YOU DON'T SAY: ETHICAL CONSIDERATIONS REGARDING INADVERTENT COMMUNICATIONS IN THE ELECTRONIC AGE

JOHN SHAMPTON*
DAVID RITTER**

I. INTRODUCTION

The inadvertent disclosure of information that is not subject to discovery is a proper concern and, occasionally, a source of liability, on the part of attorneys engaged in civil litigation. A disclosure as simple as the mere fact of representation could conceivably do harm to a client's interests, yet nearly every document produced on popular word processing software carries with it hidden information disclosing the source, history, and even revisions, of that file; information which could be confidential and the disclosure of which could, under certain circumstances, result in preventable loss to a client. While there is a body of literature covering inadvertent disclosure in general, the subject of so-called "metadata" deserves closer scrutiny. In particular, the ethical implications of removing, or failing to remove, this information from files and the use of the information by opposing counsel, if not removed, are considered.

II. WHAT SHOULD WE READ?

"Gentlemen do not read each other's mail."[1]

With these words, in 1929, Henry L. Stimson, Herbert Hoover's Secretary of State, put an end to peacetime intelligence gathering.[2] Secretary Stimson's ethical principle has stood the test of time, even though Stimson later reversed himself (and the practice of surreptitiously "reading mail" was resurrected and expanded enormously). Simply put, reading another attorney's inadvertently forwarded mail is most likely unethical. This principle is recognized in a number of ethics opinions[3] as well as the Model Rules[4] in the form of the prohibition against making use of client confidences inadvertently transmitted.

The basic principle is stated in Model Rule 4.4:

---

* Ph.D., Professor of Business and Business Law, Texas Wesleyan University, Fort Worth, Texas.
** D.B.A., Associate Professor, Texas A&M University Central Texas, Killeen, Texas.

1 Henry L. Stimson, U.S. Secretary of State 1929-1933, *in* DAVID KAHN, THE READER OF GENTLEMEN'S MAIL: HERBERT O. YARDLEY AND THE BIRTH OF AMERICAN CODE BREAKING, at ix (2006).

2 *Id.*

3 The current state of opinion on this issue is summarized in ABA Legal Tech. Resource Center, *Helping Lawyers Sort the Technology Puzzle*, *at* http://www.ABAnet.org/tech/ltrc/fyidocs/metadatachart.html (last visited 2/19/2009).

4 ABA Center for Professional Responsibility, MODEL RULES OF PROF'L RESPONSIBILITY (6th ed. 2007).

Rule 4.4 Respect for Rights of Third Persons

(a) In representing a client, a lawyer shall not use means that have no substantial purpose other than to embarrass, delay, or burden a third person, or use methods of obtaining evidence that violate the legal rights of such a person.

(b) 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.

Although interpreted in a number of different ways, the Model Rule recognizes the Golden Rule – respect the privacy of others as you would expect them to respect yours. Subsection (b) of the Model Rule, however, leaves a bit to be desired when exploring the perimeters of the principle. As noted in the official comment to this rule,[5] the response required upon receiving such a document appears to be no more than giving notice. Any additional action or inaction is to be measured by state law.

The conflict that appears in various state ethics opinions on this point lies in the tension between suffering the consequences of one's own acts as opposed to protecting the rights of the innocent client.[6] In the former view, the attorney's negligence in inadvertently forwarding the information in question results in liability on the imprudent lawyer. In the latter, of course, the interests of the innocent client are supreme. The former rule would "let the chips fall" on the head of the lawyer who is at fault. This would promote care on the part of counsel but could result in avoidable losses for clients. If such is the case, it is presumed professional liability principles will protect the client. The second option is more difficult because it could excuse incompetence or even allow surreptitious and wrongful (intentional) manipulation by "inadvertently" revealing client confidences and then demanding advantageous protective measures of some sort.

The conflict between these two options is usually resolved by looking to the reasonable expectations of the party receiving the accidental revelation.[7] That is, if the receiving party knew (or should have known) that the information was unintentionally revealed, there is an ethical obligation to both notify the sender and refrain from making use of the information or its fruits. In opposition to this simple rule, however, is the principle of waiver of privilege. Even though unintentionally done, it is clear that disclosure of privileged material in some circumstances can result in the loss of its privileged status.[8] Although the cases generally turn on intent, the impossibility of

---

[5] MODEL RULES OF PROF'L CONDUCT R. 4.4 cmt 2 (6th ed. 2007) ("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, as is the question of whether the privileged status of a document has been waived. Similarly, this Rule does not address the legal duties of a lawyer who receives a document that the lawyer knows or reasonably should know may have been wrongfully obtained by the sending person.").

[6] *See, e.g.,* Brian Beckham, *Production, Preservation, and Disclosure of Metadata*, 7 COLUM. SCI. & TECH. L. REV. 1 (2006); Nancy A. Wanderer, *E-mail for Lawyers: Cause for Celebration and Concern*, 21 MAINE BAR J. 196 (2006), Matthew A. Reiber, *Latching Onto Laches: A Rules-Based Alternative for Resolving Questions of Waiver Following the Inadvertent Production of Privileged Documents in Federal Court Actions*, 38 N.M. L. REV. 197 (2008).

[7] Beckham, *supra* note 6.

[8] *Id.*

directly determining intent is a principle of common law with deep, well-established roots. Since intention can only be known by its objective manifestation, it is often impossible to distinguish between genuinely inadvertent disclosure and disclosure which results from gross negligence or even malice. In such a case, of course, waiver is clear and the information is now in the possession of the recipient to use in zealous representation of his or her client.[9]

This determination only becomes difficult where the transmission of the information in question does not clearly fall into a nicely defined category – either information which any reasonable lawyer would have protected or disclosures of which a reasonable practitioner might not be aware. The age of technology brings us a dilemma of this sort which, though not a new problem, appears to have evolved to the point where new duties of care may have arisen. A philosopher told us *tempora mutantur* – times change. Thus, handwritten documents have given way to typed and printed ones; carbon paper is a thing of the past; handwritten, double-entry accounting records have moved to personal computers sitting on our desks or even carried in our pockets, and techniques for making the lives of computer programmers easier have now become facts of life – and liability – for the users of modern computer software. This "new" danger is not new at all, since it's been around as long as word processing and spreadsheet packages have existed.[10] Years ago, the more technologically savvy and less "gentlemanly" practitioners discovered a source of information – a sort of other people's mail – which many senders were not even aware they were transmitting. These computer insiders were able for the time being to reap the benefits of an unfair advantage arising out of programmers' need to provide structure outside the documents being created. These "secret bits" were used by the programmers to assure documents could be archived, sorted, retrieved and otherwise managed without regard to their content.[11] The same embedded notations, however, would also reveal such interesting tidbits as when the files were opened, who opened them, how often they were opened and so forth, and might even disclose editorial changes made in the process of drafting the document.[12]

Allowing advantage to be taken of this technological insight clearly seemed unfair when the issue was first discovered. Surely only the "rocket scientists" who established the arcane digital formats for these files could be expected to understand what was there. Initial response by the legal profession to the acquisition and use of these items was to cry "foul." Today, however, it is increasingly clear that the responsible – and ethical – attorney must be fully aware of what hidden dangers appear in electronic-age documents. Although once merely a technician's crutch, these bits and bytes are now a fact of life for practitioners.[13] They are called "metadata."

---

[9] David G. Ries, *Information Security for Attorneys: An Ethical Obligation*, 78 PA. BAR ASS'N. Q. 1 (2007).
[10] NATIONAL INFORMATION STANDARDS ORGANIZATION (NISO), UNDERSTANDING METADATA (2004); Philip J. Favro, *A New Frontier in Electronic Discovery: Preserving and Obtaining Metadata*, 13 B. U. J. SCI. & TECH. 1 (2007).
[11] NISO, *supra* note 10.
[12] Microsoft Office Online, Find and Remove Metadata (Hidden Information) in Your Legal Documents, *at* http://office.Microsoft.com/en-us/help/HA010776461033.aspx (last visited 2/2/2009); How to Minimize Metadata in Word 2003, *at* http://support.Microsoft.com/default.aspx?scid=kb;EN-US;825576 (last visited Oct. 30, 2008).
[13] *See, e.g.,* Annie Dike, *Comment: A Lucky Break or an Ethical Dilemma? Assessing the Appropriate Response in the Face of Inadvertent Disclosure*, 31 J. LEGAL PROF. 279, 282 (2007); Susan Ardisson,

III. METADATA REVEALED

The term "metadata" literally means "data about data," which is hardly a useful revelation.[14] It would, however, help to understand the concept by oversimplifying for a moment. We have all had the experience, at some time or another, of packing for a move. If we were extremely organized, as computers tend to be, we would place only related items into a single packing carton and then carefully label the box with its destination and contents. Fragile items would be treated differently from hardy ones and their final resting place in the new location would be known before they were sealed up. That packing carton can be analogized to a computer file of virtually any type, whether a document file, digital photograph, spreadsheet or any other digital record. The items so carefully packed and placed in it are the data the file contains. The label on the outside is metadata.

Metadata serve the purpose of allowing the identification and classification of the information contained in the file for archival, retrieval and other such purposes. They assure, like the label on your carton, that photographs will not go into document files, just like pots and pans will not go to the bedroom. For computer files, however, metadata serve many additional purposes other than merely satisfying indexing needs. Besides describing the contents of the file, metadata entries may also provide its structure (e.g., number of pages, number of words, links to objects outside the file, and the like) and details such as authors, editors, information type, digital rights management (DRM) data, and "other stuff."[15] Although it is fairly clear that unintentionally providing some of the foregoing may create problems for both an attorney and client, we need to be very aware of the "other stuff" which may include even more than names and dates – it may reveal strategy, negotiations or even provide evidence of attempts to modify or suppress information properly subject to discovery.[16]

Thus, for a document created in Microsoft Word, information regarding the creator, date of creation, last access and information regarding the revision process will accompany the file so that it can be saved and later found for reopening. This seems simple enough. However, Microsoft Word is not unusual in that it also saves deletions, comments and other data that the drafter may have thought disappeared when the file was closed.[17] Ostensibly for the purpose of allowing reconstructions (to permit one to "undelete" such changes), the system stores this information which, under certain circumstances, can be reconstructed by opposing counsel after the document file has been turned over pursuant to discovery.

Digging a little deeper, technically, we find that metadata can be classified

---

Mining for Metadata: Ethical Considerations, 10 LAW J. 7 (2008); David Hricik, *Mining for Embedded Data: is it Ethical to Take Intentional Advantage of Other People's Failures*, 8 N.C. J. L. & TECH 231 (2007); David Hricik, *I Can Tell When You're Telling Lies: Ethics and Embedded Confidential Information,* 30 J. LEGAL PROF. 79 (2005); Crystal Thorpe, *Metadata: the Dangers of Metadata Compel Issuing Ethical Duties to 'Scrub' and Prohibit the 'Mining' of Metadata*, 84 N.D. L. REV. 257 (2008).

[14] NISO, *supra*, note 10.

[15] *Id.* at 2-5.

[16] A situation which is not limited in its applicability to American courts. *See, e.g.*, Simon Dawson, *The Power of Metadata*, 23 BARRISTER, *at* http://www.barristermagazine.com/articles/issue23/metadata.htm (last visited Nov. 6, 2008).

[17] Microsoft Online Office, *supra* note 12.

according to purpose into several basic types.[18] *Administrative* metadata, which provide information necessary for the management of resources; *descriptive* metadata which identify the type of file, its name or title, date of creation and other such facts necessary for sorting and retrieval; *structural* metadata the purpose of which are to describe the internal structure of the file and its contents, such as the chapters in a book; and *technical* metadata including such things as the description of a database system used in the file, data format, encoding, character set and other such information which allows the file to be preserved over time when new technology for data storage might require conversion of the file. There are a number of other ways of classifying metadata, however, since there is no standard convention.[19]

Some additional terms may occasionally be seen in discussions of the technical aspects of metadata.[20] The *scheme*, or *schema*, consists of the items to be recorded in order to meet the needs of the particular type of metadata – technical, descriptive and so forth. The *semantics* of the schema establish the meaning of each of the elements while the *content* of the schema consists of the actual value of each such element. Rules for creating content such as identification of prohibited characters, specifying allowable label names and so on are referred to as the *grammar* of the schema and, finally, the *syntax* specifies how the content is to be coded. Metadata generally are rendered in a high-level language such as XML (extensible markup language) which is a version of the more familiar HTML (hypertext markup language) or, more commonly, the sophisticated and flexible SGML (standard general markup language). Thankfully, users of metadata rarely need to know this – only that there is information that might be buried in the file.

IV. RETRIEVING AND USING METADATA

How the discoverer of metadata goes about retrieval of the information, of course, is of great importance in analyzing the ethical considerations. In applications such as Microsoft Word, much of the descriptive metadata including the "other stuff" mentioned above can be retrieved and examined using functions provided in the software itself. Thus, by merely asking the program to show the "markup view" (where the creator has, intentionally or not, directed the program to track changes and has not removed them), previous deletions and additions will be revealed in "redline" format! As suggested above, performing such simple operations, which any reasonably proficient user of the software would be expected to understand, is unlikely to violate any expectation of privacy. That is, if the revision history has been left in the document, there should be nothing wrong with reading it, right? The fault lies with the creator who allowed such information to lie "in plain sight" to be read by anyone who wishes! Some jurisdictions, however, differ.[21]

Some other types of metadata, especially technical and structural metadata, are viewable only by examining the binary file – that is, the actual bits and bytes that make up the file on the disk – a process that requires some sophistication and specialized

---

[18] NISO, *supra* note 10, at 2.
[19] *Id*. at 1.
[20] *Id*. at 3ff.
[21] ABA, *supra* note 3.

software.[22] Using such extraordinary means to discover information that has otherwise been properly withheld would seem to violate the ethical principles discussed above. Since only the archetypal "nerd" would even know it is there much less how to retrieve it, the reasonably prudent attorney would not ordinarily have a duty to take it into account.

V. "STRIPPING" AS A SOLUTION

Since the addition of metadata is controlled by the application software and is, for the most part, automatic, preventing disclosure would require removing all such data from the file after the file has been created (a process often described as "stripping" or "scrubbing"[23] the file). For clearly privileged information such as "redlined" editorial changes, stripping is unquestionably appropriate. Other information, however, is less obviously confidential. If files are stripped routinely upon creation, of course, none of the metadata problems should arise.[24] Ethical concerns do, of course, arise when "stripping" occurs after a discovery request has been made or the metadata otherwise disclosed. Although the easy answer would be to establish a rigid policy of stripping all metadata immediately upon completion of the drafting project, it must be pointed out that the metadata exist for a reason. Routinely stripping all metadata could potentially interfere with storage, retrieval and other uses of the file outside the litigation context. Some considerations for a limited stripping policy, then, should be explored.

In the case of tracked changes, it would be appropriate that as soon as a document has been placed in final form all revision history should be deleted as a matter of course. This action would be analogous to removing prior drafts from a hardcopy file and is clearly justified by the desire (at least in the case of hardcopy) to avoid confusion as to which revision is operative. Like previous drafts retained in the attorney's working file, the electronic revision history should be non-discoverable work product.

At least some of the information in the descriptive metadata is reasonably necessary, or at least helpful, in maintaining document control within the office. There is nothing cryptic about such information – it is readily accessible in documents created in the Windows version of Microsoft Office by merely right-clicking on a file name and selecting "properties/details" (in the Macintosh version, select "get info"). Moreover, it would appear that most – if not all – of this descriptive information could be reconstructed from a simple examination of a hardcopy file, so a policy of immediate deletion may not be problematic. Indexing systems that use this data source could suffer, however. Given the potential sanctions for stripping a file at the wrong time intentionally or otherwise, the inconvenience of routinely stripping newly created files would appear to be minimal.

---

[22] A number of commercial sources exist for software intended specifically to seek out and reveal metadata at all levels of a file. *See, e.g.*, Ann Bednarz, *Software Cleanses Sensitive Documents*, 23 NETWORK WORLD 23 (2006); Randall Farrar & Susan McClellan, *Esquire Innovations, Inc. White Paper, Metadata Management in Microsoft Office: How Firms Can Protect Themselves Against Unintentional Disclosure and Misuse of Metadata*, *at* http://esquine.com/Content/WhitePapers/MetdataManagementMicrosoftOffice.php (last visited 11/6/2008).

[23] Thorpe, *supra* note 13.

[24] *Id.*

Clearly, the most interesting type of metadata would be found in the form of reviewer comments and language changes made during the creation of a document. There should be little argument that removing such metadata, even in the expectation of a discovery request, would be no more or less than the removal of other privileged material and thus certainly allowable. On the other end of the spectrum would be the metadata that are recorded in the binary version of the file – the bits and pieces which can be found only through the use of specialized software or high levels of technical expertise. It is fair to say that "mining" this source of metadata goes beyond the expected technological prowess of the average lawyer, and thus should be impermissible. The gray area, as usual, lies between these extremes – the metadata stored along with the contents of the file that indicate who has opened it and when (along with other basic descriptive facts). Not surprisingly, ethics opinions treating this matter have varied widely in their approaches and conclusions.

VI. SOME ETHICAL ISSUES

The American Bar Association Legal Technology Resource Center recently (February 19, 2009)[25] summarized the position of several states[26] on three essential questions. Those are what duties may arise on the part of the sender of documents that include metadata, to what extent may a recipient go to locate and make use of metadata received, and whether the recipient must give notice to the sender if metadata are found.

The first of these three questions shows the greatest consistency of opinion across the states surveyed. Of the nine states reported by the Legal Technology Resource Center as having dealt with the metadata matter, only one (Pennsylvania) failed to respond explicitly to the issue of whether there is a duty to protect metadata from disclosure while the eight remaining unanimously established a standard of "reasonable care" on the part of the sender in assuring that client confidences, otherwise privileged material, or other harmful information is not released. In most cases, the standards cited are based on Rules 1.1 and 1.6 concerning client confidences.[27] Thus, the ABA report notes that Alabama places an obligation on the sending attorney to take on the "ethical duty to exercise reasonable care when transmitting electronic documents to ensure that he or she does not disclose his or her client's secrets and confidences."[28] Similarly, the Arizona Bar states that "the recipient lawyer has a . . . duty not to 'mine' the document for metadata that may be embedded therein or otherwise engage in conduct which amounts to an unjustified intrusion into the client-lawyer relationship that exists between the opposing party and his or her counsel."[29]

Interestingly, the tenth reviewed authority, the ABA Standing Committee on Ethics and Professional Responsibility, purports to take no position on this issue, while at the same time comments on techniques for removing or eliminating the threat of metadata

---

[25] ABA, *supra*, note 3.
[26] *Id.* (summarizing the positions of Alabama, Arizona, Colorado, Florida, Maine, Maryland, New York, Pennsylvania and the District of Columbia as well as the ABA Standing Committee on Ethics and Professional Responsibility).
[27] FED. R. CIVIL P. 1.1, 1.6.
[28] ABA, *supra* note 3.
[29] State Bar of Arizona, *07-03: Confidentiality; Electronic Communications; Inadvertent Disclosure*, *at* http://www.myazbar.org/ethics/printop.efm?id=695 (last visited Feb. 19, 2009).

such as "scrubbing" or removing it from the file before transmittal, or entering into a prior agreement with counsel to resolve any metadata questions that may arise. While the ABA report suggests that the confidentiality requirement of rule 1.6 would apply, it is unclear whether application of that rule would mandate assuming a duty of reasonable care or not.[30]

The third question showed somewhat less agreement, with Alabama and Maine establishing no rule, and with Maryland the sole holdout (finding no obligation to give notice, but also expressly indicating that Model Rule 4.4 had not been adopted in that state) in the consensus of the rest of the jurisdictions that Model Rule 4.4 requires giving notice to the sender when metadata is retrieved. Although receiving notice would permit a sender to determine what the consequences of the disclosure might be, the official comment to Model Rule 4.4 specifically refrains from any advice as to what obligations, if any, may apply to the recipient.

As to the second question treated, whether it's legitimate to even look for metadata, Alabama, Arizona, Florida, Maine and New York say no, you may not. The ABA, Colorado, Maryland and the District of Columbia say sure, go ahead. Pennsylvania passes. It is not clear, however, that all of the jurisdictions have the same understanding of "mining" metadata. It is likely that they speak to the software-based functions, mentioned above, and not to the "bit twiddling" required to read the binary data directly from the disc files. This would be consistent with the evolving expectation of basic expertise in the use of software on the part of attorneys – if one uses a particular package, one certainly should be responsible for the regular ("default") output of those packages but not necessarily for the binary images that are created. It appears that the position of the opposed jurisdictions is based on the technicality of the document-creation process. If that is, in fact the case, then it is inevitable that a duty to understand these normal processes will eventually evolve. *Tempora mutantur*.

If there is no affirmative obligation to refrain from looking for or making use of the hidden information, the question naturally turns to what use might be made of it. Alabama, Arizona Florida and Maine argue against any use, with the Alabama commission taking the position that mining constitutes a knowing and deliberate violation of the right of confidentiality.[31]

The other jurisdictions prohibiting the search for, much less use of, metadata consistently treat such activity as, it would appear, taking advantage of an understandable level of ignorance presumed to exist in the sending party. As suggested herein, the ubiquity of metadata-laden electronic documents renders it unlikely that this position will continue to survive. Assuming, then, that at least in the foreseeable future the use of freshly dug up metadata will be permitted, a brief discussion of what it might be used for is appropriate.

It is clear that at the very least the descriptive metadata will assist the recipient in strategizing or directing additional discovery.[32] For example, if the list of editors of a document includes a previously unidentified expert it might be very interesting to find out why that expert's opinion has not been disclosed in other discovery – perhaps this

---

[30] *See* ABA, *supra* note 3; *see also* 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).
[31] ABA, *supra* note 3.
[32] Joseph, E. Gallagher, E*thics: the Ethical Dimension of Electronic Discovery Amendments to the Federal Rules of Civil Procedure*, 20 GEO. J. LEGAL ETHICS 613 (2007).

expert agrees with the recipient's position? Other uses should be obvious.

Another question, however, involves the actual admissibility of metadata obtained during discovery through the failure of the sender to protect its confidentiality.[33] Under federal rules, in particular Rule 34(b), a requesting party may "designate the form or forms in which it wants electronically stored information produced." If the form requested would include all metadata (frequently referred to as "native" files – those originally produced by the software[34]), it is clear that "stripping" such files would be a violation, as would producing them in a format such as PDF (Portable Document Format), a method of producing documents that can be read without regard to the "platform" or computer on which they are displayed but which removes at least some of the native metadata.[35] If an advocate, in possession of electronic documents with a wealth of metadata that have not been sanitized, receives such a request, Rule 26(b)(5) does permit a modicum of relief by allowing sequestration of the disclosures until a court has a chance to rule on claims of privilege. In the absence of privilege, of course, ordinary discovery practices would require the information be revealed. In such a case, the only hope would be for the technologically savvy attorney (as it appears we all must be, today[36]) to have taken steps, preferably at the creation of the documents in question, to assure no information in any way useful to an opponent lies buried within the digital corpus of the documents.

VII. CONCLUSION

The Latin aphorism referred to above is, in its entirety, *tempora mutantur, nos et mutamur in illis* – "the times are changing and we are changing with them." This is nowhere more obvious than in the technology supporting modern litigation. While deep and philosophical discussions of ethics, expectations and intent may be of academic interest (and, admittedly, even some practical usefulness), the simple fact of the matter remains to be that a responsible attorney cannot ethically refuse to enter the twenty-first century. Previous advances in law office technology, such as the typewriter, resulted in improved efficiency more than anything else. Today's digital revolution also involves the enhancement of efficiency, but at the same time produces new and frequently unexpected problems. Simply put, as systems become more complex so do solutions. These complex solutions present new hazards, both to the attorney and the client. Maintaining the technological competence to deal with these surprises is part of maintaining professional competence, which means learning how to handle such tools as metadata is becoming an ethical duty.

---

[33] Eleanor B. Kellett, U*nintended Consequences: Maintaining Basic Understandings of Technology – An Ethical Obligation*, 18 S.C. LAW. 42 (2006); Lucia Cucu, *The Requirement for Metadata Production Under Williams v. Sprint/United Management Co.: An Unnecessary Burden for Litigants Engaged in Electronic Discovery*, 93 CORNELL L. REV. 221 (2007).

[34] *See, e.g.* Mike Breen, *Nothing to Hide: Why Metadata Should be Presumed Relevant*, 50 KAN. L. REV. 439 (2008); W. Lawrence Wescott II, *The Increasing Importance of Metadata in Electronic Discovery*, 14 RICH. J. L. & TECH. 10 (2008).

[35] As suggested above, commercial software solutions abound. *See supra* note 22; *see also* Redaction of Litigation PDFs with Adobe Acrobat 8 and Other Tools *at* http://www.lexbe.com/hp/lititech-Redaction-of-Litigation-PDFs-with-Acrobat-8-and-Other-Tools.aspx (last visited Feb. 3, 2009).

[36] Bradley H. Lieber, A*pplying Ethics Rules to Rapidly Changing Technology: The DC Bar's Approach to Metadata*, 21 GEO. J. LEGAL ETHICS 893 (2008).