege, or breach of an ethical duty.

Take, for example, The SCO Group's slip-up where metadata revealed litigation strategy in a 2004 lawsuit filed against DaimlerChrysler. After the case was filed, a reporter received an electronic version of the Complaint in which the metadata revealed that earlier versions of the Complaint identified Bank of America as the defendant instead of DaimlerChrysler.[5]

Though not in a legal context, another embarrassing example involved, ironically enough, Microsoft, which posted a downloadable copy of its 1999 Annual Report on its website. The Report, which was drafted with Microsoft Word, contained metadata which revealed the document was written, at least in part, on a Macintosh computer.[6]

Metadata should also be of particular concern to attorneys billing by the hour. For efficiency's sake, lawyers often recycle (or at least start from) documents used in prior cases or transactions. Imagine the potential awkwardness when a tech-savvy client confronts his attorney with metadata in an electronic document prepared for the client that reveals the document took 25 minutes to draft (by a paralegal) rather than the two hours the client was billed (at the attorney's billing rate).

In the discovery context, attorneys are now required to produce

H. CRAIG HALL is an Assistant City Attorney at the West Jordan City Attorney's Office where his responsibilities relate primarily to civil litigation. He is also Chair of the Technology Committee of the Young Lawyers' Division of the Utah State Bar.

electronically stored information in its original electronic format if requested. This has been the case in federal courts since December 2006, and is now also required in Utah state courts as of November 2007.[7] This article examines the Rules of Professional Conduct and (sometimes contradictory) ethics opinions from various jurisdictions that discuss the issue of metadata exchanged (deliberately or inadvertently) between adversaries, co-parties, or other third-parties in the non-discovery context. To date, the Utah State Bar has not issued an ethics advisory opinion on this specific issue, and no Utah state or federal court decision has addressed the issue.

The Sending Lawyer

Utah Rule of Professional Conduct 1.6 requires that "[a] lawyer shall not reveal information relating to the representation of a client" unless a specific exception applies or the client gives consent. Comments 16 and 17 to Rule 1.6 caution lawyers to "act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure" and to "take reasonable precautions to prevent the information from coming into the hands of unintended recipients."

In 2004, the New York State Bar Association issued an ethics opinion which concluded that "lawyers have a duty under [New York's Rule 1.6 equivalent] to use reasonable care when transmitting documents by e-mail to prevent the disclosure of metadata containing client confidences or secrets."[8]

> Likewise, a 2006 Florida ethics opinion advised: "It is the sending 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, that may be included in such electronic communications."[9]

It is relatively simple to remove or "scrub" metadata from electronic documents. Perhaps the easiest method is to convert the document into a portable document file (PDF). This conversion essentially turns the electronic document into a photocopy that is viewable and printable by the recipient. The newly created PDF document no longer contains any metadata from the original document.[10] Third-party commercial products are also available for the removal of metadata. Further, Microsoft provides information to prevent metadata from being shared.[11]

Considering the relative ease with which most metadata can be removed, lawyers should take all reasonable steps to remove metadata from all types of electronic documents when communicating with other lawyers, clients, and third-parties. To date, it appears that no court has issued a ruling regarding the consequences

of disclosing confidential client information solely through metadata. However, it certainly would not be a stretch for a court to rule that disclosure of such information (1) is a violation of Rule of Professional Conduct 1.6, and/or (2) operates as a waiver of one or more legal privileges, including the attorney-client privilege.

The Receiving Lawyer

It also appears that no court has ruled on what a lawyer may or may not do when one *receives* an electronic document that contains metadata. At least two rules of professional conduct arguably apply when a lawyer receives an electronic document containing metadata.

On one hand, a lawyer may justify metadata examination under Utah Rule of Professional Conduct 1.3 and its comments, which mandate that the lawyer "shall act with reasonable diligence… in representing a client" and "must act…with zeal in advocacy upon the client's behalf." Indeed, one could argue that "reasonable diligence" and "zeal" would *require* the lawyer to search metadata for any relevant information.

On the other hand, Utah Rule of Professional Conduct 4.4(b) states: "A lawyer who receives a document relating to the representation of the [opposing] lawyer's client and knows or reasonably should know that the document was inadvertently sent shall promptly notify the sender." Comment 2 under Rule 4.4 makes clear that "document" includes e-mail or any other electronic modes of transmission subject to being read or put into readable form.[12] Thus, Rule 4.4 may be used to assert that metadata examination should never occur.

Unfortunately, the ethics opinions from other jurisdictions offer no clear guidance on this issue, as they vary greatly in their conclusions. Remember that these opinions apply only to metadata examination in the non-discovery context.

OPINIONS CONCLUDING THAT METADATA INSPECTION IS NEVER PERMITTED

New York

In 2001, the New York State Bar Association issued an opinion examining the question of whether "a lawyer ethically may use available technology to surreptitiously examine and trace e-mail and other electronic documents."[13] The opinion discussed not only metadata, but also situations where someone deliberately and secretly plants a "bug" in an e-mail sent to another lawyer which enables the user planting the bug to learn the identity of recipients and senders, and to view the comments these persons make regarding the document, as long as they have not "bug proofed" their systems.

It certainly is not surprising that the opinion concludes that such "bugging" technologies are unethical and probably illegal. But the opinion failed to distinguish between this so-called bug-placing behavior and the simple inspection of ordinary metadata when it concluded that "a lawyer may not make use of computer software applications to surreptitiously 'get behind' visible documents [to view metadata] or to trace e-mail."

Alabama

The Alabama State Bar's March 2007 opinion relies heavily on the New York opinion and states: "the use of computer technology [for purposes of metadata examination] constitutes an impermissible intrusion on the attorney-client relationship in violation of the Alabama Rules of Professional Conduct."[14] The Alabama opinion also concludes that metadata examination violates Alabama Rules of Professional Conduct 8.4(c) and (d) which prohibit "dishonesty, fraud, deceit or misrepresentation" and "conduct that is prejudicial to the administration of justice."

OPINIONS CONCLUDING THAT METADATA INSPECTION MAY BE PERMITTED IN SOME SITUATIONS

Florida

The Florida State Bar counseled against metadata examination in its 2006 ethics opinion, which advises: "A lawyer receiving an electronic document should not try to obtain information from metadata that the lawyer knows or should know is not intended for the receiving lawyer. A lawyer who inadvertently receives information via metadata…should notify the sender of the information's receipt."[15]

There is difficulty with practical application of this opinion. Apparently, the receiving lawyer *may* review metadata if one knows the metadata is intended for the receiving lawyer. But how does the receiving lawyer know if the metadata is intended for the lawyer without first viewing it? Of course, the sending attorney could specifically inform the receiving lawyer that such communication is intended. But short of this specific disclosure, receiving lawyers in Florida are effectively prohibited from even attempting to obtain information from metadata.

District of Columbia

In September 2007, the District of Columbia Bar Association advised: "A receiving lawyer is prohibited from reviewing metadata sent by an adversary only where he has actual knowledge that the metadata was inadvertently sent." [16] In all other circumstances, the receiving lawyer is free to examine the metadata.

The opinion cautioned, however, that actual knowledge may exist, not only when a receiving lawyer is told of the inadvertent disclosure before review of the document, but also when a

lawyer immediately notices upon review of the metadata that the information was obviously sent inadvertently. In footnote three to the opinion, the Ethics Committee warned that they "do not condone a situation in which a lawyer employs a system to mine all incoming electronic documents in the hope of uncovering a confidence or secret, the disclosure of which was unintended by some hapless sender."

OPINION CONCLUDING THAT METADATA EXAMINATION IS ALWAYS ALLOWED

American Bar Association

The ABA appears to stand alone in its conclusion that metadata may always be reviewed by the receiving lawyer (assuming the receiving lawyer does not obtain the electronic document in a manner that was criminal, fraudulent, deceitful, or otherwise improper).[17] In support, the opinion states: "Even if transmission of 'metadata' were to be regarded as inadvertent, [Model] Rule 4.4(b) is silent as to the ethical propriety of a lawyer's review or use of such information."

Model Rule 4.4(b), which is identical to Utah Rule of Professional Conduct 4.4(b), advises that when a receiving lawyer inadvertently receives a document, the *only* obligation created by Rule 4.4(b) is to notify the sender that the document was received. The Rule *does not* prohibit the receiving lawyer from reviewing the document. Indeed, Comment three of Rule 4.4 indicates that the receiving lawyer *may*, but is not required to, return the document unread.

Further, the ABA opinion specifically rejected the argument that a lawyer's search for, or use of, metadata violates Model Rule 8.4 (also identical to Utah's Rule 8.4), which prohibits lawyers from engaging in conduct "involving dishonesty, fraud, deceit, or misrepresentation" or conduct "that is prejudicial to the administration of justice."

In short, the ABA concludes that metadata may be reviewed by a receiving lawyer and that such review is not dishonest, fraudulent or deceitful.

Conclusion

It seems fairly apparent that a sending lawyer, in the non-discovery context, must take all reasonable precautions to either: (1) scrub all metadata from an electronic document before it is sent to an adversary, co-counsel, or some other third-party; or (2) be certain what metadata the document contains and that such metadata is intended to be sent to the recipient.

It is less clear what a receiving lawyer should do when one receives an electronic document that contains confidential information within the metadata. To date, there is no published court ruling regarding the issue. Ethics opinions vary widely in their conclusions from: "it is never acceptable to review metadata;" to "it is sometimes acceptable to review metadata;" to "reviewing metadata is always permissible." Further, the Utah State Bar has not yet issued an ethics opinion to give Utah lawyers specific guidance on this issue.

It is the author's opinion that unless Utah amends its Rules of Professional Conduct, the Utah Bar should adopt the ABA Opinion and advise that receiving lawyers may review metadata in electronic documents, even if such metadata is sent inadvertently. Although the Utah Rules regarding document disclosure require a receiving lawyer to "promptly notify" a sender of an inadvertently disclosed document, the Rules allow the receiving lawyer to fully review such a document. Inadvertently disclosed metadata should similarly be fully reviewable by the receiving attorney, especially since it is relatively simple to share electronic documents free of compromising metadata.

1. Fed. R. Civ. P. 26(f), 2006 Advisory Committee Note ¶ 26.
2. http://www.m-w.com/dictionary/metadata (last visited January 29, 2008).
3. D.C. Legal Ethics Comm., Op. No. 341, September 2007.
4. *See* examples of metadata and ways to control it at http://office.microsoft.com/en-us/help/HA011400341033.aspx (last visited January 29, 2008). One federal court opinion which is especially helpful in understanding metadata is *Williams v. Sprint/United Mgmt. Co.,* 230 F.R.D. 640, 646-47 (D. Kan. 2005).
5. *See* Jembaa Cole, *When Invisible Electronic Ink Leaves Red Faces: Tactical, Legal and Ethical Consequences of the Failure to Remove Metadata,* 1 Shidler J. L. Com. & Tech. 8 (Feb. 2, 2005), http://www.lctjournal.washington.edu/Vol1/a008Cole.html.
6. *See id.*
7. *See* Fed. R. Civ. P. 16, 26, 33, 34 and 45 (effective December 1, 2006); Utah R. Civ. P. 16, 26, 33, 34 and 45 (effective November 1, 2007).
8. N.Y. State Bar Ass'n Comm. on Prof'l Ethics, Op. No. 782 (Dec. 8, 2004).
9. Prof'l Ethics of the Florida Bar, Op. No. 06-2 (September 15, 2006).
10. One must be aware that PDF documents contain their own metadata, such as the name of the original file from which the PDF was created, the network and computer identification of the person who created the PDF, and when the PDF was created. *See* http://www.llrx.com/columns/fios6.htm (last visited January 29, 2008).
11. Third-party commercial products include iScrub, Metadata Sweeper, Workshare, and others. Information from Microsoft is available at http://www.microsoft.com/downloads/details.aspx?FamilyId=144E54ED-D43E-42CA-BC7B-5446D34E5360&displaylang=en and http://office.microsoft.com/en-us/help/HA100375931033.aspx (last visited January 29, 2008).
12. Utah Rule of Prof'l Conduct 4.4(b) and Comment 2.
13. N.Y. State Bar Ass'n, Comm. on Prof'l Ethics, Op. No. 749 (December 14, 2001).
14. Ala. State Bar, Office of Gen. Counsel, Op. No. R0-2007-02 (March 14, 2007).
15. Fla. Bar Prof'l Ethics Comm., Advisory Op. No. 06-2 (September 15, 2006).
16. D.C. Legal Ethics Comm., Op. No. 341, September 2007. It should be noted that this Opinion is based, at least in part, on District of Columbia Rule of Professional Conduct 4.4(b), which differs from the Model Rule of Professional Conduct in that the D.C. Rule specifically prohibits examination of inadvertently sent documents. *See* D.C. Rule of Prof'l Conduct 4.4(b), and Comments [2] and [3].
17. American Bar Association, Comm. on Ethics and Prof'l Responsibility, Formal Op. No. 06-442 (August 5, 2006).