Technological Entanglements: Evidentiary and Ethical Considerations of Metadata in Interjurisdictional Litigation*

Edward A. Morse

McGrath, North, Mullin & Kratz Chair in Business Law
Creighton University School
of Law, Omaha, Nebraska
(http://culaw2.creighton.edu/morse) (morse@creighton.edu).

Abstract: Ethical and evidentiary rules governing the disclosure of confidential information are interrelated in many respects. Nevertheless, these rules are generally developed independently through different legal channels. Different approaches to the inadvertent disclosure of confidential information have emerged, leading to uncertain results in different jurisdictions. Uncertainty persists with regard to metadata available from electronic document formats. This paper explores the tension between the competing approaches this emerging problem. It argues that ethical and evidentiary principles addressing the protection and discovery of metadata should be coordinated in order to avoid creating incentives to maximize litigation costs.

Keywords: confidentiality, discovery, electronic evidence, ethics, metadata

1. Introduction

Technological change has impacted the practice of law in many ways. Electronic communication practices have increased not only the speed at which we exchange information, but also the scope of available data to be stored, managed and protected. Attorneys in the United States are governed by ethical rules that constrain their professional conduct, including the handling of client information. These rules develop primarily at the state level, thereby creating obligations and protections that may differ depending on the jurisdiction(s) in which an attorney is professionally licensed. Other legal rules govern the substantive, procedural, and evidentiary dimensions of legal claims. These rules emanate from either federal or state sources, and they can directly impact the presentation (and possibly the outcome) of a client's case. Technological changes often generate modifications of legal and ethical rules to adapt to new conditions. However, the differing sources for generating these rules can translate into inconsistent obligations and results, and particularly so during these transition periods where the legal system is adapting to technological change. This paper addresses the phenomenon of metadata embedded in electronic documents. Metadata presents challenging evidentiary and ethical questions that are often interconnected, and which remain unresolved in most jurisdictions. Current legal and ethical rules need to be coordinated in order to develop a workable framework that appropriately balances the interests of client confidentiality with the associated costs to the legal system, including the costs of preventative measures to protect against the disclosure of metadata, the costs of discovering metadata content, and decision-making costs associated with disputes over evidentiary privileges.

2. What is Metadata?

Metadata is a relatively new term that can be used to describe the particulars of an electronic document. The Sedona Guidelines, which are the product of an influential working group of lawyers, judges, and technology experts, define metadata as follows: "Metadata is information about a particular data set which describes how, when and by whom it was collected, created, accessed or modified and how it is formatted (including data demographics such as size, location, storage requirements and media information)." (SEDONA GUIDELINES at 94). Whereas data content in a printed document is generally limited to what can be seen, metadata is hidden to casual observation, but can be made visible through exercising appropriate technical skills. (Lange & Nimsger at 247). Examples include the file name, size, date of creation, or dates of last access. Information about authorship, time for creation and editing, and the source of the original document may also be available. Features like the

* A version of this paper was published in Kierkegaard, S. (2006) Business Law and Technology Vol. 1 and presented in the 2006 IBLT Conference , Denmark.

"track changes" function of Microsoft Word may also provide extensive information about the nature and extent of document modifications, so that text that appears to be deleted may in fact become accessible.
Metadata adds significant utility for electronic document users, as some dimensions
of metadata are essential for the management of electronic fi les. Database functions, which allow searches by date or author, for example, could not be used without the presence of metadata. (SEDONA GUIDELINES at 84). Metadata may also prove useful in authenticating files, showing their provenance and creation within the requisite timeline. "Track changes" features also prove highly valuable for collaborative work, facilitating efficient and effective editorial modifications. On the other hand, metadata may sometimes be incorrect or misleading. For example, some software may carry forward an original author's name and not track the identity of the person making a modification to that document. (SEDONA GUIDELINES at 84; *Williams v. Sprint/United Management Co*., 230 F.R.D. 640, 646 (D. Kan. 2005). Even more problematic is the possibility that metadata may reveal information that should not be disclosed to others, whether for purely prudential reasons or to fulfill a professional obligation to protect confidential client information. Inadvertent disclosures of metadata publicized in the popular press include:

- Political operatives circulated a Microsoft Word document without attribution, seeking to criticize the nomination of Justice Samuel Alito to the Supreme Court. Metadata in this document revealed the author to be the Democratic National Committee and pegged the date of authorship to the time immediately following the
- Resignation of Justice O'Connor. (Zeller, 2005)
- A U.N. report on Syria's involvement in the assassination of Lebanon's former prime minister, when examined for metadata, showed the names of others involved in the plot that were ultimately deleted from the final draft, thus causing suspicion about their involvement. (Id.)
- The California Attorney General distributed a letter critical of the use of peer-to- peer file sharing software. Metadata revealed one of the authors of the letter was "stevensonv" – a senior VP at the MPAA, leading to political criticism. (Id.)
- A job candidate submitted a resume in Word format. The firm reviewed it and discovered that it had been heavily edited by a professor. As the firm noted, "It did not help his case." (Walker, 2006).

Attorneys also wish to avoid embarrassment and unwanted scrutiny for themselves and their clients, as shown in these examples. But other weightier matters are also involved, including the disclosure of confidential client communications or attorney work product, with potential harm to a client's case and the possibility of violating professional ethical standards. Evidentiary and ethical issues lurk here, and both are addressed below.

2. Evidentiary Issues: An Overview

Although the quest for truth is important, truth is not the only value recognized in developing a system of justice. Two important evidentiary privileges operate to protect against the disclosure of confidential communications between clients and their counsel: the attorney-client privilege and the work product doctrine. An understanding of each is important to an analysis of the significance of metadata disclosure.

A. Attorney-Client Privilege.

The attorney-client privilege is among the oldest privileges for confidential communications. Rooted in the common law, (FRE 501, 2006) it is based on the premise that promoting effective communications between lawyers and their clients will enhance not only the observance of law, but also the administration of justice. (*Swidler & Berlin v. United States*, 524 U.S. 399 (1998)). The protection of the privilege goes beyond matters of criminal liability, extending to a broad range of human motivations. As the Supreme Court has observed, Clients consult attorneys for a wide variety of reasons, only one of which involves possible criminal liability. Many attorneys act as counselors on personal and family matters, where, in the course of obtaining the desired advice, confidences about family members or financial problems must be revealed in order to assure sound legal advice. The same is true of owners of small businesses who may regularly consult their attorneys about a variety of problems arising in the course of the business. These confidences may not come close to any sort of admission of criminal wrongdoing, but nonetheless be matters which the client would not wish divulged. (*Id*., 524 U.S .at 407-408).

Though the attorney-client privilege is quite robust, it is not absolute. As discussed below, it may be waived expressly or implicitly by conduct. For example, clients may waive the privilege for matters they disclose, through testimony or otherwise. Waiver can also occur with regard to matters that their attorneys disclose in the course of the representation. For example, an attorney may waive the attorney-client privilege by offering a document into evidence which contains otherwise privileged communication. (Note: Representative cases include *Miller v. Continental Ins. Co.*, 392 N.W.2d 500, 505 (Iowa 1986); *Brandon v. West Bend Mut. Ins. Co.*, 681 N.W.2d 633, 639, 642 (Iowa 2004). ("The waiver may be express or implied. It may be based not only on words expressing intent to waive, but conduct making it unfair for a client to invoke the privilege. Thus, we recognize waiver occurs when a person holding a privilege discloses or, for purposes of discovery, plans to disclose privileged matters."))Less clear, however, is the effect on waiver in the case of an inadvertent disclosure, a problem which is shared with that of the privilege associated with work product doctrine.

B. Work Product Doctrine

A similar evidentiary privilege is followed with regard to the materials prepared by attorneys, or at their direction, in preparation for litigation. The work product doctrine provides for a qualified privilege from discovery regarding these materials. The underlying purpose of the doctrine is quite similar to that for the attorney-client privilege, as it is rooted in preserving the freedom to prepare a client's case. As the Supreme Court stated in 1996,"In performing his various duties ... it is essential that a lawyer work with a certain degree of privacy, free from unnecessary intrusion by opposing parties and their counsel. Proper preparation of a client's case demands that he assemble information, sift what he considers to be the relevant from the irrelevant facts, prepare his legal theories and plan his strategy without undue and needless interference.... This work is reflected, of course, in interviews, statements, memoranda, correspondence, briefs, mental impressions, personal beliefs, and countless other tangible and intangible ways--aptly but roughly termed ... the 'work product of the lawyer. Were such materials open to opposing counsel on mere demand, much of what is now put down in writing would remain unwritten. An attorney's thoughts, heretofore inviolate, would not be his own. Inefficiency, unfairness and sharp practices would inevitably develop in the giving of legal advice and in the preparation of cases for trial. The effect on the legal profession would be demoralizing. And the interests of the clients and the cause of justice would be poorly served." *F.T.C. v. Grolier Inc*., 462 U.S. 19, 29 (1983) (quoting *Hickman v. Taylor*, 329 U.S. 495, 511 (1947)).The work product doctrine provides a qualified privilege against discovery, but that privilege is subject to waiver or abrogation in some circumstances. However, like the attorney-client privilege, the matter of waiver may be presented when the attorney has not acted consciously, but has instead inadvertently disclosed a document or revealed information that might otherwise be covered by the privilege. Such disclosures might include the metadata embedded in electronic documents, as well as documents in other forms. This topic is addressed below.

C. Waiver by Inadvertent Disclosure.

The matter of inadvertent disclosure of otherwise privileged information has been presented in a number of U.S. jurisdictions, though it is far from resolved. As one state court recently noted, "We understand the nature and scope of the problems of inadvertent disclosure of discovery materials for trial lawyers. We also recognize that courts from other jurisdictions have taken divergent paths in their efforts to address the issue." (*Wells Dairy, Inc. v. American Indus. Refrigeration, Inc.*, 690 N.W.2d 38, 42 (Iowa 2004) (footnotes omitted).Three primary approaches have emerged for dealing with this issue: a strict approach, in which disclosure is thought to remove the protection of privilege, a lenient approach, which is highly protective of privilege in the face of inadvertent disclosure, and an intermediate approach, focusing on facts and circumstances. As discussed below, those approaches impose differing consequences that impact not only the client's case, but also the costs likely to be invested in preventing inadvertent disclosure. The strict approach is based on the proposition that since privileges are in derogation of finding the truth, waiver may occur through any disclosure, including an inadvertent one. Cases such as Wichita Land & Cattle Company v. American Federal Bank, 148 F.R.D 456 (D.D.C. 1992) reflect the view that unintentional disclosure may constitute a waiver.

However, even this court would recognize an exception for a wrongful disclosure, such as by a disgruntled employee. In that case, conferring a waiver of privilege would effectively encourage complicity with the wrongdoer in order to obtain access to the fact. The strict approach thus represents the greatest harm to the client from an attorney's error. In contrast, the lenient approach is based on the proposition that the privilege

belongs to the client, who should not suffer for human errors – as opposed to deliberate policy choices -- made by his attorney. (Examples of cases adopting this approach include: *Corey v. Norman,Hanson & DeTroy*, 742 A.2d 933, 941-42 (Me.1999); *Helman v. Murry's Steaks, Inc.*, 728 .Supp. 1099, 1104 (D.Del.1990); *Kansas-Nebraska Natural Gas Co., Inc. v. Marathon OilCo.*, 109 F.R.D. 12, 21 (D.Neb.1983); *Mendenhall v. Barber-Greene Co.*, 531 F.Supp. 951, 954-55 (N.D.Ill.1982).This approach assumes that the client should knowingly and intelligently waive the privilege, and absent those conditions, the privilege is protected. An inadvertent disclosure, such as through a mistaken release of a privileged document in response to a discovery request, would not give rise to waiver.The third approach takes a middle ground, focusing on the equities of waiver given the particular facts and circumstances of the disclosing activity. This approach recognizes that even the most stringent approach is imperfect; "reasonable precautions are not necessarily foolproof." (Bank *Brussels Lambert v. Credit Lyonnais*, 160 F.R.D. 437, 443 (S.D.N.Y.1995))A recent case summarizes the considerations undertaken in this approach as follows:

1. the reasonableness of the precautions taken to prevent inadvertent disclosure in view of the extent of document production,
2. the number of inadvertent disclosures,
3. the extent of the disclosures,
4. the promptness of measures taken to rectify the disclosure, and
5. whether the overriding interest of justice would be served by relieving the party of its error."(*Gray v. Bicknell*, 86 F.3d 1472, 1484 (8th Cir.1996) (citing *Hydrafl ow, Inc. v. Enidine Inc.*,145 F.R.D. 626, 637 (W.D.N.Y.1993)).

Some of these factors are indeterminate. For example, one court has taken the position that "reasonable precautions" may take into account the applicable costs, as well as customary practices, measured from the perspective of the time and location of the event.[1] (See, e.g., U.S. ex rel. Bagley v. TRW, Inc. 204 F.R.D. 170, 179-80 (C.D.Cal. 2001) A large number of inadvertent disclosures might well occur in the context of an electronic document production, but this might not, of itself, reflect a lack of due care. These divergent approaches produce quite different results for clients, as well as incentives for attorneys to take precautions against inadvertent disclosure. Table 1, below, summarizes several salient features of these three approaches.

Table 1: Comparison of Judicial Approaches to Waiver Approach:

Result:	*Lenient*	*Strict*	*Balancing*
Harm to Disclosing Client:	low	high	low
Incentive for Care:	low	high	moderate
Decision Costs:	low	low	high

The potential "harm to disclosing client" is defined as the risk of losing a substantive right in the preparation of his or her case for trial. The evidence disclosed, if not protected by privilege, may thus be used against the client in the judicial proceeding. The magnitude of the harm will differ depending on the nature of the disclosure. The "incentive for care" here is defined as the impact of the decision rule on the degree of care exercised by the attorney in preventing the inadvertent disclosure. For this purpose, a heightened incentive for care is also likely to involve increased costs, in the form of an investment in preventive review. The "decision costs" category refers to the likely costs of resolving a privilege dispute in the event an inadvertent disclosure occurs. The comparative simplicity of the strict or lenient approaches produces a more predictable outcome than the balancing approach, which requires proof on a number of factors. Moreover, as noted above, some of these factors are rather open-ended and context specific, leading to more extensive fact-finding and argument.

Courts have not yet settled on an approach to the matter of inadvertent disclosure in many jurisdictions. (*See, e.g., Engineered Products Co. v. Donaldson Co.*, 313 F.Supp.2d 951, 313 1020 -1021 (N.D.Iowa 2004) (noting uncertainty in Iowa on this issue). It should be noted that where state law provides the rule of decision, state law governing privilege determines the result, regardless of the fact that the decision is in federal court. *See Gray v. Bicknell*, *supra* note 5.) However, a balancing approach that focuses on whether reasonable steps

[1] "Carelessness should not be inferred merely because an inadvertent production of privileged documents occurred. The reasonableness of the precautions adopted by the producing party must be viewed principally from the standpoint of customary practice in the legal profession at the time and in the location of the production, not with the 20-20 vision of hindsight."

have been taken to secure the data is apparently gaining momentum. At the Federal level, the Judicial Conference's Advisory Committee on Evidence Rules released a "Summary for Bench and Bar" in August 2006, regarding proposed amendments to Rule 502 of the Federal Rules of Evidence. As the summary memorandum explains, the amended rule "is intended to reduce the risk of forfeiting the attorney-client privilege or work-product protection so that parties need not scrutinize production of documents to the same extent as they now do. Under the new rule, the inadvertent disclosure of privileged information would not effect a waiver if reasonable steps were taken to prevent the disclosure, and retrieval of the information is promptly demanded."

The committee notes to the proposed amendments recognize widespread concerns about the costs associated with review, particularly where electronic discovery is involved. Case law cited by the Committee includes actions where costs associated with production review for privilege would cost in the hundreds of thousands of dollars, and concerns that such costs bear "no proportionality to what is at stake in the litigation." (See Advisory Committee Notes to Proposed Amendments of F.R.E. 502 (citing *Rowe Entertainment, Inc.v. William Morris Agency*, 205 FRD 421, 452-26 (SDNY 2002); *Hopson v. City of Baltimore*,232 F.R.D. 228, 244 (D. Md. 2005)).

Another aspect of the proposed amendments to Rule 502 also merits attention. The amendments recognize the possibility of private ordering in resolving matters of privilege. Subsection (e) provides: "An agreement on the effect of disclosure of a communication or information covered by the attorney-client privilege or work product protection is binding on the parties to the agreement, but not on other parties unless the agreement is incorporated into a court order." Though case law recognizes the role of private ordering, (*See, e.g., Zubulake v. UBS Warburg* LLC, 216 F.R.D. 280, 290 (SDNY 2003)) which might allow parties to produce documents without privilege review in favor of an agreement to return any privileged documents (a so-called "claw back" agreement), this provision would further legitimate that practice. However, as the committee notes point out, if disclosure is deemed to cause waiver in separate litigation, such an agreement is not binding on other parties. A court order would be required in those circumstances.

These proposed amendments affecting federal rules would not bind state courts. Moreover, even if adopted, the incentive structures described above take into account only the effects of the law of evidence applicable to the disclosed item. Despite the reduced risks to the client if a lenient or a balancing test is adopted, there are still risks to client wellbeing on account of failure to attend to privilege issues. As one court has noted, "[O]ne cannot 'unring' a bell." (*Id.* at 443 (*quoting FDIC v. Singh*, 144 FRD 252, 253 (D. Me. 1992)).

Information revealed may nevertheless lead to the discovery of other valuable evidence, which may not have otherwise been unnoticed. Thus, incentives exist for discretion and care quite apart from the possibility of evidentiary sanctions. Professional regulations involving ethics also address these concerns.

4. Professional Responsibility Standards Affecting Inadvertent Disclosures

In addition to the evidentiary privileges allowed for attorney-client communications and items covered by the work product doctrine, attorneys are also subject to rules of conduct that affect the manner in which they relate to others, including their clients, other attorneys, and the courts. Though a comprehensive analysis of these rules is beyond the scope of this article, it is helpful to identify important principles under the Model Rules of Professional Conduct, which are adopted (albeit with some modest variations) in the vast majority of U.S. states.

A. Confidentiality

Rule 1.6(a) provides in part: "A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation, or the disclosure is [otherwise] permitted…." Comments to this rule provide that competence in safeguarding client information against inadvertent or unauthorized disclosure is expected. (Comment 16). This also includes people under the lawyer's supervision, such as support staff. Moreover, the lawyer is expected to exercise reasonable precautions in transmitting client information, which are designed to ensure that the information does not come into the hands of "unintended recipients." (Comment 17)

The scope of reasonable precautions has not always been consistently applied. For example, ethics opinions in Iowa dealing with the then-new technology of e-mail initially required written consent from clients with explanations of the risks of e-mail transmissions, or requirement to use encryption technologies. (Iowa

Ethics Opinion 96-1). However, a later opinion left matters of security to private ordering between the lawyer and client. (Iowa Ethics Opinion 97-1). After all, regular mail can also be intercepted. This rule is consistent with the current approach of the Model Rules, and with the rules adopted by the American Bar Association (ABA), which are applicable only to its members. (ABA Formal Opinion No.99-413). Since the ABA is a voluntary association, but state bar membership is mandatory for a license to practice, the ABA opinions only carry persuasive force. Moreover, reasonable precautions may also extend to the storage of client information, including electronic information. For example, Arizona Opinion No. 05-04 (July 2005), involving security of electronic information, leaves the matter of security to the attorney, requiring "reasonable and competent steps" to ensure preservation of confidential information and electronic information. "An attorney who lacks or cannot reasonably obtain that competence is ethically required to retain an expert consultant who does have that competence." This duty extends not only to inadvertent disclosure, but also to preventing hackers and others with malicious intentions to access or destroy data.[2]

B. Partisan Advocacy (and Limitations Thereon)

In an adversary system, the zealous representation of one's client is important. Model Rule 1.3 provides in part: "A lawyer shall act with reasonable diligence and promptness in representing a client." This requires dedication and commitment, described in comments as "zeal un advocacy." (Comment 1).However, comments to the rules explain that this zeal is not without limitations. Comment 1 to Model Rule 1.3 as adopted in Iowa states:

> A lawyer is not bound, however, to press for any advantage that might be realized for a client. For example, a lawyer may have authority to exercise professional discretion in determining the means by which a matter should be pursued. See rule [1.2]. The lawyer's duty to act with reasonable diligence does not require the use of offensive tactics or preclude the treating of all persons involved in the legal process with courtesy and respect.(See Iowa Ct.R.ch.33)

A similar rule prescribes fairness to opposing counsel and the opposing party. Rule 3.4 provides in part: "A lawyer shall not: (a) unlawfully obstruct another party's access to evidence or unlawfully alter, destroy, or conceal a document or other material having potential evidentiary value. A lawyer shall not counsel or assist another person to do any such act …." As will be discussed below, legal consequences may attach to the spoliation of evidence, and these consequences supplement the prescription of the rules of conduct.

Rule 4.4 provides for duties to third persons, including opposing counsel. Subsection (a) provides a general proscription against misconduct:"(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." Comments indicate, that as a general matter, "Responsibility to a client requires a lawyer to subordinate the interest of others to those of the client, but that responsibility does not imply that a lawyer may disregard the rights of third persons." (Comment 1). Subsection (b) of Rule 4.4 addresses a slightly different dimension of partisan behaviour: the ethical responsibilities in the face of inadvertent disclosure.

C. Inadvertent Disclosure: Redressing Errors of Opposing Counsel

Rule 4.4(b) states: "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." This rule only requires notice, and no more, from the receiving lawyer. It also leaves open the resolution of evidentiary matters applicable to the disclosed document, including whether waiver of privilege has occurred. Comment 2 states in part: "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." Prior approaches to the matter of an inadvertent disclosure required much more from the lawyer. In ABA Formal Opinion 92-368 (1992), the ABA Standing Committee on Ethics and Professional Responsibility essentially imposed three duties on an attorney receiving privileged materials from

[2] Some attorneys contend that destruction of hard drives of old computers may be the only acceptable way to maintain confidentiality of client data stored on them. *See* Beckman & Hirsch, *Hard Drive Homicide*, ABA JOURNAL, August 2006, at 62 ("Old hard drives must rest in pieces for lawyers to truly rest in peace.")

another attorney that were inadvertently sent: (1) refrain from examining the materials; (2) notify counsel; and (3) abide by the instructions of the lawyer who sent them. Such an approach views confidentiality as a preeminent value to be protected, over and above the potential partisan advantage from disclosure.

Although an ABA opinion does not rise to the force of law, several courts cited it with approval. For example, in *Sampson Fire Sales Inc. v. Oakes*, 201 F.R.D. 351, 362 (M.D. Pa. 2001), the court stated in part: "[Opinion 92-368] heightens the level of civility and respect among lawyers, and establishes a professional courtesy which is compatible with vigorous advocacy and zealous representation. In this regard, information that is clearly identified as confidential in nature or appears on its face to be subject to the attorney-client privilege under circumstances that make it clear it was not intended for the receiving lawyer, should not be examined. The receiving lawyer should immediately notify the sending lawyer and abide by his instructions with respect to inadvertently disclosed privileged material."

Likewise, in *Resolution Trust Corp. v. First of America Bank*, [3]the court also noted: "While lawyers have an obligation to vigorously advocate the positions of their clients, this does not include the obligation to take advantage of a clerical mistake in opposing counsel's office where something so important as the attorney-client privilege is involved." The Association of the Bar of the City of New York Committee on Professional and Judicial Ethics recently issued Opinion 2003-04 (April 9, 2004) (2004 WL 837937). This opinion also follows the approach of ABA Opinion 92-368 in dealing with inadvertent disclosures.

However, other authorities have taken a different approach, which is more akin to that of Rule 4.4(b). These jurisdictions allow the recipient to review and use information in inadvertently disclosed documents, [4] (rejecting any duty to avoid using documents inadvertently disclosed by counsel, though they leave the evidentiary impact for judicial determination. One justification offered for rejecting the ABA approach involves the requirement to return documents unread, which some see as unworkable and potentially harmful to the client. To some extent, the profligate use of "privileged" stamps may be to blame, as one court noted: "Labels such as 'Attorney Client Privilege' and 'Attorney Work Product' are overused on documents that do not truly qualify for protection. To impose an obligation on opposing counsel to notify an adversary of every document that is produced during discovery with such a label is overkill. It would provide an incentive for commonplace use of these types of labels and would be a wholly inefficient method to monitor document production." (Employer's Reinsurance Corp. v. Clarendon Nat. Ins. Co., 213 F.R.D. 422, 430 (D.Kan. 2003)).

A requirement to leave a document unread also presents problems for objective monitoring. Without the ability to detect a breach, only the most conscientious would obey the rule while the scoundrel would not. Following the promulgation of Rule 4.4(b), the ABA ultimately withdrew Opinion 92-368, noting that its approach now conflicted with that of the Rule. (ABA Formal Opinion 05-437). However, only a decade before, the ABA had touted this outcome as the product of carefully weighing the values of confidentiality and civility against the deterrent effects on future errors of granting an advantage to the recipient's client:

> Our decision [in 92-368] was influenced by the values served by principles of confidentiality and the attorney-client privilege; analogous principles governing the inadvertent waiver of the attorney-client privilege; the law governing bailment and missent property; and general considerations of common sense, reciprocity and professional courtesy. Although we considered other competing principles--including the possible deterrent effect that allowing use of such materials might have on similar future errors, and the receiving lawyer's obligation zealously to represent the interests of her client--we concluded that these considerations were not dispositive and did not justify a rule that would allow the receiving lawyer to take advantage of such inadvertent disclosures of privileged and/or confidential materials." (ABA Formal Opinion 94-382)

This shift within the ABA appears to move the profession toward a more competitive model for professional behavior, as opposed to a more cooperative one. Whereas the treatment of inadvertently disclosed documents under the approach of Opinion 92-368 would be resolved primarily in the law offices of the attorneys, the Rule 4.4(b) approach will tend to move these disputes to the courts in the form of evidentiary rulings. Instead of a strong ethical presumption favoring return of an inadvertently produced document, the current rule allows retention of that document, with a shift in the status quo likely determined through a judicial

[3] 868 F.Supp. 217, 220 (W.D.Mich. 1994),

[4] (See, e.g., Colorado Bar Ethics Opinion 108 (May 20, 2000); Lifewise Master Funding v. Telebank, 206 F.R.D. 298, 302 n.2 (D. Utah 2002); State Bar Association of North Dakota Ethics Committee Opinion 95-14 (December 4, 1995)

determination. Clients, rather than lawyers, may also be involved in the decision to return a document, to the extent that it involves the ceding of a potential litigation advantage.

Despite the fact that professional discretion may still be recognized under the rule, will an attorney be willing to exercise it against the interest of a client, particularly if the threat of a malpractice action looms in the background where a client's advantage was conceded without consultation?

The most expedient way to avoid concerns about breaching professional obligations to a client (as well as possible malpractice claims) will be to let courts make the determination as to whether the disputed item is subject to a claim of privilege or not. However, to the extent that determination is subject to multi-factor balancing test, rather than a bright-line rule, these issues likely to involve additional litigation costs for clients. Such costs would otherwise be avoided in a regime where such documents were returned as a matter of duty, or where a clearer rule dictates a more determinate legal outcome.

5. Searching for a Proper Paradigm for Metadata

Few authorities have addressed the specific problem of metadata disclosure. Technological means are available to "scrub" or remove metadata from documents, and knowledge of that ability is beginning to permeate the legal and business communities. (National Security Agency, 2006; Adobe Systems, 2006) However, it is also likely that metadata will be inadvertently disclosed; human error is pervasive and a remarkably reliable phenomenon. Moreover, as the volume of documents has increased, it is increasingly impractical to monitor metadata aspects of all documents. (Paul & Nearon, 2006). As in the case of inadvertent disclosure generally, the emerging framework for ethical duties in this particular environment is incomplete, leaving considerable uncertainty in most jurisdictions as to the appropriate response to documents containing metadata. In particular, there are two considerations: (1) the duties of the attorney receiving documents containing metadata, and (2) the duties of attorneys sending documents containing metadata. Uncertainty and variation among jurisdictions mean that attorneys in multi-jurisdictional litigation need to consider possibilities for differing results. A critique and proposed alternative approach, which combines the evidentiary privilege rules with ethical constraints, follows.

A. New York Approach

New York has taken a leading position in addressing the duties of the receiving attorney with regard to discovery of metadata. In Opinion 749 (December 14, 2001), the New York State Bar Association Committee on Professional Ethics addressed the duties of the receiving attorney with regard to discovering metadata. This opinion addressed two practices: (1) accessing metadata (including track changes in Word documents) that counsel for an opponent "has not intentionally made available to the lawyer"; and (2) secretly imbedding a "bug" in e-mail that will track its subsequent progress and comments made by subsequent recipients. Though planting spyware in e-mail is arguably quite different from reviewing metadata in a document, the opinion suggests that both are similarly unethical on the basis that they are in derogation of requirements on confidentiality. The opinion found these practices analogous to other prohibited activities, including:
(1) soliciting the disclosure of unauthorized communications, see, e.g., *Dubois v. Gradco Sys., Inc.*, 136 F.R.D. 341, 347 (D. Conn. 1991) (Cabranes, J.) (Although former employees of adverse corporate party are not within reach of the no-contact rule "it goes without saying that plaintiff's counsel must take care not to seek to induce or listen to disclosures by the former employees of any privileged attorney-client communications to which the employee was privy"); see also ABA Formal Op. 91-359; (2) exploiting the willingness of others to undermine the confidentiality principle, see N.Y. State 700 (1997); ABA Formal Op. 94- 382; and (3) making use of inadvertent disclosures of confidential communications, (see ABAFormal Op. 92-368.)

In these circumstances, the opinion viewed the use of technology to view metadata in a pejorative sense: "We believe that in light of the strong public policy in favor of preserving confidentiality as the foundation of the lawyer-client relationship, use of technology to surreptitiously obtain information that may be protected by the attorney-client privilege, the work product doctrine or that may otherwise constitute a 'secret' of another lawyer's client would violate the letter and spirit of these Disciplinary Rules." In this case, the mining of metadata was thought to be even more obviously unethical than an "inadvertent" disclosure: "In the 'inadvertent' and 'unauthorized' disclosure decisions, the public policy interest in encouraging more careful conduct had to be balanced against the public policy in favor of confidentiality. No such balance need be struck

here because it is a deliberate act by the receiving lawyer, not carelessness on the part of the sending lawyer, that would lead to the disclosure of client confidences and secrets."

However, this view presupposes that a requirement of zealous representation is not violated by the failure to examine metadata: "Prohibiting the intentional use of computer technology to surreptitiously obtain privileged or otherwise confidential information is entirely consistent with these ethical restraints on uncontrolled advocacy." It should be noted that such a view is consistent with that accorded to the use of electronic eavesdropping methods. However, such eavesdropping is a matter proscribed by the Electronic Communications Privacy Act. (Mangrum, § 27-503, 2006). No such proscriptions apply to metadata mining.

In December 2004, this committee issued Opinion 782, which reiterated support for Opinion 749 despite the effective abrogation of ABA Opinion 92-368 by the enactment of Rule 4.4(b). However, it also recognized that there was a duty of care on the part of the sending attorney, which should be exercised along with the care of the receiving attorney not to use computer technology to access secrets in metadata. In particular, "Lawyers 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."

B. Florida's Proposed Approach

Florida has adopted Model Rule 4.4(b) as part of its professional code. Nevertheless, Florida has adopted a restrictive approach toward metadata similar to that of New York. Florida issued a proposed ethics opinion dated June 23, 2006, which imposes an obligation on the sending lawyer to "take reasonable steps to safeguard the confidentiality of all communications sent by electronic means." On the other hand, the receiving lawyer is effectively enjoined from "try[ing] to obtain metadata information relating to the representation of the sender's client that the recipient knows or should know is not intended for the recipient." Further, "if the recipient lawyer inadvertently obtains information from metadata that the recipient knows or should know was not intended for the recipient, the lawyer must 'promptly notify the sender.'"

This proposal takes a dim view of efforts to access metadata. (The Board of Governors was unanimous in deploring the concept of metadata mining. As one member stated: "I have no doubt that anyone who receives a document and mines it . . . is unethical, unprofessional, and un-everything else," said board member Jake Schickel. *What's in Your Document*, FLORIDA BAR NEWS, January 1, 2006).

However, it qualifies the constraint on access by restricting it to information which the "recipient knows or should know is not intended for the recipient." An important question unanswered in this proposal is how one can know that the metadata is not intended for the recipient, particularly before one has knowledge of its contents. One approach to this knowledge problem might involve categorization of documents. For example, a settlement letter proffered to another litigant may contain metadata, but it is unlikely to be something that the sending party wanted the other to access. Alternatively, this issue might be clarified through agreements in pretrial discovery conferences. A presumption against metadata mining, which could be abrogated only by an express agreement or by judicial order if doubt as to the validity or provenance of a document is raised, could also be adopted. Either approach could remove some incentives to mine metadata on behalf of the receiving party. This, in turn, may reduce litigation costs associated with preventive monitoring of metadata, as well as in preventive steps taken in advance of the release of documents with metadata.

However, an ethical duty not to access metadata is ultimately difficult to monitor. Adopting an ethical rule that proscribes mining conduct does not ensure that this conduct will not otherwise be undertaken if the receiving lawyer finds it to the advantage of the client, particularly when there is no effective mechanism for discovering a breach of that ethical duty. Short of proffering the metadata as evidence, there may be no way to discover that metadata was mined by the recipient in violation of such a duty.

C. A Duty to Preserve Metadata?

In addition to the approaches that restrict access to metadata, discussed above, there have also been authorities in other jurisdictions that raise still another possibility: a requirement to preserve the metadata in documents that are not subject to claims of privilege. In *Williams v. Sprint/United Management Co*., 230 F.R.D. 640 (D. Kan. 2005), the defendant received a discovery request for electronic records that included Excel spreadsheets. Not only did it review for privilege, but it also produced TIFF (tagged image file format – a graphic file format) files instead of an interactive spreadsheet. The defendant was order to show cause why the business records "as maintained in the ordinary course of business" were not produced. As the court concluded:

"[W]hen a party is ordered to produce electronic documents as they are maintained in the ordinary course of business, the producing party should produce the electronic documents with their metadata intact, unless that party timely objects to production of metadata, the parties agree that metadata should not be produced, or the producing party requests a protective order. The initial burden with regard to the disclosure of the metadata would therefore be placed on the party to whom the request or order to produce is directed." (footnotes omitted).

Cases such as *Williams* illustrate the kind of issues that must be addressed in pretrial conferences regarding discovery issues. It should be noted that a failure to protect metadata could, in proper circumstances, result in sanctions against the attorney and/or the client, such as through the form of an evidentiary presumption against the party destroying the evidence. (Koesel & Turnbull, 2006). Although an extended discussion of this duty is beyond the scope of this article, it should be noted that context is highly important in evaluating duties regarding metadata preservation and disclosure.

6. Critique of Existing Frameworks

The paradigms for evidentiary and ethical rules involving inadvertent disclosure appear useful in analyzing metadata problems. However, those rules appear to have developed in isolation, rather than through a coordinated effort. Understanding the incentive structures for behavior in this context is an important dimension of evaluating the protection that both of these systems of legal authority are attempting to build upon. First, ethical rules notify the sending lawyer of responsibilities ensure that potentially harmful metadata is not disclosed. These duties may not be clearly stated in all jurisdictions, but commonly understood principles of confidentiality would appear to provide a solid basis for this position. Some attorneys are not aware of these risks, however, as we are in a transition period concerning the proper scope of duties assumed in this context. Competent representation arguably requires some precautionary measures to address known metadata issues where disclosure might compromise a client's legal position. This duty exists apart from the impact of the potential loss of an evidentiary privilege; once disclosed, this information cannot be unlearned. These rules thus already provide incentives to protective behavior, even if the item disclosed is ultimately not admitted into evidence. It is doubtful whether the evidentiary threat of a waiver of privilege would provide any additional client protection in these cases. Imposing a "penalty" for failure to take adequate steps to protect data is unlikely to induce additional protective behavior from attorneys that was not previously undertaken. Instead, adopting a clear and lenient rule on privilege, which gives maximum protection to clients from inadvertent disclosure by their attorneys, arguably provides the most appropriate outcome in the evidentiary context.

A lenient waiver rule would be preferable to the more costly balancing approach, which considers multiple facts and circumstances, including protective actions taken in discovery. It would also foster greater predictability in the treatment of putative waivers. With a clear rule, disputes over metadata discovered by opposing counsel would be less likely to become matters for judicial determinations, and more likely resolved within the framework of professional behavior. This would reduce attorney and other transactions costs for clients, which might otherwise be incurred. Attorneys receiving potentially privileged metadata would not feel the same pressure to let a court decide if the decision rule would be much clearer in favor of retaining the privilege as opposed to waiving it. As for the reciprocal duty of a receiving attorney to mine or not to mine metadata, the theoretical possibility of constraint associated with a rule such as that envisioned in Florida or New York may indeed reduce costs by giving a basis for refusing to engage in metadata mining as a matter of course. However, unless all jurisdictions adopt such a rule, there remains the possibility of simply changing counsel to those in another jurisdiction that is more lenient. tend to create a disincentive for at least some metadata mining, but an incentive for mining may nevertheless exist to the extent that a party believes that mining could lead to other useful information. The efficacy of an ethical rule prohibiting metadata mining is questionable from the perspective of enforcement, as a breach is hard to detect (apart from an attempt to admit evidence), and thus hard to sanction effectively.

Allowing freedom with regard to metadata mining would thus provide a system of ethical practices that could be administered more consistently, and remove inter-jurisdictional competition on this basis. Such an approach arguably embraces a more competitive environment among practitioners, and greater costs for litigants. However, private ordering may provide some solutions here apart from the proscription of rules. Advance agreements to address those issues with opposing counsel on a case-by-case basis would, in effect, allow the advance consideration of potential costs and benefits to clients before incurring additional costs from metadata mining. Emerging practices for electronic discovery under Rule 26(f), which include pretrial

agreements on such matters, seem to reflect an expanding role for private ordering in these matters. (Paul & Nearon, 2006); (Nelson & Simek, 2006).

Bibliography

1. Administrative Office of the U.S. Courts, *Preliminary Draft of Proposed Amendments to the Federal Rules of Practice and Procedure, A Summary for Bench and Bar* (August 2006).
2. Adobe Systems, Inc., *Redaction of Confidential Information in Electronic Documents* (2006),available online at partners.adobe.com/public/developer/en/acrobat/Redaction.pdf.
3. Beckman & Hirsch, *Hard Drive Homicide*, ABA JOURNAL, August 2006, at 62.
4. Hundley, John T., Annotation, *Waiver of Evidentiary Privilege by Inadvertent Disclosure--State Law*, 51 A.L.R.5th 603 (1997); *"Inadvertent Waiver" of Evidentiary Privileges: Can*
5. *Reformulating the Issue Lead to More Sensible Decisions?*, 19 S. ILL.U. L.J. 263 (1995).
6. Koesel, Margaret M. & Turnbull, Tracey L., SPOILATION OF EVIDENCE: SANCTIONS AND REMEDIES FOR DESTRUCTION OF EVIDENCE IN CIVIL LITIGATION (ABA 2d ed. 2006).
7. Lange, Michele C.S. & Nimsger, Kristin M., ELECTRONIC EVIDENCE AND DISCOVERY: WHAT EVERY LAWYER SHOULD KNOW 247 (ABA 2004).
8. Microsoft Office Online, *Find and Remove Metadata (Hidden Information) in Your Legal Documents*, *at* http://offi ce.microsoft.com/en-us/assistance/HA010776461033.aspx.
9. Mangrum, R. Collin, MANGRUM ON NEBRASKA EVIDENCE (Thomson/West 2006) National Security Agency, Information Assurance Directorate,
10. *Redacting with Confidence: How to Safely Publish Sanitized Reports Converted from Word toPDF* (2/2/06), *available at* http://www.nsa.gov/snac/vtechrep/I333-TR-015R-2005.PDF.
11. National Information Standards Organization, *Understanding Metadata* (2004), *available online* at http://www.niso.org/standards/resources/UnderstandingMetadata.pdf .
12. Nelson, Sharon D., & Simek, John W., *A Legal Lifeline: Protecting Your Data in Electronic Discovery*, in INFORMATION SECURITY FOR LAWYERS AND LAW FIRMS (ABA 2006)
13. Paul, George L. & Nearon, Bruce H., THE DISCOVERY REVOLUTION (ABA 2006).
14. The Sedona Conference, The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age (Charles R. Ragan *et al. eds*., Sept. 2005), *available at* http://www.thesedonaconference. org/dltForm?did=TSG9_05.pdf.
15. *What's in Your Document*, FLORIDA BAR NEWS, January 1, 2006, *available at* http://www. floridabar.org/DIVCOM/JN/jnnews01.nsf/0/ c3f75b4e10e94f78852570e50051b23e?OpenDocument.
16. Walker, Jessica M., *What's a Little Metadata Mining Among Friends?*, DAILY BUSINESSREVIEW, April 21, 2006, *available at* http://www.law.com/jsp/legaltechnology/ pubArticleLTN.jsp?id=1145538533635.
17. www.payneconsulting.com
18. WIKIPEDIA, *Metadata, at* http://en.wikipedia.org/wiki/Metadata.
19. Zeller, Tom Jr., *Beware Your Trail of Digital Fingerprints*, NEW YORK TIMES, November 7,2005.