

E-Discovery Ethics: An Ounce of Prevention...

Written by David Ries

Presenters:
Hon. Herbert Dixon, Jr.
Ralph Losey
David Ries

April 2-4, 2009
www.techshow.com

CONTENTS

I. INTRODUCTION 3

II. ETHICS RULES AND COURT RULES 3

 A. Ethics Rules 3

 B. Court Rules 9

 C. Cooperation in Discovery 9

III. PROTECTION OF PRIVILEGE 12

 A. Elements 12

 B. Corporations 12

 C. Work Product 13

 D. Waiver by Intentional Production 13

 E. Inadvertent Disclosure 13

 F. Response by Recipient of Inadvertent Disclosure 13

 G. State Privilege Law 14

 H. Privilege and Electronic Data – New Rule 502 14

IV. PRESERVATION AND SPOILIATION 17

 A. Definitions and the Duty to Preserve 17

 B. Spoliation and Sanctions 24

V. METADATA 29

VI. CONCLUSION 31

VII. ADDITIONAL INFORMATION SOURCES 32

I. INTRODUCTION

The growth in electronic discovery in recent years has been explosive. It is becoming more and more common for the evidence in today's cases – both routine and “smoking guns” – to be digital. This explosion in e-discovery has followed naturally from the exponential growth in digital data in government, businesses, and organizations. Computers and electronic communications are the way business is done today and the evidence of what occurs is largely digital. Court opinions on e-discovery issues are being published frequently, including high profile cases on issues like preservation and spoliation, cost shifting, and form of production. The new federal rules covering “electronically stored information” took effect in December of 2006. These amended rules and e-discovery generally raise ethics issues including competence, communication with clients, confidentiality, fairness to opponents, and candor to tribunals. They also raise additional professional responsibility considerations including protection of privilege and avoiding malpractice risks. This paper presents an overview of these professional responsibility considerations.

II. ETHICS RULES AND COURT RULES



Numerous ethical considerations apply to attorneys who are involved in electronic discovery. This section explores the key rules in the American Bar Association Model Rules of Professional Conduct which apply in this area and an overview of the involved court rules.¹ It is important for attorneys to consult the applicable ethics rules and court rules from the involved jurisdiction or jurisdictions.²

A. Ethics Rules

The first ethical consideration that applies to e-discovery is the duty of competence. ABA Model Rule 1.1, Competence, provides:

A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill,

¹ The current edition of Model Rules is the 2008 edition. The Model Rules are amended periodically and it takes time after amendment for the various states to consider them and either adopt or reject amendments. Copies of the current ABA Model Rules, with comments, are posted on the ABA website (listed at the end of these materials) and print copies are available from the ABA Service Center, 750 North Lake Shore Drive, Chicago, IL 60611-4497, 1-800-285-2221.

² Forty-eight states (all except California and Maine) have adopted ethics rules based on the ABA Model Rules. There are, however, numerous variations from the Model Rules. Ethics rules in the various states may differ in both subtle and significant ways.

thoroughness and preparation reasonably necessary for the representation.

Competence requires that litigators and other attorneys who may face records preservation and e-discovery matters must understand at least the basic legal and technical issues and know where to go for assistance with issues beyond their own level of competence.

Another duty which applies in this area is communication, covered by Rule 1.4, which provides:

(a) A lawyer shall:

(1) promptly inform the client of any decision or circumstance with respect to which the client's informed consent, as defined in Rule 1.0(e), is required by these Rules;

(2) reasonably consult with the client about the means by which the client's objectives are to be accomplished;

(3) keep the client reasonably informed about the status of the matter;

(4) promptly comply with reasonable requests for information; and

(5) consult with the client about any relevant limitation on the lawyer's conduct when the lawyer knows that the client expects assistance not permitted by the Rules of Professional Conduct or other law.

There are multiple areas in which attorneys need to communicate with clients about electronic data, including such areas as preservation obligations, options for collection, processing and production, and services available from consultants.

The duty of confidentiality is arguably one of an attorney's most important ethical responsibilities. ABA Model Rule 1.6 generally defines the duty of confidentiality. It begins as follows:

Rule 1.6: CONFIDENTIALITY OF INFORMATION

(a) 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 permitted by paragraph (b). . . .

Recent amendments to Model Rule 1.6., part of the Ethics 2000 revisions, added new Comment 15 (now Comment 16) to the rule. This comment requires reasonable precautions to safeguard and preserve confidential information:

Acting Competently to Preserve Confidentiality

[16] A lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1 and 5.3.

Rules 1.1 and 1.6 and this comment make it clear that attorneys must act competently and reasonably to safeguard client information which is processed and stored in information systems. The State Bar of Arizona recently issued an ethics opinion applying these rules to information security requirements. It responds to an inquiry about the steps a law firm must take to safeguard client data from hackers and viruses. It concludes:

ER's 1.6 and 1.1 require that an attorney act competently to safeguard client information and confidences. It is not unethical to store such electronic information on computer systems whether or not those same systems are used to connect to the internet. However, **to comply with these ethical rules as they relate to the client's electronic files or communications, an attorney or law firm is obligated to take competent and reasonable steps to assure that the client's confidences are not disclosed to third parties through theft or inadvertence.** In addition, an attorney or law firm is obligated to take reasonable and competent steps to assure that the client's electronic information is not lost or destroyed. In order to do that, an attorney must either have the competence to evaluate the nature of the potential threat to the client's electronic files and to evaluate and deploy appropriate computer hardware and software to accomplish that end, or if the attorney lacks or cannot reasonably obtain that competence, to retain an expert consultant who does have such competence. (Emphasis added.)

State Bar of Arizona, Opinion No. 05-04 (July 2005) (Formal Opinion of the Committee on the Rules of Professional Conduct, "advisory in nature").

Next, lawyers should provide diligent and zealous representation to their clients, including assertive and even appropriately aggressive efforts when warranted. Such representation must, however, be within proper limits, including applicable ethics rules and court rules. Rule 1.3 provides that “[a] lawyer shall act with reasonable diligence and promptness in representing a client.” The Comment to this rule notes that “[a] lawyer must also act... with zeal in advocacy in a client’s behalf.” The Preamble to the Model Rules states “[a]s an advocate, a lawyer zealously asserts the client’s position under the rules of the adversary system.” Canon 7 of the Model Code of Professional Responsibility, which predated the Model Rules, provides:

**A Lawyer Should Represent a Client Zealously Within
the Bounds of the Law.**

The key consideration in approaching records preservation and discovery is that diligent and zealous representation has limits, described in the ethics rules as “the rules of the adversary system” and “the bounds of the law.”

Under the Model Rules, attorneys have ethical obligations to cooperate in discovery and to preserve and produce, when required, documents and other evidence. Another important ethics rule which applies to document preservation and discovery is Rule 3.4:

Rule 3.4 Fairness To Opposing Party And Counsel

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;**

- (b) falsify evidence, counsel or assist a witness to testify falsely, or offer an inducement to a witness that is prohibited by law;**

- (c) knowingly disobey an obligation under the rules of a tribunal except for an open refusal based on an assertion that no valid obligation exists;**

- (d) in pretrial procedure, make a frivolous discovery request or fail to make reasonably diligent effort to comply with a legally proper discovery request by an opposing party; ...**

This rule establishes an ethical obligation of fairness to opposing parties and counsel, which includes compliance with discovery rules. It expressly prohibits obstruction of access, alteration or concealment of evidence and “other material having potentially evidentiary value.”

The following Model Rules also apply in the area of document preservation and discovery:

Rule 3.2 Expediting Litigation

A lawyer shall make reasonable efforts to expedite litigation consistent with the interests of the client.

Rule 3.3 Candor Toward The Tribunal

* * *

(b) A lawyer who represents a client in an adjudicative proceeding and who knows that a person intends to engage, is engaging or has engaged in criminal or fraudulent conduct related to the proceeding shall take reasonable remedial measures, including, if necessary, disclosure to the tribunal.

(c) The duties ... continue to the conclusion of the proceeding, and apply even if compliance requires disclosure of information otherwise protected by Rule 1.6. ...

Rule 4.4 Respect for the Rights of Third Parties

(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.

Other ethics rules which are likely to apply to e-discovery include: Rule 5.1, Responsibilities of Partners, Managers and Supervisory Lawyers, Model Rule 5.2 Responsibilities of Subordinate Lawyers, and Model Rule 5.3, Responsibilities Regarding Nonlawyer Assistants.

E-Discovery will often involve use of service providers and outsourcing. Several ethical considerations apply in this area. Attorneys must protect confidential information to which third parties, like information systems consultants and litigation support service providers, are given

access. Attorneys must take reasonable precautions to protect information to which such third parties may have access. Formal Opinion 95-398 of the ABA Standing Committee on Ethics and Professional Responsibility, "Access of Nonlawyers to a Lawyer's Database," provides guidance in this area and concludes, "[a] lawyer who gives a computer maintenance company access to information in client files must make reasonable efforts to ensure that the company has in place, or will establish, reasonable procedures to protect the confidentiality of the client information."

This analysis has been applied to information technology outsourcing which involves confidential information. For example, the State Bar of Nevada Standing Committee on Ethics and Professional Responsibility has issued Formal Opinion No. 33 (February 9, 2006) (an advisory opinion), in which it concluded that a lawyer may store confidential information electronically with a third party to the same extent and subject to the same standards as storing confidential paper in a third party warehouse. In doing so, the lawyer must act "competently and reasonably to ensure the confidentiality of the information."

The ABA Standing Committee on Ethics and Professional Responsibility recently issued Formal Opinion 08-451 "Lawyer's Obligations When Outsourcing Legal and Nonlegal Support Services" (August 5, 2008). The headnote to the opinion states:

A lawyer may outsource legal or nonlegal support services provided the lawyer remains ultimately responsible for rendering competent legal services to the client under Model Rule 1.1. In complying with her Rule 1.1 obligations, a lawyer who engages lawyers or nonlawyers to provide outsourced legal or nonlegal services is required to comply with Rules 5.1 and 5.3. She should make reasonable efforts to ensure that the conduct of the lawyers or nonlawyers to whom tasks are outsourced is compatible

with her own professional obligations as a lawyer with "direct supervisory authority" over them.

In addition, appropriate disclosures should be made to the client

regarding the use of lawyers or nonlawyers outside of the lawyer's firm, and client consent should be obtained if those lawyers or nonlawyers will be receiving information protected by Rule 1.6. The fees charged must be reasonable and otherwise in compliance with Rule 1.5, and the outsourcing lawyer must avoid assisting the unauthorized practice of law under Rule 5.5.1

B. Court Rules

Discovery obligations are defined in Rules 26 and following of the Federal Rules of Civil Procedure and in their state counterparts. As noted above, failure to comply with a discovery rule may constitute a violation of Model Rule 3.4. In addition, the discovery rules provide for sanctions for violations.

Rule 26(g) of the Federal Rules of Civil Procedure requires an attorney (or party) to sign disclosures, discovery requests, responses and objections. The signature constitutes a certification “after a reasonable inquiry” of compliance with the discovery rules. The rule also provides for sanctions for certifications made in violation of the rule.

Rule 37 of the Federal Rules provides for sanctions for evasive or incomplete disclosures or responses and for violation of discovery orders, ranging from awarding of expenses to a default or dismissal. In addition, courts have inherent powers to regulate attorneys and parties before them, including the imposition of sanctions. Courts also have inherent powers to punish litigation misconduct.

C. Cooperation in Discovery

E-discovery requires a new level of cooperation between opposing parties. This dictates an appropriate balancing of attorneys’ duty to their clients of zealous advocacy and their duty to courts and adversaries to reasonably cooperate in discovery. The recent opinion in *Board of Regents of the Univ. of Nebraska v. BASF Corp.*, 2007 WL 3342423 (D. Neb. Nov. 5, 2007) notes:

[t]he overriding theme of recent amendments to the discovery rules has been open and forthright sharing of information by all parties to a case with the aim of expediting case progress, minimizing burden and expense, and removing contentiousness as much as practicable. . . . If counsel fail in this responsibility - willfully or not – these principles of an open discovery process are undermined, coextensively inhibiting the court’s ability to objectively resolve their clients’ disputes and the credibility of its resolution.

(citations omitted.)

The Sedona Conference recently published *The Sedona Conference Cooperation Proclamation* (July 2008) to launch “a national drive . . . to facilitate cooperative, collaborative, transparent discovery.” It calls for “open and forthright sharing of information by all parties” and makes a distinction between appropriate *advocacy* and inappropriate *adversarial conduct*. It was reported in September 2008 that more than 20 judges had endorse the *Proclamation*.

The court cited the *Proclamation* in a thorough discovery opinion in *Mancia v. Mayflower Textile Servs. Co.*, 253 F.R.D. 354 (2008), an employment case in which the plaintiff sought to compel supplemental responses to its extensive discovery requests. The court found violations or apparent violations of several discovery rules by both parties, including Fed. R. Civ. P. 26(g), 33(b)(3) and 33(b)(4). It cited the Advisory Committee's notes as follows:

Rule 26(g) imposes an affirmative duty to engage in pretrial discovery in a *responsible manner* that is consistent with the *spirit and purposes* of Rules 26 through 37. In addition, Rule 26(g) is *designed to curb discovery abuse* by explicitly encouraging the imposition of sanctions.

The court noted that “[t]he failure to engage in discovery as required by Rule 26(g) is one reason why the cost of discovery is so widely criticized as being excessive—to the point of pricing litigants out of court.” It cited the *Proclamation* and other authorities and stated that “there is nothing inherent in [the adversary system] that precludes cooperation between the parties and their attorneys...to achieve orderly and cost effective discovery of the competing facts on which the system depends.”

The court directed counsel to read the *Proclamation* in *Gipson v. Southwestern Bell Telephone Co.*, 2008 U.S. Dist. LEXIS 103822 (D. Kan. Dec. 23, 2008). The case is a purported class action under the Fair Labor Standards Act in which there were more than 115 motions and 462 docket entries in less than a year. The order provided, “[t]o help the parties and counsel understand their discovery obligations, counsel are directed to read the Sedona Conference Cooperation Proclamation, which this Court has previously endorsed.”

This chart lists “5 Cs of E-Discovery.” While it does not cover all of the professional responsibility requirements in e-discovery, the “5 Cs of E-Discovery” summarizes the key areas:

The 5 Cs of E-Discovery

- **C**ompetence
- **C**onfidentiality
- **C**ommunication
- **C**andor
- **C**ooperation



E-Discovery



III. PROTECTION OF PRIVILEGE

Protection of attorney-client privilege and work product is one of the paramount considerations in e-discovery.

A. Elements

While the elements of attorney-client privilege are stated somewhat differently in different jurisdictions, the following elements are generally included:

- (1) a communication,
- (2) made between privileged and persons,
- (3) in confidence,
- (4) for the purpose of seeking, obtaining or providing legal assistance to the client,
- (5) affirmatively asserted and not waived.³

B. Corporations

The U.S. Supreme Court in *Upjohn Co. v. United States*, 449 U.S. 383 (1981) held that the attorney-client privilege applies broadly to corporations based on a subject matter test and is not limited to those in the corporation's control group. Under *Upjohn*, corporate communications are privileged if:

- (1) made by corporate employees,
- (2) to counsel for the company, acting as counsel, at the direction of corporate superiors,
- (3) concern matters within the scope of the employee's duties,
- (4) to secure legal advice, and
- (5) considered confidential and so maintained.

Id. at 394-395.

Covered communications to the attorney generally have broad protection. Depending on the jurisdiction, communications from the attorney to the client may be broadly protected or may not be protected if they do not disclose confidences received from the client.

³ E. Epstein, *The Attorney-Client Privilege and the Work Product Doctrine*, 5th ed. (American Bar Association 2007).

C. Work Product

Work product is a qualified protection, codified in Rule 26(b)(3) of the Federal Rules of Civil Procedure, which protects from discovery in civil cases:

- (1) documents and tangible things,
- (2) prepared in anticipation of litigation or for trial,
- (3) by or for another party or by or for that other party's representative (including the other party's attorney or consultant...).

Work product protection applies in a litigation context only and does not generally apply to legal services outside of disputes or litigation. It also generally terminates when the litigation ends. It is qualified because it can be overcome by a showing of substantial need for the information and inability to obtain it without undue hardship. Work product protection in criminal cases is provided by Rule 16 of the Federal Rules of Criminal Procedure.

D. Waiver by Intentional Production

While some courts have recognized a selective waiver of privilege by production of information to a government agency, there is a substantial risk that production to the government, even under a confidentiality agreement, will be a general waiver of privilege. *Compare, In re Columbia/HCA Healthcare Corp. Billing Practices Lit.*, 293 F.3d 289 (6th Cir. 2002) (disclosure of privileged information to the government waives privilege as to all other parties; agreeing with the First, Third, Fourth and D.C. Circuits) with *Diversified Industries v. Meredith*, 572 F.2d 596 (8th Cir. 1978) (en banc) (voluntary compliance with a government subpoena does not waive privilege in subsequent litigation). New Federal Rule 502, discussed below, generally provides protection from subject matter waiver.

E. Inadvertent Disclosure

Courts have taken varied approaches to the effect that inadvertent disclosure will have on privilege, ranging from strict waiver from inadvertent disclosure, to an intermediate approach (weighing several factors), to no waiver absent client consent.⁴ New Federal Rule of Evidence 502, which is discussed below, adopts the intermediate approach for federal courts.

F. Response by Recipient of Inadvertent Disclosure

ABA Formal Opinion 92-368 (1992), *Inadvertent Disclosure of Confidential Materials*, (withdrawn 2005), reaches the conclusion that:

A lawyer who receives materials that on their face appear to be subject to the attorney-client privilege or otherwise confidential, under circumstances where it is clear that they were not intended for the

⁴ *In re Columbia/HCA Healthcare Corp. Billing Practices Lit.*, 293 F.3d 289, 309-314 (6th Cir. 2002).

receiving lawyer, should refrain from examining the materials, notify the sending lawyer and abide the instructions of the lawyer who sent them

A recent amendment to Rule 4.4 of the ABA Model Rules of Professional Conduct accepts only part of this opinion and provides:

(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.

This amendment to the Model Rules will take effect in the various states only if they adopt it.

The December 2006 amendments to the Federal Rules of Civil Procedure include requirements for recipients of inadvertently produced information. The producing party may notify the party who received the information that it is privileged or protected as trial preparation material. “After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has; must not use or disclose the information until the claim is resolved; must take reasonable steps to retrieve the information...and may promptly present the information to the court under seal for a determination of the claim. Fed. R. Civ. 26(b)(5)(b). While the amendment was part of the e-discovery amendments, it applies to all production.

In federal cases, the requirements are now similar to those under the withdrawn 1992 ABA ethics opinion. Under ABA Model Rule 4.4(b), the receiving party must notify the producing party of the inadvertent production. Rule 26(b)(5)(B) requires the receiving party, if notified by the producing party, to refrain from using and to protect the involved information unless the court rules otherwise.

G. State Privilege Law

This discussion of attorney-client privilege and work product is generally based on federal law. It is critical to consult state statutes, rules and court decisions on privilege where state law governs.

H. Privilege and Electronic Data – New Rule 502

Electronically stored information presents a substantial risk of waiver of attorney-client privilege and work product because of its volume, wide distribution, and often unstructured content. It is often very difficult and expensive to locate and review potentially privileged data which may be distributed among thousands or hundreds of thousands of records, or even more. One approach in addressing this challenge has been nonwaiver agreements or “claw back” agreements, which provide that there will be no waiver in the event of inadvertent production.

These agreements are sometimes included in protective orders. This approach is recognized procedurally in the new amendments to the Federal Rules. However, there are questions concerning the scope of protection provided by these kinds of agreements and orders, and the nature of review which still needs to be performed before production. For a thorough discussion of these issues, see, *Hopson v. Mayor & City Council of Baltimore*, 232 F.R.D. 228 (D. Md. 2005) (concluding that a court order provides the best protection).

Keyword searches are sometimes used to locate potentially privileged electronic records, which are then individually reviewed for privilege. Where this approach is used, it should be carefully planned, should be tested, and should be approved in a court order. In *Victor Stanley, Inc. v. Creative Pipe, Inc.*, 250 F.R.D. 251 (D. Md. 2008), the court found a waiver of privilege by the inadvertent production of 165 electronic records where the producing party did not establish the reliability of its keyword screening and did not test its accuracy by sampling. The court cited *Equity Analytics, LLC v. Lundin*, 248 F.R.D. 331 (D.D.C. 2008), which found that search methodologies, such as keywords, can require “knowledge beyond the ken of a lay person (and a lay lawyer)” and require expert testimony.

There is a new Federal Rule of Evidence, Rule 502, that covers waiver of attorney-client privilege and work product. It became effective in September 2008. Its provisions include:

- Part (a) of Rule 502 provides that waivers in federal proceedings generally extend only to the materials disclosed and not to the subject matter. It extends to the subject matter only if the waiver is intentional and fairness requires a broader waiver.

- Part (b) of Rule 502 provides:

(b) Inadvertent disclosure.—When made in a federal proceeding or to a federal office or agency, the disclosure does not operate as a waiver in a federal or state proceeding if:

- (1)** the disclosure is inadvertent;

- (2)** the holder of the privilege or protection took reasonable steps to prevent disclosure; and

- (3)** the holder promptly took reasonable steps to rectify the error, including (if applicable) following Fed. R. Civ. P. 26(b)(5)(B).

- The rule provides that nonwaiver orders are binding on parties and nonparties, part (d), and that nonwaiver agreements are binding only on the parties, part (e).

-The rule also covers the effect in federal proceedings of potential waivers in state courts, part (c), and its effect in state proceedings and arbitrations, part (f).

- The Explanatory Note on Evidence Rule 502, prepared by the Judicial Conference Advisory Committee on Evidence Rules (Revised 11/28/2007), states, *inter alia*:

This new rule has two major purposes: 1) It resolves some longstanding disputes in the courts about the effect of certain disclosures of communications or information protected by the attorney-client privilege or as work product—specifically those disputes involving inadvertent disclosure and subject matter waiver. 2) It responds to the widespread complaint that litigation costs necessary to protect against waiver of attorney-client privilege or work product have become prohibitive due to the concern that any disclosure (however innocent or minimal) will operate as a subject matter waiver of all protected communications or information. This concern is especially troubling in cases involving electronic discovery. *See, e.g., Hopson v. City of Baltimore*, 232 F.R.D. 228, 244 (D. Md. 2005) (electronic discovery may encompass “millions of documents” and to insist upon “record-by-record pre-production privilege review, on pain of subject matter waiver, would impose upon parties costs of production that bear no proportionality to what is at stake in the litigation”).

The rule seeks to provide a predictable, uniform set of standards under which parties can determine the consequences of a disclosure of a communication or information covered by the attorney-client privilege or work-product protection. ...

A recent case that applied Rule 502 is *Rhoads Indus., Inc. v. Bldg. Materials Corp. of Am.*, 2008 WL 4916026 (E.D. Pa. Nov. 14, 2008). It is a breach of contract case in which the plaintiff inadvertently produced over 800 privileged electronic documents. The court applied the three factors set forth in Fed. R. Evid. 502(b) and found that the plaintiff’s “steps to prevent disclosure and to rectify the inadvertent production “were, to some extent, not reasonable.” The court, however, held that there was no waiver based on the interests of justice, a fourth factor established by prior case law. It noted that “[p]roper quality assurance testing is a factor considered in determining whether precautions taken to prevent inadvertent disclosure ... were reasonable.” The court also held that there was a waiver as to documents withheld from production, but not listed in a privilege log.

Another case that applied Rule 502 is *Alcon Mfg., Ltd. v. Apotex, Inc.*, 2008 U.S. Dist. Lexis 96630 (S.D. Ind. Nov. 26, 2008), a patent action in which an electronically stored document with attorney notes was inadvertently produced by plaintiffs. Defendants claimed that privilege was waived by the production and by plaintiffs' failure to immediately object when the document was used during two depositions. The plaintiffs claimed that the production was inadvertent, due to an electronic document break error during production. The court required return of the document under a protective order entered in the case and stated:

Perhaps the situation at hand could have been avoided had Plaintiffs' counsel meticulously double or triple-checked all disclosures against the privilege log prior to any disclosures. However, this type of expensive, painstaking review is precisely what new Evidence Rule 502 and the protective order in this case were designed to avoid.

There is still uncertainty about the degree of pre-production review that will be required to avoid a waiver. Attorneys should carefully review developing case law under Rule 502.

IV. PRESERVATION AND SPOILIATION

A. Definitions and the Duty to Preserve

Preservation of electronic evidence presents unique challenges because of the volume, distribution, and dynamic nature of electronic data. While it generally takes some action to discard or destroy paper records, electronically stored information can be lost through inaction. Routine operation of information systems containing the data can alter or destroy it and data is often automatically overwritten or deleted. It is critical to stop any automatic deletion or overwriting of data which must be preserved.

The e-discovery amendments to the Federal Rules of Civil Procedure require both courts and counsel to address electronically stored information early, including preservation issues. These rules do not address the issues of what must be preserved and when the duty to preserve arises. These aspects of preservation are defined by statutes, rules, and developing case law that both predate the new rules and continue under them.

Communications with clients about the duty to preserve is crucial. As the court explained it in *Zubulake*:

Lawyers and their clients need to communicate clearly and effectively with one another to ensure that litigation proceeds efficiently. When

communication between counsel and client breaks down, conversation becomes "just crossfire," and there are usually casualties.

The conduct of both counsel and client thus calls to mind the now-famous words of the prison captain in *Cool Hand Luke*: "What we've got here is a failure to communicate." Because of this failure by *both* UBS and its counsel, Zubulake has been prejudiced. As a result, sanctions are warranted.

229 F.R.D. at 424.

Spoilation is the intentional or negligent loss or destruction of evidence. A recent case defined "spoliation" as "the willful destruction of evidence or the failure to preserve potential evidence for another's use in pending or future litigation." *Trigon Insurance Co. v. U.S.*, 204 F.R.D. 277, 284 (E.D. Va. 2001). Another recent case held that spoliation includes the **intentional or negligent** loss of tangible and relevant evidence which impairs a party's ability to prove or defend a claim. *Residential Funding Corp. v. DeGeorge Financial Corp.*, 306 F.3d 99, 108-109 (2d Cir. 2002).

Courts differ on whether intentional conduct or bad faith is necessary for sanctions for spoliation or whether negligence can lead to sanctions⁵. Compare, *Residential Funding Corp.*, 306 F.3d at 101 (adverse inference instruction "may be imposed where a party has breached a discovery obligation not only through bad faith or gross negligence, but also through ordinary negligence"); *Stevenson v. Union Pacific Railroad Co.*, 354 F.3d 739, 746 (8th Cir. 2004) ("under either state or federal law – there must be a finding of intentional destruction indicating a desire to suppress the truth"); *Beck v. Haik*, 377 F.3d 624, 641 (6th Cir. 2004) ("spoliation is the intentional destruction of evidence," without discussing negligence standard); and *E*Trade Securities LLC v. Deutsche Bank AG*, 230 F.R.D. 582 (D. Minn. 2005) (showing of bad faith is necessary for sanctions for destruction of relevant information before litigation has begun; no showing of bad faith is necessary where destruction of evidence occurs after litigation is imminent or has begun.)

Destruction of paper and electronic records under a proper records management policy is generally considered to be lawful where there is no litigation or investigation, actual or reasonably anticipated. A recent article on document management notes that destruction under a valid document retention policy should generally be permitted without any adverse consequences:

⁵ See, H. Chalmers, "Circuit Split Developing Over Requisite Level of Culpability for Adverse Inference Instruction," *Litigation News*, September 2007.

. . . The destruction of hardcopy documents or deletion of electronic files pursuant to a valid document management program is clearly permissible and gives rise to no adverse inference if the documents are not available in subsequent litigation.

* * *

. . . While the standard that will be applied is one of “reasonableness” at the time of destruction (or nonpreservation), the issue will always be decided with the benefit of hindsight. . . ⁶

The U.S. Supreme Court recognized the propriety of destruction under a valid document retention policy in the recent Arthur Andersen case:

“Document retention policies”, which are created in part to keep certain information from getting into the hands of others . . . are common in business. It is not wrongful for a manager or company to instruct its employees to comply with a **valid** document retention policy **under normal circumstances**.

U.S. v. Arthur Andersen, 125 S.Ct. 2129, at 2135 (2005) (emphasis added).

The duty to preserve relevant evidence arises when litigation or an investigation has commenced or is imminent, but may arise earlier. The obligation to retain arises when a “party has notice that evidence is relevant to litigation . . . but also on occasion in other circumstances, as for example, **when the party should have known that the evidence may be relevant to future litigation**.” *Byrnie v. Cromwell*, 243 F.3d 93 (2d Cir. 2001) (emphasis added).

In addition to when preservation must start, there is also an issue of **what must be preserved**. When an investigation or litigation is started or anticipated, what is the scope of paper records and electronic data which must be preserved? A district court decision, *Samsung Electronics Co., Ltd. v. Rambus, Inc.*, 439 F.Supp.2d 524 (E.D. Va. 2006), *rev’d*, 523 F.3d 1374 (Fed. Cir. 2008), describes the scope of the duty to preserve as follows:

Corporations are not obligated, “upon recognizing the threat of litigation,” to “preserve every shred of paper, every e-mail or electronic document, and every backup tape.” *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 217 (S.D.N.Y. 2003). Indeed, “[s]uch a rule would cripple large corporations.” *Id.* Nevertheless, “[w]hile a litigant is under no duty to keep or retain every document in its possession..., it is under a duty to preserve what it knows, or reasonably should know, is relevant in the action, is reasonably calculated to lead to the discovery of admissible

⁶ BNA, “Focus – Document Retention,” *Corporate Counsel Weekly* (February 20, 2002).

evidence, is reasonably likely to be requested during discovery, and/or is the subject of a pending discovery request.” *Wm. T. Thompson Co. v. General Nutrition Corp., Inc.*, 593 F.Supp. 1443, 1455 (C.D. Cal. 1984). “[A]nyone who anticipates being a party or is a party to a lawsuit must not destroy unique, relevant evidence that might be useful to an adversary.” *Zubulake*, 220 F.R.D. at 217.

The court later noted:

. . . Any company that implements a document retention policy during or in anticipation of litigation, and destroys documents relevant to the actual or anticipated litigation, will face and lose a spoliation charge. But that is as it should be.

Courts have stated that attorneys have the primary duty for preservation of evidence:

Once on notice, the obligation to preserve evidence runs first to counsel, who then has a duty to advise and explain to the client its obligations to retain pertinent documents that may be relevant to the litigation.

Telecom Int’l America, Ltd. v. AT&T Corp., 189 F.R.D. 76, 81 (S.D.N.Y. 1999).

In *Zubulake v. UBS Warburg, LLC*, 229 F.R.D. 422 (S.D.N.Y. 2004), the fifth decision on electronic discovery in an employment discrimination case, the court observed that the duty to preserve relevant records is the responsibility of both counsel and clients. Counsel first has the duty to notify the client to preserve relevant evidence, to locate relevant evidence and to ensure preservation. This is a continuing duty. “At the end of the day, however, the duty to preserve and produce documents rests on the party.”

Zubulake states that counsel has a duty to ensure that “all sources of relevant information [are] discovered.” It lists the following as the continuing steps which attorneys should take to comply with preservation obligations:

First, counsel must issue a “litigation hold” at the outset of litigation or whenever litigation is reasonably anticipated. The litigation hold should be periodically re-issued so that new employees are aware of it, and so that it is fresh in the minds of all employees.

Second, counsel should communicate directly with the “key players” in the litigation, *i.e.*, the people identified in the party’s initial disclosure and

any subsequent supplementation thereto. . . . [T]he key players should be periodically reminded that the preservation duty is still in place.

Finally, counsel should instruct all employees to produce electronic copies of their relevant active files. Counsel must also make sure that all backup media which the party is required to retain is identified and stored in a safe place. . . . One of the primary reasons that electronic data is lost is ineffective communication with information technology personnel. By taking possession of, or otherwise safeguarding, all potentially relevant backup tapes, counsel eliminates the possibility that such tapes will be inadvertently recycled.

229 F.R.D. at 433-434.

In a “Postscript,” the court states:

Now that the key issues have been addressed and national standards are developing, parties and their counsel are fully on notice of their responsibility to preserve and produce electronically stored information.

229 F.R.D. at 440.

In *Miller v. Holzmann*, 2007 WL 172327 (D.D.C., January 17, 2007), the court notes that the duty to preserve requires “**reasonable and good faith efforts**”:

The concept of a litigation hold – that is, the prevention of the destruction of documents once litigation has commenced – has been discussed most urgently in the context of electronic discovery. . . .

The Sedona Conference has suggested the following as a principle for addressing electronic document production:

The obligation to preserve electronic data and documents requires reasonable and good faith efforts to retain information that may be relevant to pending or threatened litigation. However, it is unreasonable to expect parties to take every conceivable step to preserve all potentially relevant data.

The Sedona Conference, *Best Practices Recommendations & Principles for Addressing Electronic Document Production*, 44 (2004 Annotated Version).

In an accompanying comment to this principle, the authors indicate that “[t]he notice does not need to reach all employees, only those

reasonably likely to maintain documents relevant to the litigation or investigation.” *id.*, Comment 5.d at 54.

I find this principle reasonable and in accordance with the developing case law in this area. *See, e.g., In re Napster, Inc. Copyright Litig.*, -- F. Supp. 2d --, 2006 WL 3050864 *5 (N.D. Cal. Oct. 25, 2006); *Zubulake v. UBS Warburg, Ltd.*, 220 F.R.D. 212, 216 (S.D. N.Y. 2003).

Phoenix Four, Inc. v. Strategic Resources Corp., 2006 WL 1409413 (S.D.N.Y. 2006), shows how far counsels’ duty can extend. This is a case against the plaintiff’s investment banker, alleging breach of fiduciary duty, common law fraud and negligent misrepresentation. Strategic Resources went out of business and closed its office before the litigation was filed. (The court found that it should have anticipated litigation at that time.) Strategic Resources left behind and abandoned 10 computer workstations at its office. The individual defendants took with them 2 servers and used them in their new business. In response to a document request, the defendants told their counsel “because SRC was no longer in operation, there were no computers or electronic document collections to look through or search.” They did provide boxes of paper documents.

Within a few months, a freelance computer technician, who was working on one of the servers which was malfunctioning, discovered about 25 gigabytes of data in a dormant, partitioned section of the server – as much as 2,500 boxes of documents. The desktop computers in the new office could not access this data. A substantial production of this information was made at the end of the discovery period and it was necessary to take repeated depositions of some of the witnesses.

In addition to finding fault on the part of the clients, the court found that counsel had been grossly negligent in failing to conduct further inquiry concerning defendants’ representations that there was no electronic data. Counsel had a duty to conduct a “methodical survey” and “to search for *sources* of information.” Counsel should have asked what happened to the computers which were used at the closed office, which would have alerted counsel to the existence of the server.

In analyzing document preservation issues in the context of litigation or potential litigation, it is important to note the broad scope of discovery under the Federal Rules of Civil Procedure and equivalent state rules. Fed.R.Civ.P. 26(b)(1) permits discovery not only of admissible evidence, but also of information “reasonably calculated to lead to the discovery of admissible evidence.” Determination of what should be preserved and what must be preserved presents a challenge, particularly for large and mid-size businesses, as information moves from that which is clearly relevant to that which is marginally relevant.

It is important to understand that the duty to preserve may be broader than the duty to produce. For example, data which is not reasonably accessible does not have to be produced under the new Federal Rules unless the requesting party makes a showing of good cause. This data may, however, have to be preserved so that it is still available if such a showing is made.

The Advisory Committee Notes to Rule 26(b)(2)(b) state:

A party's identification of sources of electronically stored information as not reasonably accessible does not relieve the party of its common-law or statutory duties to preserve evidence. Whether a responding party is required to preserve unsearched sources of potentially responsive information that it believes are not reasonably accessible depends on the circumstances of each case. ...

Considerations for this analysis include such factors as the likelihood that it contains relevant information that is not available elsewhere, the importance of such information, and the cost and burden of preserving it. *See*, Hon. S. Scheindlin, "The Ten Most FAQ's in the Post-December 1, 2006 World of E-Discovery," *In Camera, Federal Judges Ass'n Newsletter* (November 29, 2006) (Question 4. Does a party have to preserve inaccessible data that it does not have to search or produce under Rule 26(b)(2)(B)?). An important area is overwriting of backup tapes. In appropriate cases, it may be necessary to suspend this process.⁷

When litigation or an investigation is initiated or anticipated, counsel should work with the client to implement a litigation hold to identify and preserve relevant information. Counsel should provide clients with clear, specific, written document preservation notices, including:

- notice from counsel to management,
- notice from counsel to key employees and IT personnel,
- appropriate follow-up, and
- notice from counsel to the adverse party to preserve its electronic evidence (should be considered).

⁷ Standards as to whether and under what circumstances backup tapes must be preserved are still developing. *Compare, The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production, Second Ed.* (The Sedona Conference 2007) p. 35, ("Absent specific circumstances, preservation obligations should not extend to disaster recovery backup tapes created in the ordinary course of business"); *Zubulake v. UBS Warburg, LLC* 220 F.R.D. 212, 217-18 (S.D.N.Y. 2003) ("As a general rule, then, a party need not preserve all backup tapes even when it reasonably anticipates litigation," but preservation of backup tapes containing relevant evidence may be necessary. Generally, a litigation hold does not apply to "inaccessible backup tapes" "maintained solely for the purpose of disaster recovery," but a hold would likely apply if they are "accessible" "*i.e.*, actively used for information retrieval.") and 7 *MOORE'S FEDERAL PRACTICE* §37A.12[5][e] ("The routine recycling of magnetic tapes that may contain relevant evidence should be immediately halted on commencement of litigation").

The notices should include specific and detailed instructions about which paper and electronic records must be preserved and how they should be maintained. It should be communicated to everyone who may have control over the involved records. Appropriate follow up and monitoring is necessary, including periodically reissuing the notices. Each step of the process should be carefully documented.

For a recent publication on legal holds and litigation holds, *see*, The Sedona Conference, *Commentary on Legal Holds* (August 2007 Public Comment Version).

B. Spoliation and Sanctions

Courts have imposed harsh sanctions for spoliation of evidence, including dismissal of a case and entry of a default judgment. The range of potential sanctions for spoliation includes:

- (1) criminal prosecution – obstruction of justice, 18 U.S.C. §§ 1501, *et seq.* (recently enhanced by the Sarbanes-Oxley Act of 2002) and state statutes
- (2) dismissal or default judgment
- (3) contempt or penalty
- (4) preclusion of evidence, claim or defense
- (5) jury instruction – adverse inference from destruction or failure to produce witness or evidence
- (6) ethics violations for involved attorneys.

While courts consider a number of factors in determining an appropriate sanction for spoliation, the most important considerations are ordinarily (1) “the degree of culpability of the party who lost or destroyed the evidence” and (2) “the degree of actual prejudice to the other party.” *E.g., U.S. v. Koch Industries, Inc.*, 197 F.R.D. 488, 490 (N.D. Ok. 1999). Decisions dealing with sanctions are generally very fact specific and it is important to review them in context. The following cases are examples of the analysis which several courts have applied to spoliation issues.

The harshest sanction for destruction of evidence is criminal prosecution for obstruction of justice. A recent example is the widely publicized prosecution of Arthur Andersen in the Enron matter. Andersen was charged with destruction of paper and electronic records when it knew of Enron’s financial problems and was aware of the likelihood of a federal investigation. The indictment charged:

... an unparalleled initiative was undertaken to shred documents and delete computer files. Tons of paper relating to the Enron audit were promptly shredded as part of the orchestrated document destruction. The shredder at the ANDERSEN office at the Enron building was used virtually constantly ... A systematic effort was also undertaken and carried out to purge the computer hard-drives and E-mail system of Enron-related files.

One of the issues in the case was an ambiguous notice from Andersen's counsel concerning compliance with Anderson's document retention policy which the government claimed was a signal to destroy records. Andersen was convicted of obstruction of justice and the conviction was initially affirmed on appeal. *U.S. v. Arthur Andersen, LLP*, 374 F.3d 281 (5th Cir. 2004), *rev'd* 125 S. Ct. 2129 (2005).

Arthur Andersen's conviction was reversed by the U.S. Supreme Court on May 31, 2005. However, the reversal was based on a jury instruction covering "knowingly corruptly persuad[ing]" another to "withhold" or "alter" documents for "use in an official proceeding," the required *mens rea*, and whether an ongoing official proceeding is necessary for a violation. While some observers point to the Supreme Court decision as an affirmation of reasonable pre-litigation or pre-investigation records retention policies, carried out in good faith, others point out that is based on a jury instruction for a criminal statute, which has now been expanded, and is likely to have little impact on sanctions in civil discovery. *E.g.*, *ABAJOURNAL eReport*, June 7, 2005.

The court imposed sanctions of preclusion of testimony and a monetary penalty of \$2,995,000 in *U.S. v. Philip Morris USA, Inc.*, 2004 WL 1627252 (D.D.C. 2004). The court found that the employees of the defendant at the highest level violated both a court order and their employer's document retention policies by deleting e-mails. The court noted that the defendant "is a particularly sophisticated corporate litigant which has been involved in hundreds, and more likely thousands of smoking-related lawsuits."

Another high profile example is *Zubulake v. UBS Warburg, LLC*, *supra*, 229 F.R.D. 422, in which the court found that sanctions of an adverse inference instruction at trial, costs of repeat discovery and costs of the sanctions motion would be imposed where the defendant willfully deleted e-mails after the court determined that they were relevant. Some of the e-mails were irretrievably lost while others were restored from backup after a number of months. In April 2005, after the adverse inference instruction was given at trial, a jury awarded \$9.1 million in compensatory damages and \$20.2 million in punitive damages.

In another high profile case, the court in *Coleman Holdings, Inc. v. Morgan Stanley & Co., Inc.*, 2005 WL 679071 (Fla. Cir. Ct. 2005), *rev'd on other grounds*, 955 So.2d 1124 (Fla. App. 4th Dist., 2007), instructed the jury to accept as established many of the allegations of the complaint which alleged that the defendant conspired to defraud the plaintiff in a major corporate acquisition. The court imposed this instruction as a sanction, based on findings of obstructionist behavior by the defendant during discovery, including failure to search approximately 1,400 backup tapes for e-mails and a false certification that a complete search had been made. After receiving the instruction on fraud, a jury, in May 2005, awarded \$604 million in compensatory damages and \$850 million in punitive damages, for a total of \$1.45 billion. In March, 2007, the judgment was reversed on damages issues, without ruling on the discovery sanctions. A dissent on the damages decision, which would remand the case, found the harsh discovery sanctions to be error.

In *Rambus Inc. v. Infineon Technologies AG*, 220 F.R.D. 264 (E.D. Va. 2004), the court dealt with issues of spoliation and the crime-fraud exception to attorney-client privilege where a

plaintiff instituted a document destruction policy and intentionally destroyed documents before filing a lawsuit, including a “Shred Day” on which approximately two million pages of documents were destroyed. *Id.* at 280. The court observed:

. . . once a party reasonably anticipates litigation, it has a duty to suspend any routine document purging system that might be in effect and to put in place a litigation hold to ensure the preservation of relevant documents – failure to do so constitutes spoliation.

* * *

Even if [the plaintiff] did not institute its document retention policy in bad faith, if it reasonably anticipated litigation when it did so, it is guilty of spoliation.

Id. at 284, 287. The court held that the crime-fraud exception to attorney-client privilege covers spoliation of evidence and negates privilege for communications created for planning, or in furtherance of, spoliation. The court directed an *in camera* review to determine whether the plaintiff committed spoliation sufficient to support application of the crime-fraud exception. *Id.* at 287.

At a nonjury trial in February 2005, the court ruled from the bench that defendant had established the defense of unclean hands based on Rambus’ prelitigation destruction of evidence and litigation misconduct. In addition, the court found that dismissal of Rambus’ claims was an appropriate sanction for spoliation. The case then settled before the court entered findings of fact and conclusions of law. *See, Samsung Electronics Co., Ltd. v. Rambus, Inc.* 439 F. Supp.2d. 524 (E.D. Va. 2006), *rev’d.* 523 F.3d. 1374 (Fed. Cir. 2008).

In a case in California involving essentially the same facts, the district court held that Rambus’ prelitigation destruction of evidence was not spoliation because litigation was not “reasonably probable” at the time. *Hynix Semiconductor, Inc. v. Rambus, Inc.*, 2006 WL 565893 (N.D. Cal. 2006). In a third case, back in the Northern District of Virginia, the court declined to follow the Northern District of California decision and again found that Rambus’ prelitigation conduct constituted spoliation. *Samsung Electronics Co., Ltd. v. Rambus, Inc.*, 439 F. Supp.2d. 524 (E.D. Va. 2006), *rev’d.* 523 F.3d. 1374 (Fed. Cir. 2008) (court of appeals found sanctions to be moot).

In yet another case, *Micron Tech., Inc. v. Rambus, Inc.*, 2009 WL 54887 (D. Del. Jan. 9, 2009), the court held that Rambus’ prelitigation destruction of documents constituted spoliation because litigation was reasonably foreseeable.

These Rambus cases demonstrate that courts can reach different conclusions when reviewing, from hindsight, similar or even identical incidents of retention and destruction.

The case of *Qualcomm v. Broadcom Corp.*, (05-CV-1968-B, S.D. Cal), has been receiving substantial attention in the legal press and online media. It includes a court finding of failure to produce about 200,000 pages of e-mails and other documents until four months after trial. In addition to imposing monetary sanctions against Qualcomm, the court ordered a hearing on sanctions against counsel. That hearing was held in October, 2007. In one of its decisions, the court found:

The Court finds by clear and convincing evidence that Qualcomm counsel participated in an organized program of litigation misconduct and concealment throughout discovery, trial and post-trial before new counsel took over lead role in the case... .

On January 7, 2008, the court issued its order on sanctions. (2008 WL 66932) The court awarded sanctions of \$8,568,633.24 against Qualcomm based on a finding of “monumental and intentional discovery violation” (subject to a credit for an earlier penalty). The court also awarded sanctions against six of the attorneys representing Qualcomm, based on:

...assisting Qualcomm in committing this incredible discovery violation by intentionally hiding or recklessly ignoring relevant documents, ignoring or rejecting numerous warning signs that Qualcomm’s document search was inadequate, and blindly accepting Qualcomm’s unsupported assurances that its document search was adequate.

The sanctions included referral to the State Bar of California for investigation and required participation in a Case Review and Enforcement of Discovery Obligations (CREDO) Program to investigate and report on the causes of the violations and processes and procedures to prevent them in the future.

In a March 5, 2008 order, the district court vacated portions of the magistrate judge’s decision and remanded the sanctions portion of the case. (2008 WL 638108.) The court held that the self-defense exception to attorney-client privilege applies and that the charged attorneys are not limited by attorney-client privilege in presenting their defenses. The exception to privilege applies because Qualcomm blamed the outside attorneys for the discovery violations.

Counsel involved in e-discovery should study this case and the court’s various decision(s) in it. *See e.g.*, John C. Tredennick, Jr., “The Qualcomm EDD Sanctions: Lessons Learned from a Bad Day at the Office, *Law Technology Today* (September 2007), available at

www.abanet.org/lpm/lit/articles/vol1/is7/firewire/The-Qualcomm-EDD-Sanctions.shtml or <http://tinyurl.com/2ts6go>.

A recent patent infringement case included a finding that discovery misconduct was “among the most egregious” the magistrate judge had seen. *Keithley v. Homestore.com, Inc.*, 2008 WL 3833384 (N. D. Cal., Aug. 12, 2008). The court found that the defendant engaged in “reckless and egregious discovery misconduct,” including such conduct as making representations to plaintiffs, which turned out to be false or misleading, making misrepresentations to the court on multiple occasions, failure to implement a litigation hold, destruction of some evidence, unduly narrow reading of a court order, and more. Finding the defendants’ conduct to be reckless, the court recommended an adverse inference instruction and awarded monetary sanctions. They included fees and costs of \$62,035 incurred in making a successful motion to compel, future expenses for certain “do over” discovery of \$97,528.50, \$135,000 for expert fees for reviewing late-produced evidence (subject to in camera review), and \$25,000 for additional “do over” discovery.

In another recent patent case, *CBT Flint Partners, LLC, v. Return Path, Inc.*, N. 1:07-CV-1822-TWT (N. D. Ga., Aug. 7, 2008), the court awarded attorneys’ fees to the non-moving party in an e-discovery dispute. After spending “an enormous amount of time” on the discovery dispute, the court found that the discovery at issue was overly broad and that the moving party “engaged in no meaningful discussion” in the meet-and-confer,” “filled the record with invective,” and made false accusations of “stonewalling, delaying, and lying.” The court awarded \$86,786.95, to be paid by the moving party or its counsel.

The following is language used by judges in recent e-discovery cases involving attorney misconduct:

“counsel participated in an organized program of litigation misconduct and concealment”

“I find [counsel’s] deficiencies here to constitute gross negligence.”

“counsel’s lack of candor”

“Defendant and Defendant's counsel are jointly and severally liable for attorneys' fees and costs caused by the failure to search for and timely produce [ESI].”

“heads will have to roll, because this is outrageous”

“providing a certificate of compliance known to be false”

Made false accusations of “stonewalling, delaying, and lying.”

“assisting Qualcomm in committing this incredible discovery violation”



V. METADATA

Electronic documents have a level of information called metadata or “data about data,” which goes beyond the text or other content of the document. Metadata is electronic information which describes the history and characteristics of the electronic record. It is generally not visible when the document is printed. Metadata includes information such as when and by whom the record was created, when and by whom it was edited, what changes have been made, when and by whom it was accessed, etc. Some metadata is automatically created by the application or operating system, while other metadata, like track changes, comments and hidden text, is added by the user. Application metadata is embedded in the electronic file. System metadata is stored externally to the file on the hard drive or network. Some metadata can be viewed by the application in which the file was created, like Microsoft Word. Other metadata can be viewed with utility programs or computer forensics programs.⁸

Metadata is an important consideration for attorneys because it can lead to compromise of confidential information contained in it, both when attorneys send electronic files to others (clients, courts, opposing counsel, etc.) and when electronically stored information is provided during discovery. Ethical duties of competence (Model Rule 1.1) and confidentiality (Model Rule 1.6) apply in this area.

Metadata in e-discovery can involve issues of competence and communications with clients (Model Rule 1.4) beyond confidentiality. In many instances, an attorney cannot zealously and competently represent a party producing or seeking electronically stored information without understanding and addressing the technical issues, including metadata.

In August of 2006, the ABA issued Formal Opinion 06-442, “Review and Use of Metadata” (August 5, 2006). The opinion concludes:

The Model Rules of Professional Conduct do not contain any specific prohibition against a lawyer’s reviewing and using embedded information in electronic documents, whether received from opposing counsel, an adverse party, or an agent of any adverse party. A lawyer who is concerned about the possibility of sending, producing, or providing to opposing counsel a document that contains or might contain metadata, or who wishes to take some action to reduce or remove the potentially harmful consequences of its dissemination, may be able to limit the likelihood of its transmission by “scrubbing” metadata from documents or by sending a different version of the document without the embedded information.

⁸ This is a simplified explanation of metadata for purposes of dealing with it in the context of the current ethics considerations. For a more detailed explanation, see Craig Ball’s article and paper listed in Information Sources at the end of this paper.

The opinion notes that Rule 4.4(b) may apply to attorneys receiving metadata if the production of metadata inadvertently includes confidential information. That would require only notice to the producing party. It does not prohibit viewing the metadata. The opinion points out that transmission of metadata is not necessarily inadvertent. That issue would require a fact-specific determination.

The opinion concludes that review and use of metadata by a receiving attorney does not violate the prohibitions against dishonesty (Rule 8.4(c)) and conduct prejudicial to the administration of justice (Rule 8.4(d)).

In Footnote 4, the opinion refers to the duty to “act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure.” Rule 1.6 and Comment 16. The footnote states that whether the sending or producing lawyer acted competently in any given fact situation is beyond the scope of the opinion.

In October 2006, the Maryland State Bar Association Committee on Ethics issued Ethics Docket No. 2007-09. This opinion generally reaches the same conclusions as the ABA opinion. It also concludes that the sending attorney generally has an ethical obligation to take reasonable measures to avoid disclosure of confidential metadata. A Colorado ethics opinion reaches similar conclusions. Ethics Committee of the Colorado Bar Association, Ethics Opinion 119 (May 17, 2008).

New York, Florida, Alabama, Arizona, and Maine have issued opinions which generally provide that attorneys receiving electronic documents should not try to obtain information from metadata that was not intended for the receiving attorney. New York State Bar Association, Committee on Professional Ethics, Opinion 749 (December 14, 2001); Professional Ethics of the Florida Bar, Opinion 06-2 (September 15, 2006); Alabama State Ethics Opinion RO-2007-02 (March 14, 2007); State Bar of Arizona, Ethics Opinion 07-03 (November 2007); Maine Professional Ethics Commission of the Board of Overseers of the Bar, Opinion #106 (October 21, 2008).

A Pennsylvania ethics opinion concludes that “it would be difficult to establish a rule applicable to all circumstances” and that “each attorney must determine for himself or herself whether to utilize the metadata contained in documents and other electronic files based upon the lawyer’s judgment and the particular factual situation.” It also states that “the Committee believes that the inadvertent transmissions of such materials should not constitute a waiver of privilege, except in the case of extreme carelessness or indifference.” Pennsylvania Bar Ass’n, Committee on Legal Ethics and Professional Responsibility, Formal Opinion 2007-500, *Mining Metadata* (an advisory opinion).

These ethics opinions generally conclude that lawyers sending electronic data must exercise reasonable care to prevent inappropriate disclosure of client confidences and secrets in metadata.

As the ABA opinion notes, programs are available to “scrub” metadata from electronic documents before they are transmitted. Some of the common programs include:

- Metadata Assistant (Payne Consulting)
- iScrub (Esquire Innovations)
- EzClean (Kraft Kennedy & Lesser)
- Workshare Protect (Workshare)

Converting a document to a format like PDF will remove much of the metadata, but PDF files have their own metadata which may or may not be a concern. Adobe Acrobat 8 added a new feature called Examine Document which eliminates hidden text and other metadata from PDFs.⁹

Metadata presents different issues in e-discovery than it does in exchange by attorneys of current electronic communications and electronic documents. **In e-discovery, metadata is generally considered to be part of relevant electronic files and must be preserved. Scrubbing of metadata in this context is likely to constitute spoliation.** Whether the metadata must be produced (rather than preserved) in the circumstances of the case is another issue. In addition, metadata may contain privileged information which must be addressed like other privileged information. *See, Williams v. Sprint/United Management Co.*, 230 F.R.D. 640 (D. Kan. 2005) and *Hagenbuch v. 3B6 Sistemi Elettronici Industriali S.R.I.*, 2006 WL 665005 (N.D. Ill. 2006).

VI. CONCLUSION

Electronic discovery is becoming more and more the norm in today's litigation. Its rapid growth will continue. It is critical for litigators and other attorneys who may face records preservation and e-discovery issues to understand at least the basic legal and technical issues and to know where to go for assistance with advanced issues. Attorneys who do not have the requisite knowledge and resources will face violation of ethics rules, compromise of privilege, sanctions, and malpractice claims.



⁹ See, http://blogs.adobe.com/acrolaw/2006/12/acrobat_8_new_e.html - more or <http://tinyurl.com/ywj5up>.

VII. ADDITIONAL INFORMATION SOURCES

General Professional Responsibility

ABA/BNA Lawyer's Manual on Professional Conduct (manual and bi-weekly current reports)

American Bar Association, *ABA Compendium of Professional Responsibility Rules and Standards* (2008 Edition) (collection of professional responsibility rules, standards and selected ethics opinions)

American Bar Association, *Model Rules of Professional Conduct (2008 Edition)*

American Bar Association, *Annotated Model Rules of Professional Conduct, (2007 Ed.)*

American Bar Association Website – www.abanet.org

- Center for Professional Responsibility – www.abanet.org/cpr/professionalism/home.html (includes online version of the most Rules of Professional Conduct and headnotes to ABA ethics opinions.)
- ETHICSearch (a service which researches ethics questions, often without charge) www.abanet.org/cpr/ethicsearch/home.htm

W. Fortune, R. Underwood and E. Imwinkelried, *Modern Litigation and Professional Responsibility Handbook: The Limits of Advocacy* (Aspen 2008 Supp.)

G. Hazard, Jr., and W. Hodes, *The Law of Lawyering*, Third Edition, (Aspen, 2008 Supp.)

FindLaw, www.findlaw.com, (Ethics and Professional Responsibility Center)

Legal Ethics Forum, a legal ethics blog by a group of law professors, <http://legalethicsforum.typepad.com/blog>

Lexis, www.lexis.com, (Ethics Library)

T. Morgan, *Lawyer Law: Comparing the ABA Model Rules of Professional Conduct with the ALI Restatement (Third) of the Law Governing Lawyers* (American Bar Association 2005)

Restatement of the Law Governing Lawyers (2000)

R. Rotunda and J. Dzienkowski, *Legal Ethics: The Lawyer's Deskbook on Professional Responsibility*, (American Bar Association 2007-2008 Ed.)

Westlaw, www.westlaw.com, (Legal Ethics and Professional Responsibility Database)

Professional Responsibility in E-Discovery

A. Adam, "The Duty to Preserve Electronic Data in the Paperless Age," *The Practical Litigator* (May 2007)

S. Bennett, "The Ethics of Electronic Discovery," *The Practical Litigator* (March 2006)

S. Bennett, "Ethics in E-Discovery," (LexisNexis Applied Discovery)

-Part 1: *Ethics Guidance Needed*

-Part 2: *Has Information Technology Raised the Level of Professional Competency?*

-Part 3: *Ethics and Inadvertent Disclosure*

-Part 4: *Ethical Implications of Overseas Outsourcing*

M. Brown and P. Weiner, "Digital Dangers: A Primer on Electronic Evidence in the Wake of Enron," *Litigation* (Fall 2003)

D. Gourash, et al., *Spoliation of Evidence: Sanctions and Remedies for Destruction of Evidence in Civil Litigation*, 2d ed. (American Bar Association 2006)

Hon. P. Grimm, "Ethical Issues Associated With the Duty to Preserve Electronically Stored Evidence," Course Materials from *Advanced E-Discovery Institute: A Practical Guide to the Implementation of the New Federal Rules*, Georgetown University Law Center (November 16-17, 2006)

G. Joseph, "Spoliation: Truth or Consequences," *The Practical Litigator* (September 2007)

D. Keyko, "Managing Ethics in E-Discovery," *Legal Technology* (January 2008)

Hon. S. Scheindlin and K. Wangkeo, "Electronic Discovery Sanctions in the Twenty-First Century." *11 Mich. Telecom. Tech. L. Rev.* 71(Fall 2004)

Hon. S. Scheindlin, "The Ten Most FAQ's in the Post-December 1, 2006 World of E-Discovery," *In Camera, Federal Judges Ass'n Newsletter* (November 29, 2006) available at [www.fjc.gov/public/pdf.nsf/lookup/FAQEDisc.pdf/\\$file/FAQEDisc.pdf](http://www.fjc.gov/public/pdf.nsf/lookup/FAQEDisc.pdf/$file/FAQEDisc.pdf) or <http://tinyurl.com/yp2ax4>

The Sedona Conference, www.thesedonaconference.org:

- *Commentary on Legal Holds* (Public Comment Version) (The Sedona Conference 2007)
- *Cooperation Proclamation* (The Sedona Conference 2008)

A. Van Laningham, “Navigating the Brave New World of E-Discovery - Ethics, Sanctions and Spoliation,” *FDCC Quarterly* (Summer 2007)

E-Discovery

BNA, *Digital Discovery & e-Evidence* (a monthly report and Internet reference service)
www.pf.com/ddeePD.asp

R. Losey, *e-Discovery: Current Trends and Cases* (American Bar Ass’n 2008)

S. Nelson, B. Olson and J. Simek, *The Electronic Evidence and Discovery Handbook* (American Bar Association 2006).

G. Paul and B. Nearon, *The Discovery Revolution – E-Discovery Amendments to the Federal Rules of Civil Procedure* (American Bar Association 2005)

P. Rice, *Electronic Evidence: Law and Practice, Second Ed.* (American Bar Association 2008)

The Sedona Conference, www.thesedonaconference.org:

- *Best Practices Commentary on Search & Retrieval Methods* (August 2007)
- *Commentary on Email Management* (August 2007)
- *Commentary on Legal Holds* (Public Comment Version) (August 2007)
- *The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age* (November 2007)
- *Commentary on Preservation, Management and Identification of Sources of Information that are Not Reasonably Accessible* (The Sedona Conference 2008)
- *Cooperation Proclamation* (July 2008)
- *Glossary for E-Discovery and Digital Information Management, Second Edition* (December 2007)
- *Commentary on Preservation, Management and Identification of Sources of Information that are Not Reasonably Accessible* (July 2008)

- “Jumpstart Outline”: *Questions to Ask Your Client and Your Adversary to Prepare for Preservation, Rule 26 Obligations, Court Conferences, and Requests for Production* (Public Comment Draft) (May 2008)
- *The Sedona Principles Addressing Electronic Document Production, Second Edition* (June 2007)

Privilege

E. Epstein, *The Attorney-Client Privilege and the Work Product Doctrine*, 5th ed. (American Bar Association 2007)

Hon. J. Facciola, “Sailing on Confused Seas: Privilege Waiver and the New Federal Rules of Civil Procedure,” *2006 Federal Courts Law Review* 6 (September 2006)

P. Rice, *Attorney-Client Privilege in the United States*, (West Group 2008 Supp.) (looseleaf treatise, periodically supplemented)

V. Walkowiak, *Attorney-Client Privilege in Civil Litigation*, Third Edition (American Bar Association 2004)

Metadata

American Bar Association, “What’s the Meta with Metadata,” *YOURABA* (January, 2006), available at www.abanet.org/media/youraba/200601/article01.html or <http://tinyurl.com/29kd4x>

C. Ball, “Beyond Data about Data: The Litigator’s Guide to METADATA,” (2005), available at www.craigball.com

C. Ball, “EDD Showcase: Understanding Metadata,” *Law Technology News* (January 2006)

J. B. Beckham, “Production, Preservation, and Disclosure of Metadata,” *7 Colum. Sci. & Tech. L. Rev.* 1 (January 2006)

B. Cowgill, “Making Sense of Metadata: a Mega-list of Links for Lawyers”, *Ben Cowgill’s Legal Ethics Newsletter* (March 7, 2006), available at http://cowgill.blogs.com/legaethics/2006/03/making_sense_of.html or <http://tinyurl.com/2dyf98>

P. Geraghty, “More Data on Metadata,” *YOURABA* (December, 2006), available at www.abanet.org/media/youraba/200612/article11.html or <http://tinyurl.com/2h3yfa>

National Security Agency (NSA), “Redacting with Confidence: How to Safely Publish Sanitized Reports Converted from Word to PDF” (December 13, 2005), available at www.fas.org/sgp/othergov/dod/nsa-redact.pdf

T. Opsitnick, “Metadata,” Chapter 18 in *Information Security for Lawyers and Law Firms* (American Bar Association 2006)

D. Payne, “How to Avoid Metadata Disasters,” *Law Technology News* (August 2006).

D. Pinnington, “Beware the Dangers of Metadata,” PracticePRO (2004), available at www.lawpro.ca

Payne Group, (publisher of Metadata Assistant – a leading metadata scrubbing program) www.payneconsulting.com

C. Witherspoon, “Confidentiality and Ethics in a Wired World,” *The Practical Litigator* (May 2007)

B. Zall, “Metadata: Hidden Information in Microsoft Word Documents and its Ethical Implications,” *The Colorado Lawyer* (October 2004)

© 2009 David G. Ries. All rights reserved.

Adapted from Chp. 9 of David G. Ries, Ed., *eDiscovery* (PBI Press 2008)