

Electronically Stored Information in Bankruptcy Cases - An Ounce of Prevention

Steven Jack McCardell
Mabey Murray LC
136 South Main Street #1000
Salt Lake City, Utah 84101
Telephone: 801.320.6702
Email: steven.mccardell@mabeymurray.com

Copyright © 2005, Steven Jack McCardell, all rights reserved.

Introduction. Discovery of electronically stored information¹ is by no means a new issue. As U.S. District Court Judge J. Thomas Greene commented twenty years ago, “it is now axiomatic that electronically stored information is discoverable under Rule 34 . . . computer stored information has become involved in every type of litigation.” *Bills v. Kennecott Corp.*, 108 F.R.D. 459, 461 (D. Utah 1985). *See also 7 Moore’s Federal Practice* §34.12[3] (“Computer records and other electronically stored data are clearly within the permissible scope of discovery. Rule 34 was amended in 1970 to include ‘data compilations from which information can be obtained, translated, if necessary, by the respondent through detection devices into reasonably usable form.’”); Ch. 37A, “Discovery of Computer-Based Information” (3d Ed. 2005). What, then, is new?

This paper notes the following recent developments: (1) issuance of court rulings imposing (astonishing) sanctions for discovery missteps relating to electronically stored information; (2) development of best practices, guidelines, and compilations of information for practitioners related to electronically stored information; (3) proliferation of electronic information management and discovery vendors; and (4) promulgation of amendments to the Federal Rules of Civil Procedure geared specifically toward electronically stored information. This paper also identifies means of reducing disputes in bankruptcy cases pertaining to discovery of electronically stored information.² This is the ounce of prevention. But, first, the pound of cure.

¹“Electronically stored information” is the term adopted in amendments to the Federal Rules of Civil Procedure to be effective December 1, 2006, although to account for possible developments in technology, revised Rule 34 already defines “documents” as including “writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations stored in any medium from which information can be obtained.” Federal Rule of Bankruptcy Procedure 9014(c) makes Rule 7034 applicable in contested matters unless the court directs otherwise.

²The literature on this topic is growing at a great rate. The ABI Journal has published several excellent articles on electronic discovery and data issues: Seward, “*Always Look Both Ways—Especially When Using Digital Electronic Communications*,” (Aug. 2005); DiBiase, “*Electronic Discovery*” (Apr. 2005); Seward, “*Back to the Future: FRCP and Electronic Discovery in Bankruptcy*” (Feb. 2005); Seward, “*Protecting Yourself Against E-Illiteracy: Avoid Being Duped*” (Sept. 2004); Schwartz and Cecil, “*Computer Forensics: Insights Into Locating Undisclosed Assets*,” (Sept. 2004); Seward, “*The Debtor’s Survival in the Digital Age*” (June 2004); Seward and Austin, “*E-Sleuthing and the Art of Electronic Data*”

1. **Zubulake.** In April 2005, a Manhattan jury awarded an employment discrimination plaintiff \$9.1 million in compensatory damages and \$20.3 million in punitive damages (in September 2005, while post-trial motions were pending, the parties settled). The plaintiff had been fired as an equities trader after lodging a discrimination complaint with the EEOC. Over the course of the litigation, U.S. District Judge Shira A. Scheindlin (a member of the Federal Rules Advisory Committee) wrote several opinions, four of which concerned the defendant's e-mail production. The Court's opinions have received wide attention because they address electronic discovery issues with clarity and illustrate some of the perils of mishandling electronic discovery.³ The several opinions in the *Zubulake* case are:

**Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309 (S.D.N.Y. May 13, 2003) (*Zubulake I*) (addressing legal standard for determining cost allocation for producing emails on backup tapes)

**Zubulake v. UBS Warburg LLC*, 2003 U.S. Dist. LEXIS 7940 (S.D.N.Y. May 13, 2003) (*Zubulake II*) (addressing *Zubulake*'s reporting obligations)

**Zubulake v. UBS Warburg LLC*, 216 F.R.D. 280 (S.D.N.Y. July 24, 2003) (*Zubulake III*) (allocating backup tape restoration costs)

Retrieval Uncovering Hidden Assets in the Digital Age" (Apr. 2004, Part III; Mar. 2004, Part II; Feb. 2004, Part I). This paper does not address lawful retrieval of publicly available electronic information on the worldwide web, which is a potentially rich source of electronic information relevant to legal proceedings. Information from company and personal websites is there for the taking. Gossipy, but often revealing, information can be found in blogs and online diaries (see DiBiase, "To Blog or Not to Blog," ABI Journal, November 2005, p. 32 (discussing litigation implications of the employee blogging phenomenon)). Besides more general search engines, several specifically search engines track blogs, in close to real time. See, e.g., Google's blog search, www.technorati.com; www.feedster.com; and www.icerocket.com. Data found in governmental and private electronic databases may be available, but numerous privacy issues and statutes are involved. See generally www.epic.org (Electronic Privacy Information Center).

³Eventually, the defendant's mistakes in evidence handling led the Court to instruct the jury: "you have heard that UBS failed to produce some of the emails sent or received by UBS personnel in August and September 2001. Plaintiff has argued that this evidence was in defendants' control and would have proven facts material to the matter in controversy. If you find that UBS could have produced this evidence, and that the evidence was within its control, and that the evidence would have been material in deciding facts in dispute in this case, you are permitted, but not required, to infer that the evidence would have been unfavorable to UBS. In deciding whether to draw this inference, you should consider whether the evidence not produced would merely have duplicated other evidence already before you. You may also consider whether you are satisfied that UBS's failure to produce this information was reasonable. Again, any inference you decide to draw should be based on all of the facts and circumstances in this case." At trial, plaintiff's counsel argued that jurors should make an example out of UBS and make it too costly for UBS ever to think about fabricating an employee's records. See generally, Scheindlin and Wangkeo, "Electronic Discovery Sanctions in the Twenty-First Century," 11 Mich. Telecomm. Tech. L. Rev. 71 (2004). A March 2004 interview with Judge Scheindlin discussing electronic discovery issues has been published at <http://www.thesedonaconference.org/content/miscFiles/ScheindlinInterview.pdf>.

**Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212 (S.D.N.Y. October 22, 2003) (*Zubulake IV*) (ordering sanctions against UBS for violating its duty to preserve evidence)

**Zubulake v. UBS Warburg LLC*, 229 F.R.D. 422 (S.D.N.Y. July 20, 2004) (*Zubulake V*) (adverse inference instruction with respect to deleted emails)

**Zubulake v. UBS Warburg LLC*, 2004 U.S. Dist. LEXIS 11525 (S.D.N.Y. February 2, 2005) (*Zubulake VI*) (denying employer's motion to add after-acquired defense)

**Zubulake v. U.S. Warburg LLC*, 382 F. Supp. 2d 536 (S.D.N.Y. March 16, 2005) (*Zubulake VII*) (granting and denying parties' motions in limine)

Among the matters addressed by the Court were the following:

*In response to a request for production of all documents concerning any communication by or between UBS employees concerning the plaintiff, UBS produced 100 pages of emails. The plaintiff had already produced over 450 pages.

*After a conference with a magistrate, UBS agreed to produce responsive emails from several accounts, but then did not search its backup tapes and optical disks. It said its original 100-page production was complete. Supplemental production from restoration and search of backup tapes produced 853 more pages of responsive emails.

*The search for backup tapes revealed that UBS had not preserved all relevant backup tapes.

*After the plaintiff filed charges with the EEOC, and after an instruction to retain relevant materials, some UBS employees deleted relevant emails.

*Discovery showed that UBS anticipated litigation from the plaintiff (and therefore the duty to preserve evidence attached) four months before she filed charges with the EEOC and ten months before she filed her lawsuit.

*UBS's attorneys gave a verbal directive to preserve relevant documents (followed later with written directives). However, not all key persons received the directive and not all who received it followed it. And the instructions did not mention backup tapes.

2. **Morgan Stanley**. In *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co.*, No. CA 03-5045 (Fla. Cir. Ct., June 23, 2005), a jury awarded approximately \$727.7 million in compensatory damages and \$850 million in punitive damages against Morgan Stanley & Co. in an accounting fraud lawsuit. The plaintiff moved for sanctions, including an adverse inference jury instruction, based on the defendant's destruction of emails. Among other things, the defendant overwrote emails after twelve months, even though required by the SEC to retain emails for two years, and certified discovery as complete even though it had not reviewed some 1,400 backup tapes. The trial court found that the defendant sought to thwart discovery and "gave no thought to using an outside contractor to expedite the process . . . knowing it lacked the technological capacity to upload and search the data[.]" Order dated March 1, 2005, 2005 WL 679071. The court further shifted the burden to the defendant to prove it did not commit fraud. In an order dated March 23, 2005, the court also disqualified defense counsel and revoked counsel's *pro hac vice* admission. Order dated March 23, 2005, 2005 WL 674885. The matter is on appeal. Because of the pending appeal, on November 10, 2005, the trial court refused to rule on pending criminal contempt motions against Morgan Stanley and four of its lawyers, including its former general counsel, for allegedly withholding emails and misrepresenting facts.

3. **Adverse Inference Instruction for Spoliation of Evidence**. *Zubulake* and *Morgan Stanley* are just two of many recent examples of sanctions for spoliation of electronic evidence.⁴

- a. **Spoliation**. Spoliation is "the destruction or material alteration of evidence or the failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation." *Silvestri v. GM Corp.*, 271 F.3d 583 (4th Cir. 2001); *Byrnie v. Town of Cromwell, Board of Education*, 243 F.3d 93, 107 (2d Cir. 1001) (quoting *West v. Goodyear Tire & Rubber Co.*, 167 F.3d 776, 79 (2d Cir. 1999)); *Zubulake IV*. See also *Rowe v. Albertsons, Inc.*, 116 Fed. Appx. 171 (10th Cir 2004) (unpublished opinion) ("The doctrine of spoliation refers to the improper intentional destruction of evidence relevant to a case. Its purpose is to prevent the subversion of the discovery process

⁴For example, in *J.P. Morgan Securities, Inc.*, SEC Admin. Pro. File No. 3-11828, J.P. Morgan settled charges involving the failure to preserve email without admitting wrongdoing; it paid \$2.1 million. On March 10, 2004, the SEC announced that it had settled an enforcement action against Banc of America Securities LLC for violations of recordkeeping and access requirements of the securities laws, including failure to produce a particular email exchange BAS knew was under investigation. The settlement included a censure and a \$10 million civil penalty. www.sec.gov/news/press/2004-29.htm. In *United States v. Phillip Morris USA, Inc.*, 327 F. Supp. 2d 21 (D.D.C. 2004), sanctions of \$2.75 million were awarded for continuing an email deletion policy after the court ordered preservation of all relevant documents. In *Kucala Enterprises, Ltd. v. Auto Wax Co., Inc.*, 57 Fed. R. Serv. 3d 501; 2003 U.S. Dist. LEXIS 19103 (October 27, 2003); subsequent opinion modifying sanctions at 2004 U.S. Dist. LEXIS 5723 (N.D. Ill. April 6, 2004), a party's post-litigation use of the "Evidence Eliminator" software program to remove files from a computer, not surprisingly, led to sanctions. 2004 U.S. Dist. LEXIS 5723 (N.D. Ill. Apr. 6, 2004).

and the fair administration of justice by destroying evidence to defeat a claim.” (citations omitted)).

- b. **Party duties.** “A party has a duty to preserve all evidence that it knows or should know is relevant to any present or future litigation.” *Clark Construction Group, Inc. v. City of Memphis*, 229 F.R.D. 131, 136 (W.D. Tenn. 2005). “The trigger date is the date a party is put on notice that it has a duty to preserve evidence.” *Id.* The “obligation to preserve evidence arises when the party has notice that the evidence is relevant to litigation – most commonly when suit has already been filed, providing the party responsible for the destruction with express notice, but also on occasion in other circumstances, as for example when a party should have known that he evidence may be relevant to future litigation.” *Kronisch v. United States*, 150 F.3d 112, 126 (2d Cir. 1998). “Identifying the boundaries of the duty to preserve involves two related inquiries: when does the duty to preserve attach, and what evidence must be preserved?” *Zubulake IV*.
- c. **Counsel Duties--The “Litigation Hold.”**

Zubulake V:

“*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 a party’s initial disclosure and any subsequent supplementation thereto. Because these ‘key players’ are the ‘employees likely to have relevant information’ it is particularly important that the preservation duty be communicated clearly to them. As with the litigation hold, the 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. In cases involving a small number of relevant backup tapes, counsel might be advised to take physical possession of backup tapes. In other cases, it might make sense for relevant backup tapes to be segregated and placed in storage. Regardless of what particular arrangement counsel chooses to employ, the point is to separate relevant backup tapes from others. 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 destroyed.”

In other words, it is not enough for counsel to issue instructions to preserve relevant evidence.⁵ Counsel must take affirmative steps to ensure that evidence is preserved: (1) identify sources of discoverable information; (2) put in place a litigation hold and make that known to all relevant employees by communicating with them directly; (3) reiterate the litigation hold instructions regularly; (4) monitor compliance so that all sources of discoverable information are identified and retained on a continuing basis; and (5) call for employees to produce copies of relevant electronic evidence and arrange for segregation and safeguarding of archival media.⁶

⁵What, exactly, does the lawyer say? Counsel’s dilemma has been illustrated this way: “So, Ms. General Counsel, thank you for inviting me to meet with you today. It’s a pleasure to have the opportunity to represent your company in this litigation. But before we talk about the defense theories in the litigation, let’s talk about your preservation obligations and let’s talk about a litigation budget before we get too far along. As you suspend your document retention policy, we need to think also about your electronic evidence. You may need to consider suspending recycling of backup tapes as part of this litigation. Given the time that we anticipate will be involved in the litigation, you are probably going to be shelving 2000 to 3000 backup tapes, based on my discussions with your IT personnel. And given the cost of those, I think you probably need to budget about \$200,000 for just the cost of those backup tapes. You also are going to need to budget for some retrieval and production costs of evidence potentially off of those tapes, and borrowing from Zubulake III, let’s estimate \$200,000 to \$300,000 for that particular cost. Now, the value of your case as we see it is roughly \$250,000 to \$500,000. So you’ve got a case with a value of about half a million dollars and I need you to budget about half a million dollars for the electronic evidence portion of retention and retrieval purely related to disaster recovery systems. What happens next? My client gets a new lawyer. They keep me but reject my advice. Settlement discussions ensue immediately. At a minimum, some very tough questions begin to be asked, and they are tough questions for outside counsel and in-house counsel to answer.” See Owens, “*Judicial Conference Advisory Committee on the Federal Rules of Civil Procedure: Conference on Electronic Discovery: Panel Four: Rule 37 and/or a New Rule 34.1: Safe Harbors for E-Document Preservation and Sanctions*,” 73 Fordham L. Rev. 71 (Oct. 2004).

⁶PSS Systems, an electronic discovery vendor, has published the following “Zubulake Checklist” (http://www.pss-systems.com/resources/zubulake_checklist.html): “(1) Enable your ‘discovery liaison’ to readily describe information custodians, systems, storage, and your retention policies; (2) Affirmatively and repeatedly communicate legal holds to all affected parties; (3) Integrate your retention policies and coordinators with discovery challenges and responsibilities; (4) Actively manage and monitor document collections; (5) Interview affected employees to determine sources of information; (6) Monitor compliance with legal holds on an ongoing basis; (7) Thoroughly document and demonstrate the efficacy of your process; (8) Prepare to take responsibility or ensuring that information is preserved, collected, and produced.”

- d. **Adverse Inference Instruction.** An adverse inference instruction is one among many sanctions a court may impose for spoliation of evidence or violation of a discovery order.⁷ A three-factor test may be used to determine whether an adverse inference instruction is warranted: “(1) whether the party having control over the evidence had an obligation to preserve it when it was destroyed or altered; (2) whether the destruction or loss was accompanied by a ‘culpable state of mind;’⁸] and (3) whether the evidence that was destroyed or altered was relevant to the claims being advanced by the party that was deprived of evidence.” Grimm, “*Ethical Issues Associated With the Duty to Preserve Electronically Stored Evidence,*” ALI-ABA Course of Study Materials, Current Developments in Employment Law, Vol. 1, July 2005. Courts vary as to the degree required for the “culpable state of mind” factor. Some courts require a showing of bad faith or knowing destruction. For others, gross negligence is enough. For others, ordinary negligence is enough. *Id.*

The United States Court of Appeals for the Tenth Circuit has required bad faith for an adverse inference instruction. In the Tenth Circuit, a trial court “has discretion to fashion an appropriate remedy depending on the culpability of the responsible party and whether the evidence was relevant to proof of an issue at trial.” *Estate of Trentadue ex rel. Aguilar v. U.S.*, 397 F.3d 840, 862-63 (10th Cir. 2005) (citing *Aramburu v. Boeing Co.*, 112 F.3d 1398, 1407 (10th Cir. 1997) (requiring bad faith before imposing adverse inference). “Mere negligence in losing or destroying records is not enough because it does not support an inference of consciousness of a weak case.” *Estate of Trentadue* at 863; *Aramburu* at 1407 (the adverse influence must be predicated on the bad faith of the party destroying the

⁷Rule 37 may also be the basis for a range of sanctions for discovery misconduct, such as an order that designated facts shall be taken to be established, an order that the disobedient party may not support or oppose designated claims or defenses, an order prohibiting the party from introducing designated matters in evidence, an order striking pleadings or parts thereof, an order staying proceedings until a discovery order is obeyed, an order dismissing the action or rendering judgment by default, and an order of contempt. It has been held that “even though a party may have destroyed evidence prior to issuance of the discovery order and thus may be unable to obey, sanctions are still appropriate under Rule 37(b) because this inability was self-inflicted.” *Turner v. Hudson Transit Lines, Inc.*, 142 F.R.D. 68, 72 (S.D.N.Y. 1991). And even where there is no discovery order, a “court may impose sanctions on a party for misconduct in discovery under its inherent power to manage its own affairs.” *Residential Funding Corp. v. DeGeorge Financial Corp.*, 306 F.3d 99, 106-107 (2d Cir. 2002). For a thoughtful discussion of sanctions in a protracted discovery war in a pre-*Zubulake* class action suit involving a bankrupt communications company, the production of over a million pages of documents, 96 non-expert fact depositions, and numerous disputes over document destruction, see *Danis v. USN Communications, Inc.*, 53 Fed. R. Serv. 3d 828, 2000 U.S. Dist. LEXIS 16900 (N.D. Ill. 2000).

⁸See, e.g., *Morris v. Union Pacific Railroad*, 373 F.3d 896 (8th Cir. 1004); *Stevenson v. Union Pacific Railroad*, 354 F.3d 739 (8th Cir. 2004) (there must be some indication of an intent to destroy the evidence for the purpose of obstructing or suppressing the truth).

records).⁹ However, other sanctions are available. For example, in *Proctor & Gamble Co. v. Haugen*, 179 F.R.D. 622 (D. Utah 1998), *aff'd in part, rev'd in part*, 222 F.3d 1262 (10th Cir. 2000), Proctor & Gamble sued parties who disseminated the rumor that P & G is a corporate agent of Satan. One of the defendants moved for sanctions because P & G had not searched or saved emails of five key employees that P & G had identified as having relevant information. Although the trial court could not determine that P & G acted in bad faith, the court assessed sanctions of \$2,000 per individual for failing to search or preserve the emails.

Proposed Rule 37(f) of the Federal Rules of Civil Procedure, as changed after publication and comment, provides the following rule for sanctions related to electronically stored information: “Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the *routine, good-faith* operation of an electronic information system” (emphasis added).¹⁰

⁹Citing Texas law in a case involving a Utah citizen’s slip and fall case against a Wal-Mart in Texas, the Tenth Circuit, in an unpublished ruling stated as follows: “Presumptions arise from the nonproduction of evidence under two circumstances: (1) the deliberate spoliation of relevant evidence, which may be rebutted by showing that the evidence in question was not destroyed with fraudulent intent or purpose; and (2) the failure of a party to produce relevant evidence or offer testimony to explain its non-production. *In re T.L.K.*, 90 S.W.3d 833, 836 (Tex. App. San Antonio 2002). Under the first circumstance, a party who has deliberately destroyed evidence is presumed to have done so because the evidence was unfavorable to its case. *WAL-Mart Stores, Inc. v. Johnson*, 106 S.W.3d 718, 722, 46 Tex. Sup. Ct. J. 685 (Tex. 2003). Thus, the initial inquiry is whether the non-producing party had a duty to preserve the evidence in question. *Id.* The person asserting the presumption must show that the party who destroyed the evidence had notice both of the potential claim and of the evidence’s potential relevance. *Id.* (quoting 1 WEINSTEIN & BERGER, WEINSTEIN’S FEDERAL EVIDENCE § 301.06 at 301-28.3 (2d Ed. 2003)). Notice of a claim does not refer to any particular statistical probability that litigation will occur; rather, it simply means that litigation is more than merely an abstract possibility or unwarranted fear. The underlying inquiry is whether it was reasonable for the investigating party to anticipate litigation and prepare accordingly. *National Tank Co. v. Brotherton*, 851 S.W. 2d 193, 204, 36 Tex. Sup. Ct. J. 715 (Tex. 1993) (Necht, J., dissenting) (discussing notice of a claim in a difficult context).” *Rowe v. Albertsons, Inc.*, *supra* (3.a.) (unpublished opinion) (internal quotation marks omitted).

¹⁰Among the factors that courts are likely to consider in interpreting this rule are ever-growing statutory and regulatory requirements pertaining to document retention. Records retention rules are found in the Internal Revenue Code and regulations, Sarbanes-Oxley and SEC regulations, and practically every regulated industry (e.g., HIPAA requirements for medical records and Patriot Act and banking laws for financial institutions).

4. Avoiding Issues in Bankruptcy Cases as to Electronically Stored Information.

- a. Informed Counsel and Client Cooperation. A significant means of limiting issues, and thus cost,¹¹ relating to disputes over electronically stored information is early involvement of counsel who, with the client, identifies and understands relevant electronic information, systems¹² and relevant personnel; secures preservation of data where required; and otherwise follows best practices relating to electronic discovery.¹³ Although a bankruptcy case requires immediate attention

¹¹The cost of discovery is a primary concern in bankruptcy cases. “An entity in bankruptcy can ill afford to waste resources on litigation; every dollar spent on lawyers is a dollar creditors will never see.” *Pioneer Investment Services Co. v. Brunswick Associates Limited Partnership*, 507 U.S. 380, 409 (1993) (O’Connor, J., dissenting). See also Federal Rule of Bankruptcy Procedure 1001: “These Rules shall be construed to secure the just, speedy, and *inexpensive* determination of every case and proceeding” (emphasis added).

¹²For example, even a small company may have both current and legacy software and hardware; multiple active or inactive servers, desktops, and laptops; archives, backup and disaster recovery systems, storage media including tapes and discs; handheld devices such as personal digital assistants; cell phones and pagers; voice messaging and audio systems; building and area security data, including security systems and cameras; fax and copy machine memory; global positioning data from fleet management systems; manufacturing and materials handling equipment computer programming and memory; and tracking data from RFID tags imbedded in materials and products. The scenario in the following tongue-in-cheek comment is fast becoming too close for comfort: “Even household appliances are now becoming Internet ready. I suspect soon there will have to be warnings on household appliances saying something like: Warning, anything you toast in your toaster may be used against you in a court of law.” Withers, *Marching Through Cyberia: Discovery in the Electronic Age*,” 221 F.R.D. 90, 95 (Judicial Conference of the Second Circuit, June 7, 2002). In addition to active and archived data, residual deleted data is discoverable, and presents its own issues. 7 *Moore’s Federal Practice* §37A.03[3] (discussing residual deleted data). For a discussion of using computer forensics to find assets, see Schwartz and Cecil, “*Computer Forensics: Insights Into Locating Undisclosed Assets*,” ABI Journal (Sept. 2004).

¹³A May 2004 survey of the Association of Corporate Counsel by the Jordan Lawrence Group showed that 24% of the companies did not have a records management policy and that 41% had a policy but no enforcement of the policy. As to records destruction, 63% answered that records were destroyed “as needed.” As to email, 28% answered that email was automatically deleted. Only 46% had an email policy in place. www.jlggroup.com. Judge Scheindlin, *supra* note 3, recommends that in-house counsel ensure (1) that there is a well-thought out records retention policy in place which takes account of statutory and regulatory obligations; (2) that there is a competent person whose primary job is records retention; (3) that a records retention committee meet regularly; (4) that the records retention policy be disseminated to all company employees, and that they be tested to be sure they have understood and implemented the policy; (5) that there is a response team every time there is a litigation need to preserve documents; (6) that outside counsel is consulted early and often; (7) that an outside vendor, if warranted, be used to organize any required litigation holds; (8) that outside counsel be encouraged to raise the cost of preservation issues with the Court at the earliest possible time; (9) that he or she is well-educated about the company’s records, available technology, accessibility of stored records, and other matters; and (10) that documents not be destroyed once the duty to preserve has attached. She recommends that outside counsel (1) learn what documents the client has, along with where and in what medium are they maintained, what is the level of accessibility, and who is knowledgeable about the company’s documents; (2) come to court prepared with very specific information regarding the burden of finding what has been requested and what it will cost; (3)

to numerous other issues, in the long run an appropriate early focus on management of electronic documents is in the interest of creditors and the estate. It is increasingly important for a debtor in possession, in particular, to be able to demonstrate to the Court, to the United States Trustee, and to creditors and other parties in interest that electronic information issues are under control.¹⁴

- b. **Documents Professionals.** Hiring a document professional is expensive, but, as the cases cited above painfully illustrate, failing to address electronic documents appropriately can be much more expensive. In the proper case, hiring a competent electronic information professional should reduce disputes, and thus the overall cost, of electronic discovery. With Court approval, a trustee or debtor in possession may employ under Section 327 electronic information experts, including professional electronic document managers and computer forensics experts,¹⁵ to identify sources and implement appropriate procedures.¹⁶
- c. **Case Management.** Bankruptcy Courts have both inherent and statutory authority to manage bankruptcy cases and adversary proceedings. Under Section 105(d)(2), the Court may enter orders addressing such issues “as the Court deems appropriate to ensure that the case is handled expeditiously and economically.” Accordingly, in appropriate cases the Court may enter a general order addressing the identification, retention, and discovery of electronic documents. In adversary proceedings, Rule 16 provides a means to address electronic information issues. Proposed amendments to Rule 16 will explicitly provide for a process for addressing at an early stage the disclosure and discovery of electronic information. Procedures developed under

negotiate with opposing counsel before coming to court; (4) explain to the client litigation realities, such as the client’s burden to bear its own costs; and (5) argue that the Court should limit discovery according to the proportionality rule found in Rule 26(b)(2). See generally, Howell, “Strategic Planning At Outset of E-Discovery Can Save Money in the End,” 5 Digital Discovery & e-Evidence, Best Practices & Evolving Law (Feb. 2005).

¹⁴Seward, “*The Debtor’s Survival in the Digital Age*,” ABI Journal (June 2004) (“The ideal situation is for debtor’s counsel to arrange for the digital forensic accounting technologist to immediately view the computers and digital devices in place on-site at the start of the case.”) (listing 14 items debtor’s counsel should consider making available to the creditors committee before the 341 meeting).

¹⁵Wall and Paroff, “*Cracking the Computer Forensics Mystery*,” 17 Utah Bar J. 10 (Oct. 2004).

¹⁶Given the proliferation of vendors with varying skills and costs, the variety of tasks, and developments in legal requirements, selecting an appropriate expert is no small task. See *Best Practices for the Selection of Electronic Discovery Vendors: Navigating the Vendor Proposal Process* (July 2005), available at www.thesedonaconference.org.

amended Rule 16 may be used in a case management order under Section 105.

- d. **Rule 26 Disclosures.** Rule 26(a)(1), where applicable,¹⁷ requires that parties provide to other parties, without discovery, “a copy of, or a description by category and location of all documents, data compilations, and tangible things that are in the possession, custody, or control of the party and that the disclosing party may use to support its claims or defenses, unless solely for impeachment.” Compliance with this rule, where applicable, would eliminate some disputes over electronically stored information.
- e. **Rule 26 Agreements.** Under Rule 26(f), where applicable,¹⁸ the attorneys of record and all unrepresented parties that have appeared in the case are jointly responsible for arranging a conference to attempt to agree in good faith on a discovery plan. Agreements can go a long way to reduce cost. For example, counsel might agree to first search in active electronic and paper files and then, after an appropriate showing of a need and allocation of cost, search further into backup, metadata¹⁹ and other information.²⁰ Counsel should discuss the form

¹⁷Rule 9014(c) provides that Rule 26 applies in contested matters unless the Court directs otherwise, or unless otherwise provided in the rule. Rule 9014(c) states that Rule 26(a)(1) (mandatory disclosure) shall not apply in a contested matter unless the court directs otherwise.

¹⁸ Rule 9014(c) provides that Rule 26 applies in contested matters unless the Court directs otherwise, or unless otherwise provided in the rule. Rule 9014(c) states that Rule 26(f) (mandatory meeting before scheduling conference/discovery plan) shall not apply in a contested matter unless the court directs otherwise.

¹⁹Production of metadata may not be just a discovery issue. It may also be an ethics issue. See New York State Bar Ass’n Committee on Professional Ethics, Opinion 782 (12/8/04) (lawyers have a duty to use reasonable care when transmitting documents by email to prevent the disclosure of metadata containing client confidences or secrets). For this reason, the use of “clawback” agreements, under which production without intent to waive will not waive privilege, confidential or secret trade information, or trial preparation material objections, is becoming popular. Such agreements are not a cure-all. See *Westlake Vinyls, Inc. v. Goodrich Corp.*, Case No. 5:03CV-00240-R, 2005 U.S. Dist. LEXIS 16339 (W.D. Ky. Aug. 8, 2005) (tacit clawback agreement but court reviewed a number of factors to determine dispute: (1) reasonableness of precautions taken to prevent inadvertent disclosure; (2) number of inadvertent disclosures; (3) extent of inadvertent disclosure; (4) promptness of measures taken to rectify the situation; (5) whether the interests of justice would be served by relieving party of the error). Comments to proposed rule 26(f) suggest that parties “may agree that the responding party will provide certain requested materials for initial examination without waiving any privilege or protection—sometimes known as a ‘quick peek.’ The requesting party then designates the documents it wishes to have actually produced. This designation is the Rule 34 request. The responding party then responds in the usual course, screening only those documents actually requested for formal production and asserting privilege claims as provided in Rule 26(b)(5)(A). On other occasions, parties enter agreements—sometimes called ‘clawback agreements’—that production without intent to waive privilege or protection should not be a waiver so long as the responding party identifies the documents mistakenly produced, and that the documents should be returned under those circumstances. Other voluntary arrangements may be appropriate depending on the circumstances of each litigation.”

of production, such as whether the electronic information will be presented in its native format, whether it will be produced electronically or in hard copy, and whether metadata will be produced.²¹ Conferring in good faith (or attempting to do so) is a prerequisite to seeking a protective order under Rule 26(c) or a motion to compel discovery under Rule 37(a) and many local rules of court. Proposed amendments to Rule 26 will require parties to discuss issues relating to disclosure and discovery of electronically stored information during the discovery-planning conference.²²

- f. **Preservation Letters and Orders.** Absent agreement, it is increasingly common for parties to send preservation letters.²³ In addition to the inherent power courts have over matters before them, Bankruptcy Code Section 105(d) and Rule 16(c) provide a basis for a preservation order.²⁴

²⁰September 2005 Report of the Judicial Conference Committee on Rules of Practice and Procedure, at p. 40: “Lawyers sophisticated in these problems [i.e., difficulty of accessing certain forms of electronic information] are developing a two-tier practice in which they first sort through the information that can be provided from easily accessed sources and then determine whether it is necessary to search the difficult-to-access sources.” See also “Judicial Conference Advisory Committee on the Federal Rules of Civil Procedure: Conference on Electronic Discovery: Panel Four: Rule 37 and/or a New Rule 34.1: Safe Harbors for E-Document Preservation and Sanctions,” 73 Fordham L. Rev. 71 (October 2004) (Stephen G. Morrison, discussing Texas Rule of Civil Procedure 196.4).

²¹See *Williams v. Sprint/United Management Co.*, Civil Action No. 03-220 (D. Kan. Sept. 29, 2005) (dispute over discovery dispute where party scrubbed metadata from Excel spreadsheets and locked certain spreadsheet data; court reviews current state of the law on production of metadata).

²²Under Federal Rule of Bankruptcy Procedure 9014(c), Rule 26(f) does not apply in a contested matter unless the Court directs otherwise. Any party may request, or the Court may direct, that the rule apply in a contested matter. Under amended Rule 26(f), counsel will have an express obligation “to discuss any issues relating to preserving discoverable information,” “issues relating to disclosure or discovery of electronically stored information, including the form or forms in which it should be produced,” and “any issued relating to claims of privilege or of protection as trial-preparation material, including—if the parties agree on a procedure to assert such claims after production—whether to ask the court to include their agreement in an order.” The comments to amended Rule 26(f) note that counsel and parties will have to discuss and become familiar with the parties’ information systems and, with that information, develop a discovery plan that takes into account the capabilities of their computer systems. Early identification of individuals with special knowledge of a party’s computer systems is recommended.

²³See Ball, “The Perfect Preservation Letter,” www.craigball.com; “Effective Preservation Letters for Electronic Evidence,” www.forensicon.com/articles/preservation-letters.asp; Form Spoliation Letter to Opposing Counsel, www.discoveryresources.org/01_electronic_discovery_tools.html.

²⁴Rule 16(c)(12) (pretrial order may address the need for adopting special procedures for managing potentially difficult or protracted actions that may involve complex issues, multiple parties, difficult legal questions, or unusual proof problems) and (16) (such other matters as may facilitate the just, speedy, and inexpensive disposition of the action). Rule 7016 makes it applicable in adversary proceedings. Although Rule 9014(c) does not apply Rule 16 to contested matters, the court may order that it apply under Rule 9014(c) (the court may at any stage in a particular matter direct that one or more of the other rules in Part VII shall apply). In addition, the court may enter an order under Section 105(d) (order prescribing such limitations and conditions as the court deems appropriate to ensure that the case is handled expeditiously

- g. **Orders Limiting Discovery.** Under Rule 26(b)(2),²⁵ the Court may order limits on discovery otherwise permitted if the Court determines that: “(i) the discovery sought is unreasonably cumulative or duplicate or is obtainable from some other source that is more convenient, less burdensome, or less expensive; (ii) the party seeking discovery has had ample opportunity by discovery in the action to obtain the information sought; or (iii) the burden or expense of the proposed discovery outweighs its likely benefit, taking into account the needs of the case, the amount in controversy, the parties’ resources, the importance of the issues at stake in the litigation, and the importance of the proposed discovery in resolving the issues.” For example, it is easy to ask for emails but it may be very difficult to produce them, especially where the only source is backup tapes.²⁶ In *United States ex re Tyson v. Amerigroup Illinois, Inc.*, Case No. 02-6074, 2005 U.S. Dist. LEXIS 24929 (N.D. Ill. Oct. 21, 2005), the relator in a health care fraud *qui tam* action served a subpoena on a non-party state department of public aid demanding emails of two current and one former employees for a five-year period, limited to specified search terms appearing in the emails. After reviewing a detailed (and unrebutted) affidavit of a chief information systems officer, the Court determined that responding would be an undue burden because, among other things, the project involved restoring emails through use of backup tapes²⁷ and

and economically. In *Antioch Co. v. Scrapbook Borders, Inc.*, 210 F.R.D. 645 (D. Minn. 2002), the court issued a records preservation order before the parties’ Rule 26(f) conference and before the court’s pretrial conference. Proposed Rule 16(b)(5) will expressly provide that the scheduling order may include “provisions for disclosure or discovery of electronically stored information.”

²⁵Rule 9014(c) provides that Rule 7026(b) is applicable in contested matters unless the Court directs otherwise.

²⁶*See generally*, 7 *Moore’s Federal Practice*, §37A.33[4] (significant cost and burden involved in retrieving emails). For a mock argument involving a dispute over production of email backup tapes, *see* “*Marching Through Cyberia: Discovery in the Electronic Age*,” 221 F.R.D. 90, 113-128 (Judicial Conference of the Second Circuit, June 7, 2002).

²⁷While backup tapes figure prominently in many electronic discovery disputes and the failure to handle them properly can lead to terrible sanctions, the *Amerigroup* Court recognized that restoring emails through the use of backup tapes, which in the hierarchy of accessibility are near the bottom, is a unique burden. *See Hagemeyer North America, Inc., v. Gateway Data Sciences Corp.*, 222 F.R.D. 594, 600 (E.D. Wis. 2004). The September 2005 Report of the Judicial Conference Committee on Rules of Practice and Procedure explains that difficulties in accessing information may arise from a number of different reasons primarily related to the technology of information storage: “back-up tapes intended for disaster recovery purposes that are often not indexed, organized, or susceptible to electronic searching; legacy data that remains from obsolete systems and is unintelligible on the successor systems; data that was ‘deleted’ but remains in fragmented form, requiring a modern version of forensics to restore and retrieve; and databases that were designed to create certain information in certain ways and that cannot readily create very different kinds or forms of information” p. 40. Specialized equipment is required to read them and, as systems change, reading them with current equipment may no longer be possible. In addition, there may be unavoidable data loss even in properly handled backup tapes. Furthermore, backup tapes may cost \$50 to \$100 each

eighteen weeks of work requiring substantial equipment and manpower use. Asking for all of the company's emails may roughly be the equivalent of asking for the files (or for a deposition of) every employee in the company, whether or not they have anything to do with the litigation, which obviously is not something a court would allow.²⁸ Rational limits related to available resources and the nature of the proceeding are imperative. Bankruptcy cases frequently may present circumstances where an order limiting electronic discovery is needed to protect the bankruptcy estate from undue burden or expense.²⁹

- h. **Examiners, Special Masters, and Court-Designated Experts.** In appropriate cases, the Bankruptcy Court has power to order the appointment of an examiner under Section 1104(c). Under Section 1106(b), an examiner's duties include designated investigative powers and may be ordered to perform "any other duties of the trustee that the court orders the debtor in possession not to perform." This might include identification and preservation of electronically stored information. Although Rule 9031 specifically forbids the appointment of Special Masters in bankruptcy cases, nothing prevents the Bankruptcy Court from appointing an examiner or an expert witness under Federal Rule of Evidence 706.³⁰

and, if properly stored, have a monthly off-site (temperature controlled) storage cost. Restoration, searching, cataloging, transporting, de-duplicating, and other services add to the cost. Given these costs, the realities of the hypothetical conversation given in note 4 are apparent. For a discussion of backup tapes issues, see Friedberg, "To Recycle or Not to Recycle, That is the Hot Backup Tape Question," www.strozllc.com/publications.html.

²⁸See "Judicial Conference Advisory Committee on the Federal Rules of Civil Procedure: Conference on Electronic Discovery: Panel Four: Rule 37 and/or a New Rule 34.1: Safe Harbors for E-Document Preservation and Sanctions," 73 Fordham L. Rev. 71 (October 2004) (Laura Lewis Owens). One 2002 estimate figured that a company with 100 employees may generate 7.5 million emails a year. Ken Withers, "Digital Discovery," Nat. L. J. (Nov. 4, 2002).

²⁹The Bankruptcy Code recognizes that in bankruptcy cases, information for information's sake is not the object. See, e.g., Section 1125 (defining "adequate information" in a disclosure statement in terms of what is "reasonably practicable in light of the nature and history of the debtor and the condition of the debtor's books and records"). For example, electronically stored information may include: "voice mail messages and files, back-up voice mail files, email messages and files, backup email files, deleted emails, data files, program files, backup and archival tapes, temporary files, system history files, web site information stored in textual, graphical or audio format, web site log files, cache files, cookies, and other electronically-recorded information." *Super Film of America, Inc., v. UCB Films, Inc.*, 219 F.R.D. 649 (D. Kan. 2004). Bankruptcy Courts are not likely to require trustees or debtors in possession as a matter of course to preserve, reconstruct and produce in searchable form of every bit of electronic data relevant to a bankrupt company, particularly when the Federal Rules of Bankruptcy Procedure mandate that the rules "be construed to secure the just, speedy, and inexpensive determination of every case and proceeding." Rule 1001.

³⁰For a discussion of bankruptcy court appointment of experts under Rule 706 as opposed to employment under Section 327, see *Baehr v. Touche Ross & Co. (In re Philadelphia Mortgage Trust)*, 930 F.2d 306 (3d

5. **Selected Resources on Electronically Stored Information.** The following materials provide background and resources on the management and discovery of electronic information.

a. **The Sedona Conference Materials.** In response to growing concerns over electronic discovery, the Sedona Conference Working Group has produced a series of useful publications. The materials are updated periodically and can be found at www.thesedonaconference.org.

(i) **The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age (September 2005).** The principles discussed at length in this publication are:

1. An organization should have reasonable policies and procedures for managing its information and records.

- a. Information and records management is important in the electronic age.
- b. The hallmark of an organization's information and records management policies should be reasonableness.
- c. Defensible policies need not mandate the retention of all information and documents.

2. An organization's information and records management policies and procedures should be realistic, practical and tailored to the circumstances of the organization.

- a. No single standard or model can fully meet an organization's unique needs.
- b. Information and records management requires practical, flexible and scalable solutions that address the differences in an organization's business needs, operations, IT infrastructure and regulatory and legal responsibilities.
- c. An organization must assess its legal requirements for retention and destruction in developing an information and records management policy.

Cir. 1991). Even where formal designation of an expert under Rule 706 is not needed, the use of a third party reviewer may help to resolve discovery disputes. In *McCurdy Group, LLC v. American Biomedical Group, Inc.*, No. 00-6183, 2001 U.S. App. LEXIS 10570, at *1, 9 Fed. Appx. 822 (10th Cir. May 21, 2001), during a discovery dispute over electronically stored information that involved privileged information, one party offered to produce certain disc drives to a third party computer forensics expert for inspection. The other party refused the offer and moved to compel. The Court held that the moving party had failed to explain why it should be allowed to conduct a physical inspection of the hard drives and "why inspection of the zip drive and/or inspection of the hard drive by [the expert] would not have been sufficient to satisfy its concerns."

d. An organization should assess the operational and strategic value of its information and records in developing an information and records management program.

e. A business continuation or disaster recovery plan has different purposes from those of an information and records management program.

3. An organization need not retain all electronic information ever generated or received.

a. Destruction is an acceptable stage in the information life cycle; an organization may destroy or delete electronic information when there is no continuing value or need to retain it.³¹

b. Systematic deletion of electronic information is not synonymous with evidence spoliation.

c. Absent a legal requirement to the contrary, organizations may adopt programs that routinely delete certain recorded communications, such as electronic mail, instant messaging, text messaging and voice-mail.

d. Absent a legal requirement to the contrary, organizations may recycle or destroy hardware or media that contain data retained for business continuation or disaster recovery purposes.

e. Absent a legal requirement to the contrary, organizations may systematically delete or destroy residual, shadowed or deleted data.

f. Absent a legal requirement to the contrary, organizations are not required to preserve metadata.

4. An organization adopting an information and records management policy should also develop procedures that address the creation, identification, retention, retrieval and ultimate disposition or destruction of information and records.

a. Information and records management policies must be put into practice.

³¹Implementing a document destruction policy can have terrible consequences, as the sad case of Arthur Andersen illustrates. *Arthur Andersen LLP v. United States*, 125 S. Ct. 2129 (May 31, 2005). Although the term “Shred Day” is popular in identity theft prevention events, holding a “Shred Day” where documents may be relevant to litigation may not be such a good idea. In *Rambus, Inc., v. Infineon Technologies AG*, 220 F.R.D. 264 (E.D. Va. 2004), a company developed in 1998 a document retention and destruction policy with the help of a law firm. That summer, the company’s executives gave presentations on the policy and kicked off the program with “Shred Day,” where all headquarters employees received a burlap sack with instructions to bag documents for shredding. Approximately 20,000 pounds of documents, some 2 million pages, were shredded that day, with additional documents shredded later. Naturally, a litigation opponent who filed a lawsuit two years later made much of “Shred Day,” painting it as a sinister event “pointing to internal Rambus emails that reflect that Shred Day culminated in a 5:00 PM beer, pizza, and champagne ‘celebration.’” The company was hard pressed to frame “this beer, pizza, and champagne treat not as a ‘celebration,’ but rather as corporate incentive and morale boosting after a day of heavy sack lifting and laborious document review.” 222 F.R.D. at 280.

b. Information and records management policies and practices should be documented.

c. An organization should define roles and responsibilities for program direction and administration within its information and records management policies.

d. An organization should guide employees regarding how to identify and maintain information that has a business purpose or is required to be maintained by law or regulation.

e. An organization may choose to define separately the roles and responsibilities of content and technology custodians for electronic records management.

f. An organization should consider the impact of technology (including potential benefits) on the creation, retention and destruction of information and records.

g. An organization should recognize the importance of employee education concerning its information and records management program, policies and procedures.

h. An organization should consider conducting periodic compliance reviews of its information and records management policies and procedures, and responding to the findings of those reviews as appropriate.

i. Policies and procedures regarding electronic management and retention should be coordinated and/or integrated with the organization's policies regarding the use of property and information, including applicable privacy rights or obligations.

j. Policies and procedures should be revised as necessary in response to changes in workforce or organizational structure, business practices, legal or regulatory requirements and technology.

5. An organization's policies and procedures must mandate the suspension of ordinary destruction practices and procedures as necessary to comply with preservation obligations related to actual or reasonably anticipated litigation, government investigation or audit.

a. An organization must recognize that suspending the normal disposition of electronic information and records may be necessary in certain circumstances.

b. An organization's information and records management program should anticipate circumstances that will trigger the suspension of normal destruction procedures.

c. An organization should identify persons with authority to suspend normal destruction procedures and impose a legal hold.

d. An organization's information and records management procedures should recognize and may describe the process for suspending normal

records and information destruction and identify the individuals responsible for implementing a legal hold.

e. Legal holds and procedures should be appropriately tailored to the circumstances.

f. Effectively communicating notice of a legal hold should be an essential component of an organization's information and records management program.

g. Documenting the steps taken to implement a legal hold may be beneficial.

h. If an organization takes reasonable steps to implement a legal hold, it should not be held responsible for the acts of an individual acting outside the scope of authority and/or in a manner inconsistent with the legal hold notice.

i. Legal holds are exceptions to ordinary retention practices and when the exigency underlying the hold no longer exists (*i.e.*, there is no continuing duty to preserve the information), organizations are free to lift the legal hold.

(ii) *The Sedona Principles: Best Practices & Recommendations for Addressing Electronic Document Production* (July 2005). The principles discussed at length in this publication are:

1. Electronic data and documents are potentially discoverable under Fed. R. Civ. P. 34 or its state law equivalents. Organizations must properly preserve electronic data and documents that can reasonably be anticipated to be relevant to litigation.

2. When balancing the cost, burden, and need for electronic data and documents, courts and parties should apply the balancing standard embodied in Fed. R. Civ. P. 26(b)(2) and its state law equivalents, which require considering the technological feasibility and realistic costs of preserving, retrieving, producing, and reviewing electronic data, as well as the nature of the litigation and the amount in controversy.

3. Parties should confer early in discovery regarding the preservation and production of electronic data and documents when these matters are at issue in the litigation, and seek to agree on the scope of each party's rights and responsibilities.

4. Discovery requests should make as clear as possible what electronic documents and data are being asked for, while responses and objections to discovery should disclose the scope and limits of what is being produced.

5. 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.

6. Responding parties are best situated to evaluate the procedures, methodologies, and technologies appropriate for preserving and producing their own electronic data and documents.

7. The requesting party has the burden on a motion to compel to show that the responding party's steps to preserve and produce relevant electronic data and documents were inadequate.

8. The primary source of electronic data and documents for production should be active data and information purposely stored in a manner that anticipates future business use and permits efficient searching and retrieval. Resort to disaster recovery backup tapes and other sources of data and documents requires the requesting party to demonstrate need and relevance that outweigh the cost, burden, and disruption of retrieving and processing the data from such sources.

9. Absent a showing of special need and relevance a responding party should not be required to preserve, review, or produce deleted, shadowed, fragmented, or residual data or documents.

10. A responding party should follow reasonable procedures to protect privileges and objections to production of electronic data and documents.

11. A responding party may satisfy its good faith obligation to preserve and produce potentially responsive electronic data and documents by using electronic tools and processes, such as data sampling, searching, or the use of selection criteria, to identify data most likely to contain responsive information.

12. Unless it is material to resolving the dispute, there is no obligation to preserve and produce metadata absent agreement of the parties or order of the court.

13. Absent a specific objection, agreement of the parties or order of the court, the reasonable costs of retrieving and reviewing electronic information for production should be borne by the responding party, unless the information sought is not reasonably available to the responding party in the ordinary course of business. If the data or formatting of the information sought is not reasonably available to the responding party in the ordinary course of business, then, absent special circumstances, the costs of retrieving and reviewing such electronic information should be shifted to the requesting party.

14. Sanctions, including spoliation findings, should only be considered by the court if, upon a showing of a clear duty to preserve, the court finds that there was an intentional or reckless failure to preserve and produce relevant electronic data and that there is a reasonable probability that the loss of the evidence has materially prejudiced the adverse party.

(iii) *Best Practices for the Selection of Electronic Discovery Vendors: Navigating the Vendor Proposal Process* (July 2005). This publication explains in detail what electronic discovery vendors do and how to go about selecting and retaining an appropriate vendor,³² including how to

³²Hiring an expert who does not follow best practices can undermine what otherwise might be a solid case for seeking sanctions against an opponent for document destruction. *See Gates Rubber Co. v. Bando Chemical Industries, Ltd.*, 167 F.R.D. 90 (D. Colo. 1996) (plaintiff hired a technician who overwrote and thereby lost data on 7-8 percent of a hard drive before starting his efforts to copy the contents; failed to

design requests for information and requests for proposals in specific litigation. The Sedona Conference website lists the following vendors as having agreed to respond within the framework of its RFP guidelines (the list is updated periodically) (the web sites of many of these vendors have helpful reference materials as well):

ACT Litigation Services
Applied Discovery
Aspen Systems Corporation - iCite Division
Attenex Corporation
Capital Legal Solutions
CaseCentral
Cataphora, Inc.
The Common Source, Inc.
CompuLit
CoreFacts
Cricket Technologies, LLC
Digital Mandate
Diskcovery Information Management Pty Ltd
DolphinSearch, Inc.
Electronic Evidence Discovery, Inc.
Encore Lex Solutio
Fios, Inc.
Forensics Consulting Solutions, LLC
FTI Consulting, Inc.
Guidance Software
H5 Technologies, Inc.
InData
KPMG
LECG
LDM - Legal Document Management Ltd.
LextraNet
National Data Conversion
NTI Breakwater
On-Site E-Discovery
Relevant Evidence, LLC
Renew Data
SPI Litigation Direct
Stratify, Inc.

obtain creation dates of files failed to do an “image backup” of the hard drive, thereby failing to use the method which would yield the most complete and accurate results; these failures weakened the plaintiff’s sanctions case).

Numerous vendors outside this group provide electronic discovery services, including litigation support services firms, most large accounting firms, and firms specializing in electronic discovery. A Google search of the term “electronic discovery services” produced over 20,000 hits. Some of the firms advertising services in this area currently are: Alpha Systems, Arete Legal, Arma International, Data Discovery Direct, Daticon, Deloitte Touche, Discovery Mining, DOAR Litigation Consulting, DolphinSearch, Emag Solutions, Electronic Data & Evidence Discovery Services, Electronic Evidence Retrieval, Fast Track Litigation Support, Forensicon, Forensic Computer Service, Global Digital Forensics, Ernst & Young, Guardent, Inc., Iron Mountain Digital Solutions, Kroll Ontrack, Lateral Data, Litigation Solution, Inc., Merrill Corporation, Planet Data Solutions, PriceWaterhouseCoopers, RLS Legal Solutions, Servient, SoundEvidence, and Stroz Friedberg LLC.

Some of the certifications available for computer forensics experts include Certified Forensic Computer Examiner (CFCE) (law enforcement only) (there are several other law enforcement certifications as well), Certified Computer Examiner (CCE), EnCase Certified Examiner (EnCE—issued by Guidance Software),³³ Certified Information Forensics Investigator (CIFI—issued by the International Information Systems Forensics Association, IISFA), Certified Computer Forensic Technician (CCFT), Certified Information Systems Security Professional (CISSP).³⁴

(iv) *The Sedona Conference Glossary for E-Discovery and Digital Information Management* (May 2005). From “ablate” to “Zone OCR,” this glossary defines terms used in computer technology, electronic discovery and electronic records management.

b. **New Federal Rules on E-Discovery.** Pending proposed amendments to the Federal Rules of Civil Procedure dealing with discovery of electronically stored evidence are discussed elsewhere in these materials (materials prepared by Holly R. Shilliday of Snell & Wilmer L.L.P.). The proposed rules, which would become effective December 1, 2006, are the result of a five-year process conducted by the Rules Advisory Committee and can be viewed at www.uscourts.gov/rules/newrules6.html. The Federal Courts web page summarizes the principal amendments as follows:

³³<http://www.encase.com/training/ence/referrals.asp> lists individuals certified by Guidance Software.

³⁴Grindstaff, “*Finding a Computer Forensics Specialist*,” NC Lawyers Weekly, 4/1805. Numerous software programs, such as EnCase, Forensic tool Kit, SMART, Maresware, ProDiscover, Datalifter, and P2 are available. *Id.* See also, Nelson and Simek, “*Finding Wyatt Earp: Your Computer Forensics Expert*” (2005) at <http://www.senseient.com/default.asp?page=publications/article34.htm>; Computer Forensics, Cybercrime, and Steganography Resources at <http://www.forensics.nl>.

Civil Rule 16 (Pretrial Conferences; Scheduling; Management) (establishes process for the parties and court to address early issues pertaining to the disclosure and discovery of electronic information)

Civil Rule 26 (General Provisions Governing Discovery; Duty of Disclosure) (requires parties to discuss during the discovery-planning conference issues relating to the disclosure and discovery of electronically stored information)

Civil Rule 33 (Interrogatories to Parties) (expressly provides that an answer to an interrogatory involving review of business records should involve a search of electronically stored information)

Civil Rule 34 (Production of Documents and Things and Entry Upon Land for Inspection and Other Purposes) (distinguishes between electronically stored information and “documents”)

Civil Rule 37 (Failure to Make Disclosure or Cooperate in Discovery; Sanctions) (creates a “safe harbor” that protects a party from sanctions for failing to provide electronically stored information lost because of the routine operation of the party's computer system)

Civil Rule 45 (Subpoena) (technical amendments that conform to other proposed amendments regarding discovery of electronically stored information)

Form 35 (Report of Parties' Planning Meeting) (technical revision reflecting the proposed amendment to Civil Rule 26)

c. **Court Rules on Discovery of Electronic Documents.** The Ad Hoc Committee for Electronic Discovery of the U.S. District Court for the District of Delaware has developed a default standard for the discovery of electronic documents which is available for use by parties in litigation in that district. See <http://www.ded.uscourts.gov/OrdersMain.htm>. Local rules with specific provisions for electronic discovery have been adopted by United States District Courts in Wyoming, New Jersey, and Arkansas. Mississippi and Texas have adopted civil electronic discovery rules. In September 2005, the Conference of Chief Justices Working Group on Electronic Discovery published draft Guidelines for State Trial Courts Regarding Discovery of Electronically Stored Information. See <http://www.ncsconline.org/>

d. **Federal Judicial Center Materials.** The Federal Judicial Center's web site includes a page with links to numerous electronic discovery resources for civil litigation, including annotated case law on electronic discovery, workshop and seminar materials, research reports, court rules on electronic discovery, and sample forms and orders. See <http://www.fjc.gov>. In addition, the

web site of Kenneth J. Withers, a research associate at the Federal Judicial Center and expert on electronic discovery issues, www.kenwithers.com, collects materials on electronic discovery. See also Mr. Withers' discussion, "*Marching Through Cyberia: Discovery in the Electronic Age*," 221 F.R.D. 90-128 (Judicial Conference of the Second Circuit, June 7, 2002), followed by a mock argument of a dispute involving electronic discovery.

e. **Additional Web Sites with Electronic Document and Discovery Resources.**

<http://www.abanet.org/litigation/taskforces/standards.html>

(ABA Discovery Standards Task Force Web Site)

www.discoveryresources.org (website sponsored by Fios)

<http://www.e-evidence.info/legal1.html> (Electronic Evidence Information Center)

www.fiosinc.com/resources/index.html (Fios resources page)

www.forensicon.com/resources.asp (Forensicon resources page)

www.lexisnexis.com/applieddiscovery/clientResources/clientWhitePapers.asp (Lexis/Nexis white papers on electronic documents/discovery issues)

www.practicepro.ca/practice/eDiscovery_Rlist.asp (electronic discovery reading list and resources)