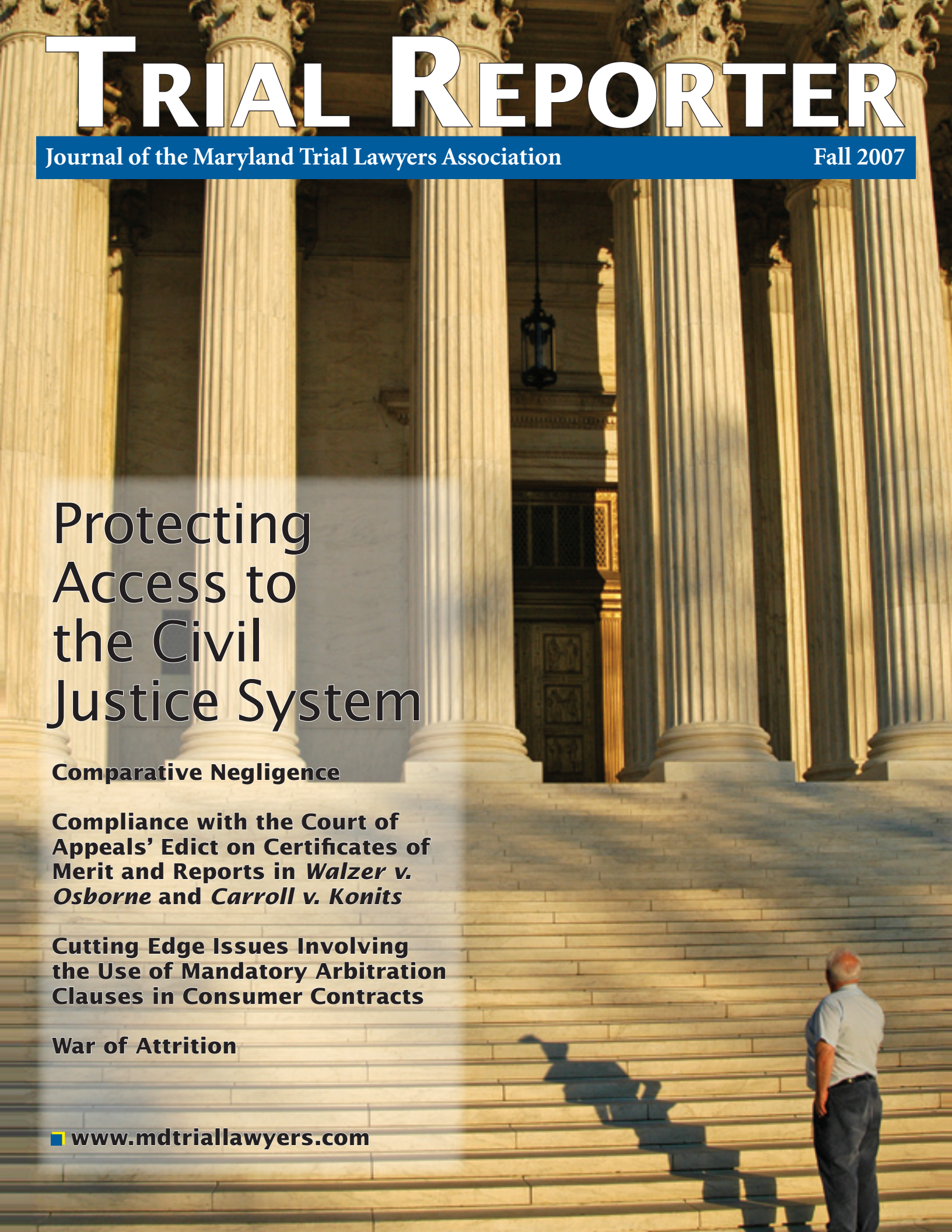
Trial Reporter

Journal of the Maryland Trial Lawyers Association Fall 2007



Protecting Access to the Civil Justice System

Comparative Negligence

Compliance with the Court of Appeals' Edict on Certificates of Merit and Reports in *Walzer v. Osborne* and *Carroll v. Konits*

Cutting Edge Issues Involving the Use of Mandatory Arbitration Clauses in Consumer Contracts

War of Attrition

www.mdtriallawyers.com

by John Cord, Chair MTLA Technology Committee

Metadata: Pitfalls and Prevention

The continuous march of technology and its invasion into the everyday practice of law can certainly cause anxiety in lawyers who have to consider their ethical duties when adapting any technology. Rather than adopting the view of the Luddites[1]; however, attorneys should embrace the advances of technology and learn enough about it to comport with their ethical requirements. One frequent topic of consternation is the advent of metadata and its impact in the legal arena.

What is Metadata?

Metadata is behind-the-scenes information stored in electronic documents.[2] It includes typically benign information, including the author, date of document creation, and date the document was last modified. However, it can also include the document revisions, prior versions, and a history of comments associated with the document.

Practically, this is important when sending documents that have at any time included sensitive information. For example, an attorney who sends a proposed settlement demand letter to his partner in Microsoft Word with a comment about the client's bottom-line, which is later replaced by the actual demand figure and forwarded to defense counsel, runs the risk that the bottom-line number is discoverable, even though it is not apparent on the face of the document. This risk is highest when utilizing the 'Track Changes' feature of Microsoft Word;[3] however, other features of this and other word processing applications, such as comments, hidden text, and old file versions can all lead to inadvertent data disclosure. Additionally, PDF documents converted from Word or WordPerfect may contain similar metadata in the form of comments, or even the underlying word processing file.

Ethics of Sending and Viewing Metadata

Most law firms send a substantial percentage of their documents out by e-mail, either exclusive of or in addition to regular mail. Lawyers that do so run the risk of violating the Rules of Professional Conduct if proper precautions are not taken. The Maryland State Bar Association's Committee on Ethics published Ethics Docket 2007-09, "Ethics of Sending and/or Using Metadata." There, the committee explored first, whether an attorney has an obligation to prevent transmission of metadata; and second, whether an attorney may review metadata sent by others.

Regarding the first question, the sending of electronic documents containing metadata, the committee pointed to Rules of Professional Responsibility 1.1[4] (competence) and 1.6[5] (confidentiality of information) and noted that attorneys have an ethical obligation "to take reasonable measures to avoid the disclosure of confidential or work product materials." This takes a common-sense approach toward metadata. First, it does not assume that disclosure of metadata is *per se* unethical. Rather, the metadata itself must be either confidential or work product to bring the disclosure within the possible scope of an ethics violation. Second, the opinion only requires that attorneys take "reasonable" measures to preclude disclosure. This does not equate into an absolute prevention of the transmission of confidential and/or work product metadata, which may be nearly

[1] Luddites were 19th century Leicestershire workers who destroyed textile machinery to protest technological advances brought about in the industrial revolution, which they feared would threaten their livelihoods. The term, along with "neo-luddism," has evolved to signify one opposed to technological change.

[2] The technical definition for 'metadata' is "data that provides information about other data." Merriam-Webster's online dictionary (visited July 27, 2007) <http://mw1.merriam-webster.com/dictionary/metadata>. Less enigmatically, it is "information describing the history, tracking, or management of an electronic document." Williams v. Sprint/United Management Co., 230 F.R.D. 640, 646 (D. Kan. 2005).

[3] For example, open a new Microsoft Word document. Type "Plaintiff will accept $10,000." Enable the track changes feature from the 'Tools' drop-down menu. After deleting the sentence, the document appears clean unless the 'Mark-up' feature is selected from the 'View' drop-down menu. Future recipients of the document will be able to see these changes made to the document.

[4] Rule 1.1 of the Maryland Lawyers' Rules of Professional Responsibility provides:
Competence. A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

[5] Rule 1.6 of the Maryland Lawyers' Rules of Professional Responsibility provides, in part: Confidentiality of information. (a) 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, and except as stated in paragraph (b).

impossible in this day and age of increasingly sophisticated hackers. Instead, it requires that attorneys be aware of the possibility of metadata transmission and take steps to avoid it.

On the second question, the committee approved the review and use of metadata received by an attorney and did not require that the recipient attorney verify whether the disclosure was intentional.[6] Furthermore, the Maryland ethics rules do not impose an obligation on the recipient attorney to report potentially inadvertently disclosed information.[7] However, the new Rules to the Federal Rules of Civil Procedure may alter this analysis for federal cases.[8]

Preventing Metadata Transmission

The Maryland opinion on metadata does not strictly prohibit disclosure, but requires "reasonable" measures to preclude disclosure. As an initial matter, attorneys and their staff should take great care before transmitting any documents electronically to determine if those documents ever contained confidential or otherwise sensitive information (for example, draft answers to interrogatories with notes of client conversations, or settlement demand packages with bottom-line dollar figures). An office policy should be established based on the likelihood of sensitive information in the document. Necessary precautions could entail:

- Print the document out and scan it in using a commercially-available scanner. The only significant metadata present will be the date the document was scanned and the title. This is the safest method, aside from simply producing hard copies.
- Word processing files (i.e., Microsoft Word and WordPerfect) can be "cleaned" of unwanted metadata by using a simple-text editor, like Windows Notepad, which is incapable of saving metadata. Select the text from your word-processing program (*cntrl-A*), copy the text (*cntrl-C*), and past the text into the Notepad document (*cntrl-V*). This will remove all metadata, but will also remove all formatting. Then copy the text from the Notepad document, and paste it into a **new** word processing program.
- Computer users with Acrobat 8 can eliminate metadata by clicking the 'Document' drop-down menu, select 'Examine Document,' click 'Check All' and 'Remove all Checked Items.' This will remove metadata, annotations and comments, hidden text, and bookmarks, leaving only a clean document.
- Microsoft Word users can follow the procedures listed on Microsoft's website to remove personal information, comments, revision marks, hidden text and old file versions.[9]
- WordPerfect Office X3 features a "save without metadata" option.
- When converting documents into PDF files from Microsoft Word, click 'Change Conversion Settings' from the 'Adobe PDF' drop-down menu, and make sure 'Attach source file to Adobe PDF' is unchecked. Otherwise, the underlying word processing document will be attached to the PDF document.
- Finally, other commercially-available products "scrub" metadata from individual files, including e-mails.[10]

A full list of steps is not possible here; however, attorneys and/or their IT department should check with their software manufacturers to determine the most efficient and practical methods for preventing metadata transmission.

With the advent of electronic court filing, many courts recommend that attorneys use the "convert to PDF" feature of their word processing programs to create PDF documents for filing. This creates a cleaner-looking document than manual scanning. However, the underlying document should be cleaned of metadata and other potentially sensitive information before converting the document to PDF, because that information can follow into PDF format. Using the methods above will ensure that for documents received by opposing counsel, "what you see is what you get."

Conclusion

Technological advances are inevitable, and only a Luddite would stoically refuse to accept those advances that can have a beneficial effect on his or her profession. Metadata is not something to be feared, but only something to be cautious of. With the proper precautions, client confidences can be maintained and documents can continue to be transported at the click of a button. ■

About the Author

John Cord, Janet, Jenner & Suggs, LLC, graduated from the University of Colorado School of Law in May 2003. Mr. Cord concentrates his practice on assisting victims of birth trauma and other serious injuries of medical negligence. He is licensed to practice in Maryland, the District of Columbia, Pennsylvania, Georgia and Minnesota. He is a member of the American Association for Justice and is the current chair of the Maryland Trial Lawyers Association Technology Committee.

[6] Other states find differently on these issues. For example, the Florida Bar opined that in some cases lawyers are not allowed to look for metadata in documents sent to them by opposing counsel ("It is the recipient lawyer's concomitant obligation, upon receiving an electronic communication or document from another lawyer, not to try to obtain from metadata information relating to the representation of the sender's client that the recipient knows or should know is not intended for the recipient.")(Opinion 06-02, issued Sept. 15, 2006).

[7] The view of the American Bar Association, promulgated by the Standing Committee on Ethics and Professional Responsibility in Formal Opinion 06-442 (Aug. 5, 2006), is that metadata may be used by the receiving attorney; however, an attorney who receives inadvertently sent information must notify the sender. The opinion does not discuss whether transmission of documents containing metadata is "inadvertent," but notes that the analysis may be fact-specific.

[8] See Grimm, Paul W., Ethical Issues Associated with Accessing and Using Metadata Related to Electronic Records, The Advocate, Young Lawyers Section–Maryland State Bar Association, v. 22, no. 3 (2007). Judge Grimm analyzes the potential impact of the recent amendments to the Federal Rules of Civil Procedure on the ethical obligations of attorneys with regard to metadata.

[9] Microsoft, *How to minimize metadata in Word 2003*. (visited July 27, 2007) <http://support.microsoft.com/kb/825576>.

[10] See, e.g., www.payneconsulting.com; www.esqinc.com; and www.litera.com; and www.docscrubber.com.