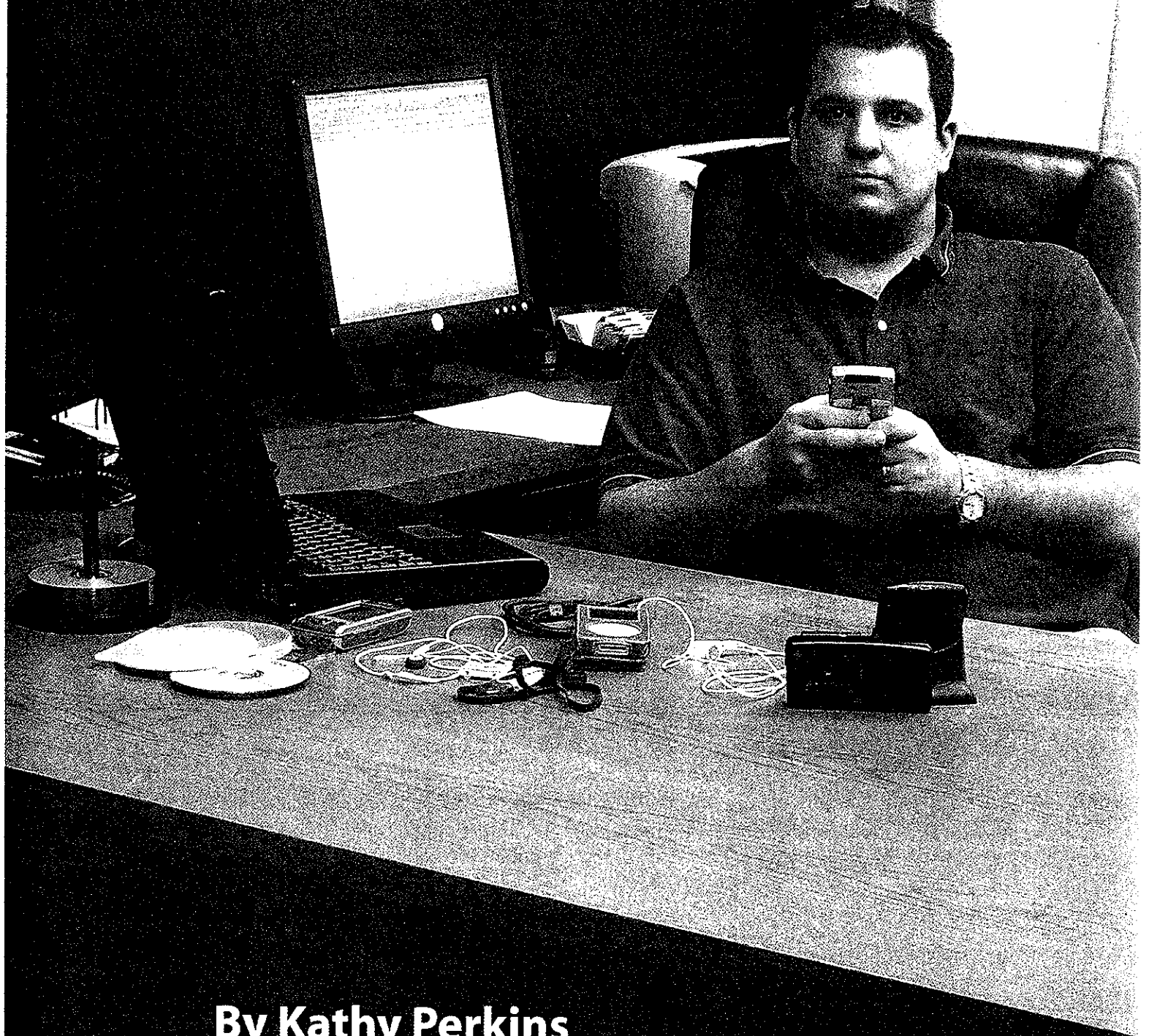


# **"BYTE" ME!**

**Protecting Your Backside in an  
Electronic Discovery World  
(Not Just for Litigators)**



**By Kathy Perkins  
with Dave Deppe**

## I. Introduction

"To see confusion clearly is to understand."<sup>1</sup> I harken back to a law school class motto in my effort to understand the capabilities and intricacies of today's hardware, software, computer memory, and data storage systems in the context of our obligations — and opportunities — as lawyers. For a baby boomer, the developments are astounding. My newly acquired MP3 player holds substantially more data than the mainframe in the computer center when I was in college.

The courts, and we as practitioners, are just now realizing the extent and implications of the new technological era, which has permanently changed our communications, record keeping, data collection, and storage. The fallout is a little scary and can be enormously expensive and divisive for unwary litigants — and litigators. Wall Street brokerage firm Morgan Stanley and its law firm, Kirkland & Ellis LLP, learned this lesson the hard way in a Florida state court in 2005. A jury awarded investor Ronald Perelman \$1.45 billion in a high profile fraud case, arising out of the sale of the Coleman Outdoor Co., against Morgan Stanley in which electronic discovery sanctions played a major role.<sup>2</sup>

Perelman moved for sanctions due to Morgan Stanley's destruction of e-mails and other noncooperative conduct in the course of electronic discovery. Essentially, the court granted the motion, found Morgan Stanley to be grossly negligent in turning over electronic documents, approved an adverse inference instruction due to spoliation, shifted the burden of proof for the fraud claim, and revoked the *pro hac vice* license of defendant's trial lawyer, two weeks before trial.<sup>3</sup> In the midst of this, Morgan Stanley declared it had become clear that the court had "lost all confidence in any statement or representation made" by lawyers for Kirkland & Ellis LLP. Moreover, Morgan Stanley had put the firm on notice of "a potential malpractice claim" arising out of its representation.<sup>4</sup>

If mega law firms and their deep pocket patrons are finding themselves in this much trouble over compliance with electronic discovery, where does that leave lawyers who practice alone or in firms with fewer resources for cost-conscious clients? This article will explore practical suggestions for reducing the risks of noncompliance and capitalizing on the benefits of new technology, following these basic principles:

- Educate yourself on technology and terminology (and/or team up with an expert);
- Know the rules and how the courts are applying them;
- Communicate aggressively and proactively with your clients; and
- Utilize electronic discovery with common sense and creativity.

## A. What are we dealing with?

It is estimated that more than 90 percent of all information generated today is in digital form.<sup>5</sup> Nearly all business activities are computerized. The federal government is mandated by the Government Paperwork Elimination Act (GPEA) to reduce or eliminate paper from its operations. Electronically stored information (ESI) differs from its paper counterpart in volume, location, kind, and volatility.

### 1. Differences in volume

It was estimated that daily e-mail traffic for 2003 was almost equal to annual deliveries by the U.S. Postal Service.<sup>6</sup> If printed, a gigabyte (GB) of ESI would yield an average of 75,000 pages. The average user generates 2 GB of data per year, or 150,000 pages. Assuming 2,500 pages to a banker's box, printing the typical user's annual data output would fill 50 boxes if printed. Responding to a discovery request for a particular custodian's data over a five-year period, as often is done in employment cases, becomes a monumental task.

## 2. Differences in location

Digital data and e-documents can be found in a myriad of locations, both stationary and portable. Servers and computer hard drives (including home PCs) are examples of stationary storage locations. Many transportable devices, including digital telephones, smart cards, flash drives, PDAs, CDs, and DVDs, also generate and/or store digital information. A distinguishing feature of digital information is that, until it is converted to hard copy, it does not exist apart from the medium in which it is stored. And, one must not forget "legacy data" — data that resides on obsolete or replaced equipment. All of this information is capable of being reproduced or copied and can be the object of a properly crafted discovery request in litigation.

## 3. Differences in kind

Metadata and system data have no counterpart in the paper world. Metadata is data about data, often hidden on a computer screen, but easily accessed. Examples include e-mail headers and routing information, word processing profiles and editing history, spreadsheet data sources and formulae, and database structure and relationships. System data is data about the use and operation of a computer system. It can show such things as computer log-ins, access to network resources, use of printer, fax, and other peripherals, as well as use of e-mail and the Internet. The closest counterpart in the paper world would be a filing cabinet filled with indexed hanging files with labeled manila subfolders. Unlike a classic filing system, however, metadata is created automatically.

## 4. Differences in volatility

ESI is far more volatile than paper documents. Data is subject to easy alteration and deletion through overwriting and routine handling. For example, when a Microsoft Office document is copied from one location to another, two of the three operating system time stamps will change such that the header maintains the original date and time

## FOOTNOTES

1. Professor Henry Steiner, First Year Torts 1983, Harvard Law School.

2. 1/19/06 Daily Rec. (Kan. City, Mo.) 2006 SLNR 1129685.

3. *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co. Inc.*, No. CA 03-5045 AF, 2005 WL 679071, at \*3 (Fla. Cir. Ct., 15th Cir. Mar. 1,

2005), 2005 WL 674885, at \*10 (Mar. 23, 2005).

4. <http://www.law.com/jsp/article.jsp?id=1113901509182>.

5. The Sedona Principles: Best Practices, Recommendations, & Principles for Addressing Electronic Document Discovery 11 (The Sedona Conference Working Group Series, July 2005 Version).

6. *Id.* at 14.

while the "creation" and "accessed" time stamps in the operating system reflect the instant it was copied. To the untrained eye the document appears to have been altered.

Many organizations have retention policies under which they purge e-mail and associated electronic documents according to a schedule. Other companies have purchased metadata scrubbing software that removes deletable fields of metadata from files attached to e-mails or residing on the network. Failure to take appropriate measures to secure the integrity of ESI in litigation leads to allegations of destruction of evidence (spoliation), whether intentional or unintentional, and to sanctions for discovery abuse. Scrubbing equates to shredding after there is a reasonable anticipation of litigation.

On the other hand, it can be harder to get rid of ESI than it is to shred a document. "Delete" does not mean "destroy" in the cyber world; it means "ignore" unless a specific utility is employed to truly erase the ESI. The file information remains on the hard drive as "ghost files" or in slack space on the drive. Comput-

ers abhor a vacuum and fill blank space with digital "packing material." This is data left behind from previous files or from active working files. The data is not "saved" on the computer in lay terms, but it remains and can be retrieved years after it was originally created unless and until it is overwritten or forensically removed. Moreover, it can be transferred to other computers as unnoticed baggage during an upgrade or replacement of a computer system.

### B. What do the rules say?

Even without the amendments to Rules 16, 26, 33, 34, 37, and 45 of the Federal Rules of Civil Procedure that went into effect Dec. 1, 2006, it is clear that the scope of discovery encompasses ESI. The U.S. District Court for the District of Kansas has also developed ESI Guidelines<sup>7</sup> that indicate, among other things, counsel should become knowledgeable about their clients' information management systems and operation; include electronic information in Rule 26(a)(1) disclosures; and communicate with opposing counsel about electronic discovery issues, including scope, cost, format, and how to address privileged material. Although ESI has not yet been addressed by Kansas statute or court rule, and although to date there have been no reported cases in the Kansas state courts on this point, it is reasonable to assume that ESI would be included within the scope of Kansas discovery requests and that the federal rules may well be used for guidance when issues arise.

Highlights of the amendments to the federal rules are:

#### 1. Parties must discuss e-discovery issues

Rules 26(f) and 16(b) have been amended to require litigants, at the initial planning and scheduling stage of the litigation, to consider and address electronic discovery issues, including the form of production and the preservation of electronically stored information. At the initial planning conference, the parties' attorneys must discuss:

##### a. Preservation of ESI

Note that this is the first time the concept of preservation has been addressed

by the federal rules. The integrity of metadata, not just the content of the document or system, must be preserved. By this point in the litigation a party should have a preservation plan in place. Information technology (IT) staff or a consultant should be involved to preserve existing information and build in tools to "journal" e-mail on a progressive basis to remove end users' ability to delete before they are captured for preservation.

#### b. Disclosure and discovery of ESI according to the committee notes, topics for discussion include:

- The parties' computer systems (identifying e-mail server, network environment, work stations, peripheral devices, etc.);
- Identity of individuals with special knowledge of the systems (and who may be asked to give a Rule 30(b)(6) deposition);
- Subject matter and time frame of records;
- Source and accessibility; and
- Form(s) of production. What does the form of production mean in this context? "Native format" would involve production in the file format in which it was created, e.g., Microsoft Word as .doc, Excel as .xls, and PowerPoint as .ppt. Native format will include track changes, author notes, etc. By contrast, "static format" would involve converting documents to TIFF (tagged image file format) or PDF (portable document format). The parties can also agree that specified fields of metadata referenced to static images will be produced.

#### c. Inadvertent disclosure

The parties may agree on a protocol for protecting privilege and retrieval of ESI, e.g., so-called "quick peek" and "claw back" agreements.

#### 2. ESI explicitly identified

Rule 34 now adds electronic data as a separate category of information subject to production, even if it never existed as a physical document. Note that in the revised Rule 34 the party requesting production of documents may specify

**HEIRS LOCATED**  
NO FEE TO THE ESTATE



TEL 800 443 9004  
FAX 615 822 9316  
www.tracerusa.com

Box 182  
Madison, TN 37116-0182

Established 1960

<http://www.ksd.uscourts.gov/guidelines/electronicdiscoveryguidelines.pdf>

the form of production, native or static. The producing party may object and specify an alternative form. If the requesting party does not specify a form of production, the responding party must produce ESI in the form in which it is normally maintained (native) or an alternative form, which is reasonably usable. This might include static images linked to identifying fields of metadata. A party must produce ESI in only one form and may not convert from a form in which it is ordinarily maintained to one less usable. Rule 45, applicable to nonparty subpoenas, has been correspondingly revised.

### 3. Retrieval of privileged information

New Rule 26(b)(5)(B) provides a mechanism to seek return of inadvertently produced privileged information. Upon notice, which sets forth the basis for the claim of privilege, the receiving party must return, sequester, or destroy the ESI and take reasonable steps to retrieve it if disseminated. The ESI may be submitted under seal to the court for a ruling. Be aware that this is not a rule of evidence, although there is currently consideration of an amendment to Rule 502 of the Federal Rules of Evidence, which would provide for no waiver in the event of inadvertent production.

### 4. Limited discovery of inaccessible documents

Under the authority of new Rule 26(b)(2)(B), parties need not provide discovery from sources identified as not reasonably accessible unless the other party can show good cause. Evaluation of whether inaccessible ESI must be subject to discovery will take into account issues such as relevance and cost. However, parties must still preserve ESI identified as inaccessible.

### 5. Safe harbor for good faith inadvertent destruction

New Rule 37(f) provides that no sanctions will be imposed where ESI is lost due to routine modification resulting in overriding or deleting data. This protection will only be available to a party that has acted in good faith to prevent destruction of ESI, including intervention with a litigation hold when the notice of the dispute arises.

### 6. Complying with the new rules

As a practical matter attorneys must work first with their client and then the opposing party to consider relevant ESI and develop a discovery and preservation plan at the initial stage of litigation with these goals:

- Preserve relevant information flawlessly;
- Meet and discuss method of preservation;
- Agree on file types with potentially responsive information;
- Propose search terms to identify potentially responsive documents of opposing party;
- Develop an e-discovery protocol that will be endorsed by the court; and
- Identify forms of production, including treatment of redacted documents.

### C. One e-discovery journey through the court system

As of the completion of this article there were no reported Kansas state court e-discovery decisions. However, Kansas practitioners should be aware of several relatively recent e-discovery rulings by our federal judges, which are addressed below in the practical advice section.

There are a growing number of federal and state court decisions throughout the country interpreting the obligations and limits of the discovery rules. The most cited are a scholarly series of opinions

by U.S. District Judge Shira Scheindlin of the Southern District of New York. *Zubulake v. UBS Warburg*<sup>8</sup> started out as a relatively routine single plaintiff employment discrimination lawsuit, although the plaintiff was a very high income employee. Electronic discovery disputes protracted the *Zubulake* litigation for several years. It is an interesting case to explore because its series of opinions covers a wide range of e-discovery challenges and because we know what ultimately happened. With the sanction of an adverse inference instruction for failure to preserve and produce electronic data, the jury returned a verdict for more than \$29 million in compensatory and punitive damages in April 2005.<sup>9</sup> This is a noteworthy employment verdict, even in New York City.

Laura Zubulake worked as an equities trader for UBS. She filed a sex discrimination complaint with the Equal Employment Opportunity Commission (EEOC) and was fired within two months. She sued for discrimination and retaliation.

(continued on next page)



## LAW OFFICES OF SPETH & KING

Suite 230 R.H. Garvey Bldg.  
300 West Douglas  
Wichita, KS 67202

e-mail: slstjk@spethking.kscoxmail.com

◆ 35% Referral Fees

◆ All Expenses Advanced

◆ Settlements or Trial

◆ All types and sizes  
of cases

◆ Proven track record  
of success

PERSONAL INJURY

WRONGFUL DEATH

(316) 264-3333

1-800-266-3345

<sup>8</sup> *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309 (S.D.N.Y. May 13, 2003) (*Zubulake I*) (addressing the legal standard for determining the cost allocation for producing e-mails contained on backup tapes); *Zubulake v. UBS Warburg LLC*, 230 F.R.D. 290 (S.D.N.Y. May 13, 2003) (*Zubulake II*) (not an e-discovery decision); *Zubulake v. UBS Warburg LLC*, 216 F.R.D. 280 (S.D.N.Y. July 2, 2003) (*Zubulake III*) (allocating backup tape restoration costs between Zubulake and UBS); *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212 (S.D.N.Y.

Oct. 22, 2003) (*Zubulake IV*) (reconsidering cost shifting and ordering additional discovery); *Zubulake v. UBS Warburg LLC*, 229 F.R.D. 422 (S.D.N.Y. July 20, 2004) (*Zubulake V*) (sanctioning UBS); *Zubulake v. UBS Warburg LLC*, 231 F.R.D. 159 (S.D.N.Y. Feb. 3, 2005); and *Zubulake v. UBS Warburg LLC*, 382 F. Supp. 2d 536 (S.D.N.Y. March 16, 2005) (excluding evidence).

<sup>9</sup> 4/8/05 *INDY HERALD TRIB.* 17, 2005 WLNR 5506332.

Zubulake requested production of "all documents concerning any communication by or between UBS employees concerning plaintiff." The term "document" in the request was defined to include ESI. In response, UBS produced documents, including 100 pages of e-mails. Zubulake argued that UBS had not been diligent in responding to the document request because she herself had retained and produced approximately 450 responsive e-mail pages. An initial visit to the court resulted in an order that UBS produce for deposition a person with knowledge of its e-mail retention policies in an effort to determine whether backup tapes contained the deleted e-mails and, if so, the burden of producing them.

In *Zubulake I*, Scheindlin held that Rule 34 requires production of electronic documents that are currently in use and also documents that may have been deleted and now reside only on backup disks, so long as they are relevant to claims in the lawsuit. The court found that the disparity in the number of e-mails produced was indication enough that UBS had not searched adequately for ESI.

In *Zubulake I*, the court described the factors to be considered in determining whether to shift the financial burden of electronic discovery. Scheindlin noted the presumption that the responding party must bear the expense of complying with discovery requests and held as a first principle that cost shifting must not be considered in every case involving the discovery of electronic data:

Many courts have automatically assumed that an undue burden or expense may arise simply because electronic evidence is involved. ... This makes no sense. Electronic evidence is frequently cheaper and easier to produce than paper evidence because it can be searched automatically, key words can be run for privilege checks, and the production can be made in electronic form obviating the need for mass photocopying.<sup>10</sup>

The court held that deciding disputes regarding the scope and cost of discovery of electronic data requires a three-step analysis:

*First*, it is necessary to thoroughly understand the responding party's computer system, with respect to active and stored data, considering cost shifting only when electronic data is relatively inaccessible (such as in backup tapes).

*Second*, because the cost shifting analysis is so fact intensive it is necessary to determine what data may be found on the inaccessible media, which may involve requiring the responding party to restore and produce responsive documents from a small sample of disks.

*Third*, in conducting the cost shifting analysis, the following factors should be considered, weighted more or less in this order:

1. The extent to which the request is specifically tailored to discover relevant information;
2. The availability of such information from other sources;
3. The total cost of production, compared to the amount in controversy;
4. The total cost of production, compared to the resources available to each party;
5. The relative ability of each party to control costs and its incentive to do so;
6. The importance of the issues at stake in the litigation; and
7. The relative benefits to the parties of obtaining the information.<sup>11</sup>

Scheindlin held that cost shifting should be considered only when electronic discovery imposes an undue burden or expense on the responding party, specifically when the ESI is in an inaccessible format. Scheindlin generally characterized two categories of documents as inaccessible — backup tapes (which generally employ some sort of data compression making restoration more time consuming and expensive) and erased, fragmented, or damaged data. The court ordered UBS to produce all responsive e-mails from accessible sources at its expense and samples of data from backup tapes at which point the court would conduct a cost shifting analysis.

Approximately two months after the court's decision in *Zubulake I*, the parties returned with the results of the backup tape sampling and UBS renewed a request for cost shifting. In *Zubulake III*, Scheindlin reviewed the cost shifting factors from *Zubulake I* and ordered cost shifting with UBS paying 75 percent and Zubulake 25 percent of the consultants' fees to restore the backup tapes. Significantly, she held that only the costs of restoration and searching be shifted, but not costs of reviewing and producing the documents.<sup>12</sup>

During the restoration effort, the parties discovered that some monthly backup tapes were missing. In addition there was evidence that UBS had deleted some e-mails after the initial EEOC charge, only some of which were available on the backup tapes. Zubulake sought sanctions against UBS for its failure to preserve the missing backup tapes and deleted e-mails. The court in *Zubulake IV* first considered when the obligation to preserve evidence arose, noting that it was when the parties knew or should have known that the evidence may be relevant to future litigation. Although Zubulake's charge of discrimination was not filed until August 2001, the court held the duty to preserve attached in April 2001 because of UBS e-mails predicting a claim by Zubulake. "Once a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a 'litigation hold' to ensure the preservation of relevant documents."<sup>13</sup>

The court found that UBS did not comply with its counsel's directive to retain documents, issued when the charge was first

<sup>10</sup> *Zubulake I*, 2003 WL 2137613, at \*8 (S.D.N.Y. 10/6/03).

<sup>11</sup> Scheindlin notes that the producing party has the exclusive ability to control the costs of reviewing the documents. In this case, UBS decided to use a vendor to have a vendor associate at a top New York City law firm conduct the privilege review at a cost of \$410 per hour.

but the job could just as easily have been done (while perhaps not as well) by a firm or associate or contract attorney at a far lower rate. UBS could similarly have obtained paralegal assistance for far less than \$170 per hour. *Zubulake III*, 2003 WL 2137613, at \*9n.

<sup>13</sup> *Zubulake IV*, 2004 WL 1313, at \*13.

filed, and that UBS had a duty to preserve the backup tapes, which were destroyed. However, the court denied Zubulake's request to reconsider the cost shifting order to require UBS to pay the entire restoration cost. Zubulake also requested the court to order an adverse inference instruction due to the spoliation of evidence. The court denied this request, finding that Zubulake could not demonstrate the lost evidence would have supported her claims. UBS was sanctioned to the extent it was ordered to bear Zubulake's costs for redepositing certain witnesses to inquire into issues related to the missing documentation.

During the redepositions required by *Zubulake IV*, Zubulake learned about additional deleted e-mails and about the existence of previously undisclosed e-mails preserved on UBS' active servers for at least a period of time after the dispute commenced. Some of these e-mails were then produced — nearly two years after the initial requests — and some were lost altogether. This matter was back before the court on Zubulake's renewed request for sanctions.

In *Zubulake V*, Scheindlin determined from evidence presented by the parties that:

- at least one of the alleged perpetrator's e-mails had been lost altogether;
- there were four additional missing backup tapes;
- the alleged perpetrator had deleted e-mails from his active files and not provided them to counsel after counsel's warnings to retain documentation; and
- relevant e-mails had not been timely produced because nobody requested them from UBS employees who had segregated them upon notice of the need to preserve.

The court discussed at length counsel's duty to monitor compliance with a litigation hold order to preserve relevant documents. The court stated that "once a 'litigation hold' is in place, a party and her counsel must make certain that all sources of potentially relevant information are identified and placed on hold."<sup>14</sup> This requires counsel to become fully familiar with the client's document retention policies and data retention architecture. "This will invariably involve speaking with information technology personnel, who can explain system-wide backup procedures and the actual (as opposed to theoretical) implementation of the firm's recycling policy. It will also involve communicating with the 'key players' in the litigation, ... in order to understand how they stored information."<sup>15</sup>

Further, it is not sufficient to notify all employees of a litigation hold and expect that the party will then retain and produce all relevant information. "Counsel must take affirmative steps to monitor compliance so that all sources of discoverable information are identified and searched."<sup>16</sup> Finally, counsel should instruct all employees to produce electronic copies

of their relevant active files and to make sure that all backup media, which the parties are required to retain, is identified and stored in a safe place.

The court found that counsel failed to communicate the litigation hold order to all key players and failed to ascertain each of the key players' document management habits. However, Scheindlin did note that at the end of the day, the duty to preserve and produce documents rests on the party. "Although more diligent action on the part of counsel would have mitigated some of the damage caused by UBS' deletion of e-mails, UBS deleted the e-mails in defiance of explicit instructions not to."<sup>17</sup>

Scheindlin concluded UBS acted willfully and destroyed potentially relevant information and ordered these sanctions:

- *First*, the jury will be given an adverse inference instruction with respect to certain lost e-mails;
- *Second*, UBS is ordered to pay the cost of any depositions or re-depositions required by late production of e-mails; and
- *Third*, UBS is ordered to pay the costs of the motion.<sup>18</sup>

As noted earlier, this case went to trial and, predictably given the adverse inference instruction, resulted in a very high verdict for the plaintiff.

#### D. Practical advice based on case law<sup>19</sup>

##### 1. Yesterday, today, and tomorrow — litigation or no litigation — proactively counsel clients on good electronic document retention practices.

One size certainly does not fit all and the time spent to develop a well-tailored program that can be and is, in actual practice, followed will ultimately pay dividends. Note the amendment to Fed. R. Civ. P. 37, which protects a party from sanctions if electronic information is lost as a result of routine, good-faith operation of its system. That said, once the policy is in place, failure to comply with it could lead to a spoliation finding, an adverse inference instruction, or even dismissal or default judgment. One company found itself under scrutiny for intentional spoliation and privilege waiver under the crime/fraud exception when discovery in a complex patent infringement dispute revealed a retention program featuring "Shred Day" on which employees were rewarded with pizza and beer after destroying some 2 million documents.<sup>20</sup>

The Sedona Guidelines<sup>21</sup> are an excellent and well-reasoned resource on this topic. They were developed by The Sedona Conference think tank, which is comprised of leading jurists, lawyers, experts, and academes. The guidelines themselves, each of which is bulleted by a number of illustrative principles and supported by extensive information, are:

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

<sup>14</sup> *Zubulake V*, 229 F.R.D. at 432.

<sup>15</sup> *Id.* at 432 (emphasis added, footnote omitted).

<sup>16</sup> *Id.* at 432.

<sup>17</sup> *Id.* at 436.

<sup>18</sup> *Id.* at 437.

<sup>19</sup> This is not a comprehensive survey of e-discovery case law, but rather selected case examples to illustrate its recommendations. For a collection of e-discovery cases updated as of Aug. 1, 2005, see Kenneth J.

Withers, Annotated Case Law on Electronic Discovery, [http://www.jlc.gov/public/pdffirst/lookup/ElecDio9.pdf/\\$file/elecDio9.pdf](http://www.jlc.gov/public/pdffirst/lookup/ElecDio9.pdf/$file/elecDio9.pdf).

<sup>20</sup> *Rambus Inc. v. Infineon Technologies AG*, 220 F.R.D. 264 (F.D. Va. 2004).

<sup>21</sup> The Sedona Guidelines, Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age (The Sedona Conference Working Group Series, September 2005).

- b. An organization's information and records management policies and procedures should be realistic, practical, and tailored to the circumstances of the organization.
- c. An organization need not retain all electronic information ever generated or received.
- d. 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.
- e. 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.

**2. Communicate aggressively and proactively with your clients.**

- a. **The moment you are aware of a dispute (from receipt of demand letter to service of complaint), notify the client in writing of the duty to preserve and institute a litigation hold.**

Even if your client is a sophisticated business, it is not safe to assume they will implement a litigation hold without your guidance and the consequences could be severe. For example, in *MasterCard International Inc. v. Moulton*,<sup>22</sup> the defendant failed to preserve e-mails until five months after a lawsuit for trademark infringement was filed despite knowledge of the lawsuit and a pending discovery request. The plaintiff moved

for spoliation sanctions. The court held the defendant did not act in bad faith in deleting the e-mails but was grossly negligent. Although the plaintiff did not meet a burden to show the potential significance of the e-mails sufficient to warrant ruling certain key issues conclusively established, an adverse inference instruction was deemed an appropriate sanction.

*Zubulake V* clearly places a burden on counsel to take steps to prevent a client's intentional or inadvertent destruction of electronic evidence. If and when you are faced with defending a Fed. R. Civ. P.30(b)(6) or K.S.A. § 60-230(b)(5) deposition of the client designee on the issue of records retention policies and efforts to preserve, a motion to compel, or another form of scrutiny, your own conduct may be subject to examination.

**b. Be persistent in learning a client's practices, systems, and retention policies and practices.**

How many times has a client said, "That's all we have," and that little voice in your head is pestering you, wondering if that's really true? While attorneys cannot be guarantors of their client's conduct, a superficial effort to ensure compliance is not adequate to protect the client or yourself. The courts are increasingly dismissive of pleas of ignorance. In *Anderson v. Crossroads Capital Partners LLC*,<sup>23</sup> the court was unimpressed by a plaintiff in a sexual harassment case whose computer was made available for examination by the defendant's expert. Although she claimed it was the computer she used at the time in question, the expert determined it was manufactured two years later. Additionally, she had installed and run a file-wiping program, which she claimed was not intended to destroy evidence. The judge found the plaintiff's "exceedingly tedious and disingenuous claim of naïveté ... defies the bounds of reason."<sup>24</sup>

Insist upon early access to a business client's information systems or technology (IS or IT) department to gain a better understanding about their systems and practices. Particularly if you represent an individual or small business, consider utilizing a consultant if you don't have the expertise in your office. A recommended practice is requiring the client to complete a questionnaire about its practices and the identity of its key individuals, and then return it to you with copies of relevant policies.

Make sure the client understands that the litigation hold or preservation order might require disabling routine e-mail deletion practices. In *United States v. Philip Morris USA Inc.*,<sup>25</sup> Philip Morris USA was fined a total of \$2.75 million — \$250,000 for each of 11 officers and managers who, for two years after a blanket data-preservation order was entered, continued their routine practice of deleting e-mail more than 60 days old. The 11 were also prohibited from testifying.

Thanks to the addition of  
Martie Ross, our health care  
practice has never  
**felt better.**



Martie Ross

Lathrop & Gage is proud to announce Martie Ross has moved from Wichita to join our Overland Park office. Our interdisciplinary health law department offers clients comprehensive legal representation. Martie's addition makes our health care practice — the largest in the region — even stronger.



BOULDER • DENVER • JEFFERSON CITY • KANSAS CITY • NEW YORK  
OVERLAND PARK • SPRINGFIELD • ST. LOUIS • WASHINGTON, D.C.  
913.451.5100 • WWW.LATHROPGAGE.COM

22. No. 03-Cv-43613, 2004 WL 4393992 (S.D.N.Y. June 22, 2004).

23. No. Civ. 01-2090, 2004 WL 256512 (D. Minn. Feb. 10, 2004).

24. *Id.* at 8.

25. 327 F. Supp. 2d 21 (D.D.C. 2004).

**c. Take responsibility for making sure the information gets to everybody who needs to know.**

Certainly *Zubulake V*, where a number of managers got the message to preserve data but were never asked to turn it over, illustrates the importance of diligently communicating requirements and monitoring compliance. In an ERISA class action case, *Keir v. Unumprovident Corp.*,<sup>26</sup> the failure to involve IT staff in the negotiation of a data preservation order, followed by a relatively short delay (two weeks) between entry of the order and communication to IT staff, caused the loss of a fair bit of data. This unintentional failure to preserve was criticized by the court, which recommended the parties retain an expert to determine the full extent of the loss.

In *re Prudential Insurance Co. of America Sales Practices Litigation*<sup>27</sup> was another case involving an ineffective method of communicating a preservation order requiring preservation of certain sales data. It led to widespread destruction of evidence and sanctions, including a \$1 million fine, attorneys' fees award, and an adverse inference. Specifically, the instruction was issued by bulk e-mail, typically ignored by the sales people who had to comply.

In *Metropolitan Opera Association Inc. v. Local 100, Hotel Employees and Restaurant Employees International Union*,<sup>28</sup> failures in communication compounded by counsel's misrepresentations to the court resulted in evidence destruction, including replacement of computers subject to discovery shortly before an on-site inspection. The end result? Judgment was entered against the defendant and attorneys' fees awarded.

**d. Effectively communicate the consequences of active refusal to cooperate, carelessness, flippancy, and spoliation to clients.**

Counsel should advise their clients that intentional or accidental destruction of data, failure to adequately search, or misrepresentation about the efforts or data can result in sanctions ranging from fines, to payment of attorneys' fees, to an adverse inference instruction, or even judgment. This may help motivate cooperation and avoid unpleasant surprises.

Case law varies on the standard for issuing sanctions. For example, the 8th U.S. Circuit Court of Appeals requires a finding of "intentional destruction indicating a desire to suppress the truth" before spoliation will yield an adverse inference instruction. *Morris v. Union Pacific Railroad*.<sup>29</sup> The 2nd U.S. Circuit Court of Appeals gives trial judges discretion to consider "purposeful sluggishness" leading to destruction of discoverable data to be equal to spoliation.<sup>30</sup>

**e. Take heed of metadata.**

Recently, U.S. Magistrate Judge David J. Waxse, District of Kansas, ordered a party to produce the metadata for spreadsheets responsive to discovery requests in *Williams v. Sprint/United Management Co.*<sup>31</sup> As noted above, metadata is information describing the history, tracking, or management of an electronic document. It may include file names, file locations, file type, dates and authors of the document, changes and modification dates, print-out dates, and names of recipients. Metadata may be altered intentionally or inadvertently and can be inaccurate in some circumstances, such as when a form document reflects the author as the template author rather than the drafting author.

When ordered to produce spreadsheets in the electronic form in which they were maintained, Sprint used special software to "scrub" the spreadsheets and remove the metadata, arguing that the metadata removed was irrelevant and contained privileged information. Sprint also argued that plaintiffs had never specifically requested the spreadsheets be produced with the metadata intact. Waxse held, however, that an order to produce electronic data "in the manner in which it was maintained" did not allow for the scrubbing of metadata prior to production.<sup>32</sup>

(continued on next page)

**GTrust**  
**Security for Generations**  
 An Independent Trust Company



**Unparalleled Competence**  
**Uncompromising Integrity**  
**Client-Centered Approach**



**EXPERT FEE-ONLY SERVICES INCLUDE:**

**INVESTMENT MANAGEMENT**  
**ADMINISTRATION OF LIVING TRUSTS**  
**FINANCIAL PLANNING**  
**RETIREMENT PLAN ADMINISTRATION**  
**CONSERVATORSHIPS**  
**STRUCTURED SETTLEMENTS**



*We are proud to be the Investment Manager  
 for the Kansas Bar Foundation*

**TOPEKA • OVERLAND PARK • WICHITA • LARNED**  
**785.273.9993 • SECURITY@GTRUST.COM**  
**WWW.GTRUST.COM**

26 No. 02-Cv-8781-2003-WL-21997747 (S.D.N.Y. Aug. 22, 2003).

27 306 F.3d 99, 110 (2nd Cir. 2002).

28 212 F.R.D. 173 (S.D.N.Y. 2003).

29 373 F.3d 896, 901 (8th Cir. 2004).

30 *Residential Funding Corp. v. DeGeorge Financial Corp.* 306 F.3d 99, 110 (2d Cir. 2002).

31 230 F.R.D. 640 (D. Kan. 2005).

32 *Id.* at 656.

The court's ruling relied heavily on the Federal Rules of Civil Procedure and the (then proposed) amendments, The Sedona Guidelines and the scant available case law regarding discovery of metadata. Significantly, Waxse held that:

When a party is ordered to produce electronic documents as they are maintained in the ordinary course of business ... the producing party should produce the electronic documents with their metadata intact, unless the party timely objects to production of the metadata, the parties agree that the metadata should not be produced, or the production party requests a protective order.<sup>33</sup>

The *Williams* opinion places the burden of objecting to production of metadata on the responding party. Appropriate objections to the production of metadata may be relevancy or an objection based upon the work-product and/or attorney-client privilege.<sup>34</sup>

In *Williams*, the producing party also "locked" the spreadsheets' cells and data, reportedly to ensure the integrity and prevent accidental or intentional alteration of the data. The court held there were more appropriate ways to ensure data integrity exists, suggesting as an example that the producing party could have run the data through a mathematical process to generate a "hash mark," thereby creating the digital equivalent of a tamper-proof seal.<sup>35</sup>

### 3. Utilize e-discovery with commonsense and creativity.

#### a. Notify the opposing party of anticipated electronic discovery at the outset.

At the commencement of a dispute, it is wise to evaluate the relevant electronic information you will seek and advise the other side. This can take the form of a "no spoliation" letter, reminding the party that it has a duty to retain relevant

electronic data. The letter will be more effective in securing compliance and, if necessary, later moving to compel or for sanctions if it is narrowly and specifically tailored to material issues in the litigation.

#### b. Be prepared for a cost/benefit analysis whether you are seeking discovery or objecting to a response.

*Zubulake I* identifies cost shifting factors. Other courts have adopted similar factors, sometimes weighting them differently.<sup>36</sup>

As Schindlein noted in *Zubulake I*, it is not necessarily true that electronic discovery is more costly than traditional paper review. However, it can be, especially when requiring expert assistance to restore "inaccessible" data or review computers and disks for deleted information. These costs should be taken into account when determining the scope of your discovery.

On the "benefits" side of the analysis, a party should have some support for a belief that relevant information will be uncovered. A plaintiff in an employment discrimination case contended there was a discriminatory e-mail but could not produce a copy of it. When defendant reported there was no such e-mail, plaintiff sought to have the court appoint a special master to conduct a forensic examination of the defendant's computer system. The court denied the motion noting that the plaintiff's belief of the existence of the e-mail was "at best [a] highly speculative conjecture."<sup>37</sup> Similarly, in *Byers v. Illinois State Police*,<sup>38</sup> plaintiffs in a sex discrimination case requested discovery of e-mail backup tapes going back eight years. The court determined a cost/benefit analysis was necessary due to the enormous volume and substantial cost, found plaintiffs had not adequately shown the e-mails would support their case, and ordered the plaintiffs to bear the costs of licensing the defendant's old e-mail program.

In another case the court directed a plaintiff, seeking discovery about a data entry she claims she made in the defendant's computer system before she was discharged, to file a motion to compel if and when she was willing to retain a forensic computer expert at her own expense.<sup>39</sup>

The volume of information available can also increase costs. Out of an abundance of caution, and not wanting to leave any stone unturned, lawyers often make sweeping production requests for "any and all documents in any way whatsoever related at all to ..." Be careful what you ask for — you might get it. A defendant in an unfair trade practices case requested "[a]ll documents, including but not limited to internal memoranda, internal e-mails, and correspondence with [IBM] or any other entity or person, referring or relating to actual or potential effects on Compuware's business of any past, present, future, or contemplated conduct by IBM." After initially objecting that the request was overbroad, the plaintiff responded by producing all of the requested documents, estimated in the "tens of millions," on compact disks. Arguing that the production was overbroad, the plaintiff asked the judge to narrow the scope of its own request and order the defendant to index the documents on the CDs and designate those that were relevant to the subject matter of the dispute. The court denied the request.<sup>40</sup>

Also consider potential long term ramifications, even if you are successful in getting costs shifted to responding parties. One court held costs of searching computer databases should be shared evenly by the party, but would be classified as court costs, making them recoverable by the prevailing party.<sup>41</sup>

33. *Id.* at 652 (footnotes omitted).

34. *Id.* at 653-54.

35. *Id.* at 655.

36. See e.g. *Rowe Entmt' Inc. v. William Morris Agency Inc.*, 205 F.R.D. 421 (S.D.N.Y. 2002); *Wiginton v. CB Richard Ellis Inc.*, 229 F.R.D. 568 (N.D. Ill. 2004).

37. *Williams v. Mass. Mutual Life Ins. Co.*, 226 F.R.D. 144, 146 (D. Mass. 2005).

38. 53 Fed. R. Serv. 3d 740 (N.D. Ill. June 3, 2002) (mem.).

39. *Laurin v. Pokoik*, No. 02 Civ. 1938, 2004 WL 2724767, at \* (S.D.N.Y. Nov. 30, 2004).

40. *Compuware Corp. v. Moody's Investors Services Inc.*, 2004 WL 2931401, at \*2 (E.D. Mich. Dec. 15, 2004).

41. *Multitechnology Services L.P. v. Verizon Southwest*, 2004 WL 1553480, at \*2 (N.D. Tex. July 12, 2004).

### c. Come to court with the cleanest hands possible.

Amended Fed. R. Civ. P. 37 will not only provide some protection for good faith efforts, but it will also help a party who has been diligent fare better when seeking the assistance of the court. For example, in *Marcin Engineering LLC v. Founders at Grizzly Ranch LLC*,<sup>42</sup> a defendant's motion for extension of time for discovery of the plaintiff's expert's work was denied. The court noted the motion had not been brought until five days before the deadline after defendant had delayed for five months reviewing the materials originally produced. Such delay and carelessness in requesting electronic discovery was, according to the court, not compatible with the showings of diligence and good cause necessary to extend discovery deadlines. The court also noted that it had repeatedly advised defendant that the proposed discovery, "when considered in the light of the amounts claimed as damages, made no economic sense."<sup>43</sup>

In *Super Film of America Inc. v. UCB Films Inc.*,<sup>44</sup> defendant had requested discovery of e-mails, documents, databases, and spreadsheets. Claiming it was beyond its knowledge and expertise to retrieve and produce these documents, plaintiff proposed that defendant could access its computers and retrieve data itself. The defendant objected and the court agreed the offer was an unreasonable attempt to shift discovery costs from the responding to the requesting party. The court rejected plaintiff's claim that providing the discovery was burdensome and granted defendant's motion for the discovery.

### d. Consider offensive use

A defendant in a trade secrets action was successful on a summary judgment motion by presenting evidence from its own independent expert that a review of defendant's computer systems revealed no evidence, including remnants, of the proprietary software plaintiff claimed had been stolen. The court held that where plaintiff did not conduct its own

discovery into defendant's system, its circumstantial evidence was not sufficient to meet its burden of proof.<sup>45</sup>

### e. Conduct discovery about computer systems and retention programs.

This approach certainly paid off in the *Rombus* case noted above, where the retention policy included a "Shred Day." In *Sonnino v. University of Kansas Hospital Authority*,<sup>46</sup> Waxse overruled defendant's objection to an interrogatory seeking information about its computer and e-mail systems. In addition to interrogatories and document requests, consider noticing a deposition of party designees who can describe the computer systems from data management to e-mail, types of hardware and software, retention policies (and practices which may be different), and efforts to comply with discovery requests in the case.

### f. Take special precautions to preserve privilege and protect privacy.

Electronic data presents new challenges in the protection of privileged information and work product. The amendments to Fed. R. Civ. P.26(f) and 16(b) encourage the parties to set a process for inadvertent disclosures, but, absent those, a party might waive privilege and unnecessarily expose that information to scrutiny. One court found waiver when a party failed to timely identify a particular printout of customer contacts. The party argued the document was not generated until after the log was due, but the court held the failure to identify the database from which the printout was made would be deemed waiver.<sup>47</sup>

U.S. Magistrate Judge James P. O'Hara, District of Kansas, addressed the issue of properly identifying e-mail chains in a privilege log in *In re Universal Service Fund Telephone Billing Practices Litigation*.<sup>48</sup> Defendant AT&T had developed a privilege log that was the subject of a motion to compel and that the court found to be deficient as a result of an overly aggressive, impru-

dent litigation tactic.<sup>49</sup> O'Hara rejected AT&T's position that a single identification of an e-mail strand or string of e-mails on a particular subject is sufficient as to all the individual communications it contains. Noting that "electronic discovery is a rapidly evolving area in which litigants (and judges) often have little or conflicting guidance,"<sup>50</sup> the court relied on well-established case law regarding privileges and privilege logs, as well as the "obvious and unavoidable byproduct of the rule advanced by AT&T would be stealth claims of privilege, which, by their very nature, could never be the subject of a meaningful challenge by opposing counsel or actual scrutiny by a judge ..." rendering Rule 26(b)(5) a nullity.<sup>51</sup> The court did hold that in this case no blanket waiver of privilege would be declared, but went on to require production of a number of the e-mails contained within strands listed on the privilege log.

The volume of electronic information can be overwhelming to review and the ability to easily "cc" or "bcc" anyone and everyone on e-mail may require close review of many nonprotected documents. Generally the courts are not shifting the costs of review for privilege.<sup>52</sup>

As we gain access to electronic records, perhaps especially e-mail, it is also important to consider individual privacy interests. A computer forensic expert once told me he could ferret out multiple affairs in just about any company in an hour on the computer system. We need to take steps to avoid disclosure unnecessarily of individual's medical, financial and other personal information, as well as social security numbers.

### g. Don't sign your name when you're not sure.

Extra caution in ensuring compliance with ethics rules K.S.A. § 60-211 and Fed. R. Civ. P.11 is warranted when making commitments about electronic discovery. More than one lawyer has suffered credibility damage — and worse — having been misled by a client or simply been too relaxed about confirm-

42. 219 F.R.D. 516 (D. Colo. 2003)

43. *Id.* at 526

44. 219 F.R.D. 649 (D. Kan. 2004)

45. *Tempco Electric Heater Corp. v. Temperature Engineering Co.*, 2004 WL 1254134, at \*10 (N.D. Ill. June 3, 2004)

46. 220 F.R.D. 633, 655 (D. Kan. 2004)

47. *S.E.C. v. Beacon Hill Asset Management LLC*, 231 F.R.D. 134

(S.D.N.Y. 2004)

48. 232 F.R.D. 669 (D. Kan. 2005)

49. *Id.* at 671

50. *Id.* at 672

51. *Id.* at 673

52. *Supra* note 12

ing information. Press clients for accurate information about document availability.

This admonition extends to serving as local counsel. Do you trust the primary, out of state counsel enough to take the risk of representations to the tribunal about the completeness of e-disclosures? If not, insist upon undertaking your own investigation or consider withdrawing if refused. We should always be concerned about this role, but this is an area of greater risk and less developed means of risk avoidance than more traditional aspects of representation.

## II. Conclusion

Electronic discovery provides us with both obligations and opportunities. Use it creatively but not with a scorched earth mentality. Focus the available time (your's and the client's) and money on evidence significant to the case. The access to such a greater depth and breadth of information should be exercised with an eye to professionalism, civility, and client resources. ■

### About the Authors

*Kathy Perkins is a managing member in the Kansas City, Mo., office of Constangy, Brooks & Smith LLC. Perkins represents employers in all aspects of employment law and has more than 20 years of experience in this area. She received her juris doctorate from Harvard University in 1983 and her B.S. in civil engineering from Kansas State University. She is a frequent speaker and published author on employment law subjects. Perkins is admitted to practice in Kansas, Missouri, the District of Columbia, and Idaho.*

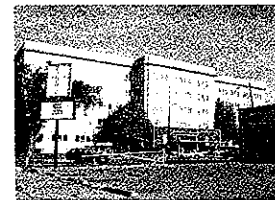


*Dave Deppe is a founding partner of Focus Legal Solutions, a national litigation support company. Deppe is responsible for the management of forensic data collections and e-discovery productions nationwide. He has managed national data collections for Fortune 500 companies, governmental agencies, and top 50 national law firms. Deppe participated as an electronic discovery expert for Western Union and First Data Corp. in a matter with the Networks and Technology division of the U. S. Department of Justice in Denver. He has also provided expert testimony on behalf of several Kansas and Missouri law firms. Deppe's experience has given him the unusual ability to mesh the legal requirements of discovery with practical, efficient technological solutions.*



**\* Office space available for lease\***

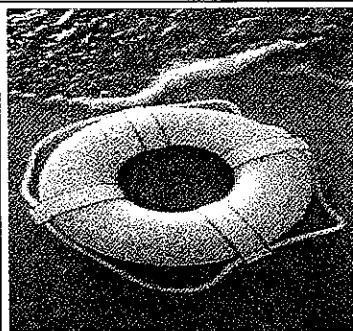
**Call for details**



**Independence Corporate Offices**

**Independence, Kansas**

**866-667-0995**



## Kansas Bar Association Members:

Take Advantage of Premium Discounts

Up to 30%

on Individual Disability Income Insurance from  
Principal Life Insurance Company

During the course of your career, you are 3 1/2 times more likely to be injured and need disability coverage than you are to die. (Health Insurance Association of America, 2000)

The Verdict is in: **You and Principal Life are a winning combination.**

**For More Information Contact:**

**Jason Heffner, Financial Representative**

The Principal Financial Group  
7300 West 110<sup>th</sup> Street, Suite 620  
Overland Park, Kansas 66210

**Phone:** 800-245-8895, ext. 3533

**E-mail:** [Heffner.Jason@principal.com](mailto:Heffner.Jason@principal.com)

Insurance issued by Principal Life Insurance Company, a member of the  
Principal Financial Group®, Des Moines, IA 50392.

#4093062008

# THE JOURNAL

of the Kansas Bar Association  
March 2007 • Volume 76 • No. 3



**"BYTE" ME!**  
**Protecting Your Backside in an  
Electronic Discovery World  
(Not Just for Litigators)**

PHOTO: JEFFREY M. HARRIS