

Digital Discovery & e-Evidence

BEST PRACTICES & EVOLVING LAW

Vol. 3, No. 11 | November 2003

Zubulake Not Entitled to Adverse Inference Instruction

The fourth opinion addressing discovery issues arising from a gender discrimination case that is apparently setting the standard for e-discovery practice focuses on the scope of a litigant's duty to preserve electronic documents and the consequences of failing to preserve documents that fall within the scope of that duty. *Zubulake v. UBS Warburg*, ___ F.R.D. ___, 2003 WL 22410619 (S.D. N.Y., decided October 22). The court holds that the employer had a duty to preserve backup tapes containing potentially relevant e-mails of key employees and would be required to pay the costs of certain depositions required to develop evidence arising out of the tapes' destruction. Judge Shira Scheindlin refuses, however, to reconsider her earlier order allocating the costs of restoring the backup tapes between the parties or to grant the plaintiff's motion for an adverse inference instruction.

The Underlying Case

Since the *Zubulake* saga has been covered extensively since it began (see *DDEE*, June 2003, p. 1 and August 2003, p. 1), Judge Scheindlin provides only this brief recitation of the facts and procedural history: "Laura Zubulake, an equities trader who earned approximately \$650,000 a year with UBS, is suing UBS for gender discrimination, failure to promote, and retaliation under federal, state, and city law. She has

repeatedly maintained that the evidence she needs to prove her case exists in e-mail correspondence sent among various UBS employees and stored only on UBS's computer systems. On July 24, 2003, I ordered the parties to share the costs of restoring certain UBS backup tapes that contained e-mails relevant to Zubulake's claims. In the restoration effort, the parties discovered that certain backup tapes are missing. . . . In addition, certain isolated e-mails—created after UBS supposedly began retaining all relevant e-mails—were deleted from UBS's system, although they appear to have been saved on the backup tapes. . . . Zubulake now seeks sanctions against UBS for its failure to preserve the missing backup tapes and deleted e-mails. In particular, Zubulake seeks the following relief: (a) an order requiring UBS to pay in full the costs of restoring the remainder of the monthly backup tapes; (b) an adverse inference instruction against UBS with respect to the backup tapes that are missing; and (c) an order directing UBS to bear the costs of re-deposing certain individuals . . . concerning the issues raised in newly produced e-mails."

Preservation Duty: What and When

The court's analysis begins with an exploration of the extent of a party's duty to preserve evidence, for a party

Inside

- 3-8 Cases:** Attorney E-mail Forwarded to Martha Stewart's Daughter Retains Privilege • *Zubulake* Factors Disfavor Cost-shifting in Securities Dispute • Defendants Must Return Documents Inadvertently Copied to Hard Drive Evidence • Judge Chastises Party for Inadvertent Erasure of E-mail Backup
- 9 Book Review:** *Elements of Electronic Discovery* • *Electronic Discovery and Evidence*
- 11 Talking Tech:** Electronic Format Clearly Superior for E-mail Production
- 14 Vendor News:** Kroll-Ontrack Offers E-discovery Specialist Certification Course
- 15 Calendar**

can only be sanctioned for destroying evidence if it had a duty to preserve it. Relying on *Fujitsu Ltd. v. Federal Express Corp.*, 247 F.3d 423 (2d Cir. 2001) and *Kronish v. United States*, 150 F.3d 112 (2d Cir. 1998), Judge Scheindlin asserts that the obligation to preserve evidence arises when the party has notice that the evidence is relevant to litigation or when a party should have known that evidence may be relevant to future litigation. Here, the duty to

continued on page 2

preserve arose at the latest on August 16, 2001, when Zubulake filed a charge with the Equal Employment Opportunity Commission. To their credit, at that time UBS in-house counsel instructed employees to retain all documents, including e-mails and backup tapes that could be relevant to Zubulake's claim. Evidence in the form of e-mails, however, demonstrates that almost everyone associated with Zubulake recognized the possibility that she might sue as early as April 2001. Accordingly, that is the trigger date on which UBS's duty to preserve attached.

But what was the scope of that duty? Citing *Concord Boat Corp. v. Brunswick Corp.*, 1997 WL 3335279 (E.D. Ark.), Aug. 29, 1997, and *The Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Discovery cmt. 6.h* (Sedona Conference Working Group Series 2003, see *DDEE*, April 2003, p. 1), Judge Scheindlin flatly states that it does not extend to preserving all backup tapes even when litigation is reasonably anticipated. It does, however, "certainly extend to any documents or tangible things (as de-

finied by [Fed.R.Civ.P.] 34(a), made by individuals likely to have discoverable information that the disclosing party may use to support its claims or defenses. The duty also includes documents prepared for those individuals ... [and to] information that is relevant to the claims or defenses of any party, or which is relevant to the subject matter involved in the action" (emphasis in original). Unfortunately for UBS, all the individuals whose backup tapes were lost fall into this "key player" category.

Preservation Procedure

Judge Scheindlin acknowledges that there are many ways to manage electronic data, leaving it to the litigants to choose a method for accomplishing this task. UBS, however, could have created a complete set of relevant documents by retaining all backup tapes that existed for the relevant personnel as of the April 2001 trigger date, cataloging any later-created documents in a separate electronic file, and taking a mirror-image of the computer system on the trigger date. She offers the following summary of a party's preservation obligation:

Once a party reasonably antici-

pates litigation, it must suspend its routine document retention/destruction policy and put in place a "litigation hold" to ensure the preservation of relevant documents. As a general rule, that litigation hold does not apply to inaccessible backup tapes (e.g., those typically maintained solely for the purpose of disaster recovery), which may continue to be recycled on the schedule set forth in the company's policy. On the other hand, if backup tapes are accessible (i.e., actively used for information retrieval), then such tapes would likely be subject to litigation hold.

She posits one exception to this general rule: if a company can identify where particular employee documents are stored on the backup tapes, then the tapes storing the "key players" documents should be preserved.

Sanctions

Despite issuing an appropriate preservation directive, the UBS employees did not comply with it, and three backup

Digital Discovery
 & e-Evidence
www.pf.com/digitaldisc.asp

Managing Editor , Carol L. Eoannou	800/255-8131 ext. 269 (ceoannou@pf.com)
Legal Editor , Robert Emeritz	800/255-8131 ext. 258 (remeritz@pf.com)
News Editor , Scott Sleek	800/255-8131 ext. 291 (ssleek@pf.com)
Contributing Editor , Faith Ruderfer	800/255-8131 ext. 288 (fruderfer@pf.com)
Group Publisher , Meg Hargreaves	800/255-8131 ext. 229 (mhargreaves@pf.com)

Copy Editor, Marie Unger; **Layout and Design Manager**, Jennifer Andruzzi

Published monthly, except for August. ISSN: 1537-5099
 Subscription rate: \$549
 © Copyright ©2003 Pike & Fischer, Inc. All rights reserved.

POSTMASTER: Send address changes to: *Digital Discovery*, Pike & Fischer, Inc., 1010 Wayne Avenue, Suite 1400, Silver Spring, MD 20910

Disclaimer: Pike & Fischer, Inc., has created this publication to provide you with accurate, concise and authoritative information on developments in electronic evidence and discovery. However, the information in this publication should not be interpreted as legal advice, and should not be used as a substitute for advice from an attorney. Pike & Fischer is not responsible for any claim, liability, or damage related to the use of information in *Digital Discovery & e-Evidence*. Also, the views expressed by outside authors do not necessarily represent the views of Pike & Fischer.

Publisher: Pike & Fischer, Inc., a subsidiary of The Bureau of National Affairs, Inc., 1010 Wayne Avenue, Suite 1400, Silver Spring, MD 20910

No reproductions may be made without prior written authorization from Pike & Fischer, nor shall this information, either in whole or in part, be redistributed or put into a computer without the prior written permission of Pike & Fischer.

tapes containing the e-mail of the four key players in the litigation were lost, along with two others that were not the subject of any preservation directive until August 2002, when Zubulake made a discovery request.

To punish UBS for this loss, Zubulake has asked the court to reconsider its July 24, 2003 order, which allocated the costs of restoring the backup tapes 75 percent to UBS and 25 percent to Zubulake. Judge Scheindlin rejects this option, as she factored in the lost tapes and deleted e-mails in rendering her original decision on cost-shifting.

The court similarly rejects

Zubulake's petition that the jury be instructed that it can infer from the fact that UBS destroyed certain evidence that the evidence, if available, would have been favorable to Zubulake and harmful to UBS. Characterizing the adverse inference instruction as an extreme sanction that should not be given lightly, the court finds that UBS had and breached a duty to preserve the backup tapes at issue and was grossly negligent, if not reckless, in failing to do so. However, in order to be granted an adverse instruction, Zubulake must also demonstrate that a reasonable trier of fact could find that the missing e-mails

would support her claims. Since there is no reason to believe that peculiarly unfavorable evidence resides solely on the missing tapes, which were a small portion of the materials that UBS produced, Zubulake did not satisfy her burden of demonstrating that the lost tapes contained relevant information. UBS, however, is not immunized from culpability for destroying e-mails that should have been produced to Zubulake. It is ordered to bear the costs of depositions of various witnesses to explore the issues raised by the destruction of evidence and any newly-discovered evidence.

— C. Eoannou

Cases

Work Product Privilege

E-mail to Attorney Forwarded to Client's Daughter Retains Privilege

United States v. Martha Stewart, No. 03 Cr. 717 (MGC), S.D. N.Y., decided October 20.

An e-mail that Martha Stewart originally sent to her attorney while she was the subject of a grand jury investigation is protected work product, and its immunity was not waived when Stewart forwarded the document to her adult daughter. The court finds that the e-mail was created in preparation for litigation and its disclosure did not substantially increase the opportunities for potential adversaries to obtain the information.

Judge Miriam Goldman Cedarbaum's opinion is the latest round in the action arising from media mogul Stewart's alleged misuse of inside information to sell stock of ImClone Systems Inc. the day before the company's lead product was denied FDA approval. Stewart composed the e-mail on June 23, 2002, approximately six months after the stock sale and the launch of the government's investigation of it. It contained Stewart's account of the facts relating to her sale of ImClone stock, and was sent originally to one of her attorneys. The following day, Stewart retrieved the e-mail from her own e-mail account, and forwarded an unchanged copy to her adult daughter.

The grand jury that was convened to investigate the ImClone stock sale issued a subpoena on August 12, 2002 seeking documents from Stewart relating to the sale and

"all desktop and laptop computers used by Stewart" and her employees. The parties negotiated terms of compliance that required Stewart to provide the requested computers and files to the grand jury and the government to refrain from reviewing the files until Stewart identified the documents that were responsive to the subpoena. Stewart also agreed to provide privilege logs, one reflecting documents that existed as hard copies, and one reflecting documents that were computer files. The June 23 and 24 e-mails are listed on the log of hard copy privileged documents as one entry, and the attorney-client privilege is asserted for them. The June 23 e-mail (to the attorney) appears on the log of privileged computer files, but the June 24 copy to the daughter does not.

After the grand jury returned an indictment against Stewart on June 4, 2003, an Assistant United States Attorney (AUSA) discovered the June 24 e-mail to the daughter in the course of preparing for trial. The documents apparently were never reviewed in the course of the grand jury investigation and the AUSA was unaware of the terms for production that the parties had negotiated.

Stewart objected to production of the June 24 e-mail, maintaining that it was protected by the attorney-client and work product privileges, neither of which Stewart waived by forwarding the e-mail to her daughter.

Attorney-Client Privilege

The court finds that the June 23 e-mail to the attorney was clearly protected by the attorney-client privilege, as it fell squarely within the parameters of *In re Grand Jury Sub-*

poena Duces Tecum Dated September 15, 1983, 731 F.2d 1032, 1036 (2d Cir. 1984). That case held: “(1) where legal advice of any kind is sought (2) from a professional legal advisor in his capacity as such, (3) the communications relating to that purpose, (4) made in confidence, (5) by the client, (6) are at his instance permanently protected (7) from disclosure by himself or by the legal advisor, (8) except the protection be waived.” Sadly for Stewart, apart from a few recognized exceptions, disclosure to third parties of attorney-client privileged materials results in a waiver of that privilege. No exception was applicable to the disclosure to the daughter, so the court finds that Stewart waived the attorney client privilege.

Work Product Privilege

Stewart fares better with her assertion that the e-mail was work product, even though it arose in the unusual context of the forwarding of a purportedly work product-protected document to a nonlawyer family member whose interest in the case were purely personal. The Second Circuit followed Fed. R. Civ. P. 26(b)(3) when it stated that a document acquires work product protection if it “was created because of anticipated litigation, and would not have been prepared in substantially similar form but for the prospect of that litigation.” The e-mail fits comfortably within that definition. Moreover, the Supreme Court has asserted that work product protections are “even more vital” in criminal matters, and suggests that protection in the grand jury context should be, at the very least, no weaker than in others.”

Against this backdrop, the court is persuaded that it is sufficient for purposes of work product that Stewart prepared the e-mail in response to her attorneys’ ongoing requests for factual information in the furtherance of their legal representation. And since waiver of the work product privilege has been found only when the disclosure “substantially increased the opportunities for potential adversaries to obtain the information,” copying the e-mail to the daughter did not constitute waiver. The court concludes, “The disclosure affected neither side’s interest in this litigation: it did not evince an intent on Stewart’s part to relinquish work product immunity for the document, and it did not prejudice the government by offering Stewart some litigation-based advantage.”

Finally, the e-mail’s defective listing on the privilege log was irrelevant to the issue of work product waiver. The court observes that both sides in this matter made errors in the process of producing and reviewing documents, and the problems with the privilege log do not merit a finding that Stewart waived any privilege.

Cost Allocation

Zubulake Factors Disfavor Cost-shifting in Securities Dispute

Xpedior Credit Trust v. Credit Suisse First Boston (USA), Inc., 2003 WL 22283835 (S.D. N.Y., decided October 2)

Applying the factors first articulated in *Zubulake v. UBS Warburg*, ___ F.R.D. ___, 2003 WL 21087884 (S.D. N.Y. May 13, 2003), District Judge Shira Scheindlin orders a defendant/investment bank to bear its own costs of production in a class action alleging that it required extra payments from investors in return for allocations of Initial Public Offerings it was underwriting. The defendant had moved for a protective order requiring the plaintiff to bear half the costs of restoring certain electronic documents generated by defendant’s predecessor in interest.

Judge Scheindlin explains that the documents at issue had been archived on optical disks, a medium generally considered accessible as “nearline” data. In this case, however, the optical disk system was decommissioned and the related servers were recycled when the defendant merged with its predecessor in interest. Operationally, this required the defendant to reconstruct the entire system in order to access both the optical disks, as well as data that had been stored on Digital Linear Tapes. The defendant expended “hundreds of thousands of dollars” to perform the restoration. Judge Scheindlin observes, “While the technology was ‘accessible’ at the time that [defendant’s predecessor] used it, the technology was rendered inaccessible by virtue of the fact that [defendant] decommissioned it. . . . As a factual matter, the . . . records were inaccessible at the time this litigation commenced.” Their inaccessibility is what triggers the court to consider cost shifting by analyzing the *Zubulake* factors.

Factor 1: The extent to which the request is specifically tailored to discover relevant information

The plaintiff’s requests, which were for e-mails and word processing documents, were appropriately tailored to discover relevant information, since these types of documents would be the likely source of information about valuation and pricing of issuers’ IPO shares. However, because the systems on which such records reside have been decommissioned, the defendant was required to perform a restoration before it could produce any of these records. This factor does not favor cost shifting.

Factor 2: The availability of such information from other sources

The documents sought are available exclusively from the

decommissioned servers. This factor therefore does not favor cost shifting.

Factor 3: The total cost of production, compared to the amount in controversy

The defendant estimates the cost of production at approximately \$400,000. Damages claimed range from \$68.7 million to \$7 billion, if the class is certified. Since the cost of production is relatively insignificant compared to the sum at stake, this factor does not favor cost shifting.

Factor 4: The total cost of production, compared to the resources available to each party

Defendant reported net revenues of \$5.7 billion in fiscal year 2002. Plaintiff is a bankrupt corporation with virtually no assets. Since defendant's assets clearly dwarf plaintiff's, this factor weighs against cost shifting.

Factor 5: The relative ability of each party to control costs and its incentive to do so

This factor is essentially neutral, since the restoration is substantially complete and its cost fixed. To the extent possible, however, plaintiff has promised to work with defendant to minimize costs.

Factor 6: The importance of the issues at stake in the litigation

As a contract dispute between sophisticated commercial entities, this case does not raise the type of public policy issues that might affect cost shifting; this factor is therefore neutral.

Factor 7: The relative benefits to the parties of obtaining the information

Both parties will benefit from production; the plaintiff, because all the documents it needs to prove its case are contained on the decommissioned system, and the defendant, because it would be required to restore many of the same systems for the purposes of a related case. This factor therefore emerges as neutral.

The Tally

Zubulake factors one, two, three, and four weigh against cost shifting, while five, six, and seven are neutral. This is the basis for Judge Scheindlin's conclusion that cost shifting is inappropriate in this case.

Inadvertent Disclosure

Defendants Must Return Documents Inadvertently Copied to Hard Drive

United States v. Rigas, 2003 WL 22203721 (S.D. N.Y., decided September 22)

Defendants in a securities fraud action cannot retain certain privileged documents contained on a computer hard drive that the government produced to them during discovery. The court's ruling recognizes that the government took reasonable precautions to protect the asserted privilege, that it released a relatively small number of privileged documents compared to the total number of documents produced, that it asserted privilege and requested that the documents be returned immediately upon discovery of the disclosure, and that no one defendant will be prejudiced vis-à-vis any other defendant by the return of the documents to the government.

The Facts

The charges of conspiracy, bank fraud, wire fraud, and securities fraud arose from defendants' management and control of a communications company. In response to a government subpoena, the company produced exact copies of 26 computer hard drives used by their employees during the relevant time frame. The copies were created by PriceWaterhouseCoopers; the original drives remained with the communications company "in pristine condition." The government subsequently made the copied drives available to the defense counsel for their own replication, conditioned on counsel's agreement that any vendor they hired for the job could be interviewed by the defense.

To access the data on the hard drives, the Assistant United States Attorneys (AUSAs) assigned to the case had their IT staff install the drives in certain computer terminals belonging to the United States Attorney's Office (USAO), which were housed in a secure federal building. The AUSAs impressed upon the IT staff the importance of installing the drives in such a way as to prevent additions or deletions to them, as befitted their status as "evidence." After the installation, authorized persons could view documents on the hard drive only from the secure room, but not through the USAO network.

After each hard drive was installed on a terminal, a USAO paralegal conducted a cursory review of the drive to confirm it could be accessed. During one of these reviews, the entire content of the paralegal's network account was copied on to one of the 26 hard drives, through a unique and unexpected confluence of circumstances. It included Grand Jury mate-

rial, confidential law enforcement information, and the paralegal's work product relating not only to the instant case but also to others on which she was assigned. When defense counsel discovered this material had been produced, he immediately notified the AUSA, advising him that neither he nor any other member of his firm had read the material. The same day the AUSA learned of the inadvertent disclosure, he sent defense counsel a letter asserting the work product privilege with respect to the paralegal's files and requested their prompt return. A motion allowing the defense to retain the materials ensued.

Middle of the Road Test

Defendants argue that the government waived its work product privilege when it voluntarily permitted defense counsel to copy the hard drive containing the paralegal's network account. The Southern District of New York follows the "middle test" approach applied by various courts to the issue of inadvertent discovery of privileged communications. It provides that waiver is decided by consideration of the following factors:

- the reasonableness of the precautions taken to prevent inadvertent disclosure,
- the amount of time it took the producing party to recognize its error,
- the scope of the productions,
- the extent of the inadvertent disclosure, and
- the overriding interests of fairness and justice.

(The other two popular tests are the "never waived" approach, which holds that a disclosure that is merely negligent can never affect a waiver, and the "strict accountability" rule, which holds that disclosure automatically affects a waiver regardless of the intent or inadvertence of the privilege holder.) Analysis of these factors militates against a finding of waiver here.

Reasonable Precautions

The court begins its examination of this factor by asserting, "Generally, courts in this District will not find waiver by inadvertent disclosure unless the producing party's actions were 'so careless as to suggest that it was not concerned with the protection of the asserted privilege.'" The court cites the following as evidence of the care taken by the government to ensure the confidentiality of the work product: the files were maintained on a secure computer network, access to which required a security clearance, and within a private password-protected account on that network; the vendor charged by defense counsel with the copying was

prohibited from accessing the network, his work was supervised by a USAO employee, and entered on a log; the drives themselves were stored in a secure federal building under tight security; the legal team communicated clearly and specifically with its IT team about its requirements and the significance of the drives. While the court concedes, "With the benefit of hindsight ... the Government could have avoided the inadvertent disclosure ... by producing a 'pristine' version rather than a working copy of the hard drives," it emphasizes that "the reasonableness of a party's actions to protect privileged information should be measured in light of the risks *foreseeable* to that party at the time the precautions were taken." The circumstances through which the copying occurred were considered "unique" and therefore not foreseeable.

Scope of Discovery vs. Extent of Disclosure

Since the government released a relatively small number of privileged documents compared to the total number of documents produced, this factor weighs against a finding of waiver. The court characterizes the overall volume of discovery documents produced by the government as "tremendous," comprising thousands of pages of paper documents and hundreds of CD ROMs, along with the 26 hard drives, each of which contained 11.2 gigabytes of data, or approximately two million pages per drive. The paralegal disclosure, by contrast, amounted to roughly 130 files.

Timeliness of Privilege Assertion

Since the government asserted the work product privilege by letter to defense counsel the same day it learned of the inadvertent disclosure, this factor clearly weighs against a finding of waiver.

Fairness

In the context of privilege waiver, fairness relates to how widely the privileged materials were disseminated. The court explains, "Fairness concerns are especially salient when some parties have reviewed the information while others have not." No such risk of prejudice is present in this case, as all defense counsel have refrained from reviewing the privileged material pending resolution of the discovery dispute.

The court rejects the defense argument that returning the documents to the government effectively punishes the defendants for promptly notifying the government of the disclosure and for refraining from reviewing the disclosed documents. The court points out that attorneys always "bear responsibility for acting in accordance with ethical norms of the legal profession," and sees the effects of its decision not

as taking anything away from the defendants but rather as preventing a windfall to them. Accordingly, this factor precludes a finding of waiver.

The defense motion for an order allowing it to retain the documents is denied.

Preservation Orders

Judge Chastises Party for Inadvertent Erasure of E-mail Backup

Keir v. UnumProvident Corp., 2003 WL 21997747 (D.N.J., decided August 22)

Calling sanctions “premature,” a U.S. District Judge from New Jersey is nonetheless highly critical of a defendant whose restoration efforts resulted in the erasure of critical e-mails it was under order to produce in discovery. U.S. District Judge Denise Cote’s findings of fact demonstrate what a minefield electronic discovery can be even to a technologically sophisticated entity like the largest American provider of disability insurance.

The Underlying Case

On November 4, 2002, policyholders filed an action alleging that UnumProvident formally encourages its employees to deny claims where the anticipated payouts would be high. UnumProvident’s practices in this regard were featured on the October 13, 2002 episode of NBC’s “Dateline” and the November 17, 2002 episode of CBS’s “60 Minutes.” Among the documents plaintiffs sought in discovery were the e-mails sent by the defendant within three days of the airing of the two television programs. They theorized that e-mails sent contemporaneously with the broadcasts could reasonably be expected to contain damaging admissions made in their wake and serve to identify witnesses who were willing to acknowledge the existence of defendant’s questionable business practices.

The parties and the court engaged in extensive discussions and hearings on how best to conduct discovery in light of UnumProvident’s complex electronic storage systems and equally complex document destruction/retention policies. On December 27, 2002, the court entered a preservation order wherein plaintiffs agreed *inter alia* to allow the defendants to follow their customary e-mail destruction policy on a going forward basis if they produced the tapes for the three days following each of the two broadcasts.

The Operative Technology

UnumProvident’s electronic storage system is described in great detail in the court’s opinion; it is maintained pre-

dominantly by IBM employees. Initial inquiries indicated that the targeted e-mails were contained on 18 to 20 Exchange servers that were regularly backed up and would have been on 20 to 70 of a total of 300 tapes.

Commercial disaster recovery software, Tivoli Storage Manager (TSM), was in use on the system. When TSM identifies tapes that contain only “expired” data, those tapes are recalled from off-site storage and reused. The court explains, “When a tape is reused, it is overwritten. It may be possible to retrieve some data from tapes that are partially overwritten. It may also be possible to obtain data from the portion of a tape that is overwritten, but a finding of the likelihood of success from such an undertaking would require expert testimony that has not been provided to the court. Generally, off-site tapes are returned to on-site tape libraries for reuse within one to seven days of the date on which TSM determines that the retention date for all of the data on the tape has expired.”

TSM also features an indexing system, through which data on the backup tapes can be identified, retrieved and reassembled. The court notes ultimate control over the retention policy resides with UnumProvident, which can deviate from the default retention policy and customize a special policy for specific servers, applications or databases.

The Efforts to Preserve the E-mail

Jonathan Hyler, UnumProvident’s “enterprise security architect,” put the preservation process into motion. He believed that the only way to preserve data on the backup tapes was to restore and re-save the data, a process that he estimated would take over two weeks to complete. In an attempt to compensate for the cycle of tapes “expiring” and returning to the system for overwriting, his preservation attempts were limited to creating a special “snapshot” backup that would back up the e-mails that were on the system as of the day or days the snapshot was taken. He implemented the snapshot backup between December 20 and 23.

While this method preserved the existing e-mail in employees’ mailboxes on the date of the backup along with e-mail that had been deleted within the previous two weeks, it did not capture the e-mail environment as it existed on November 4, 2002, the date the suit was filed and UnumProvident’s preservation obligation attached, nor did it preserve any e-mail in the backup system. Moreover, in creating the December snapshot, IBM unwittingly caused the backup tapes to re-enter the system prematurely, and as a result, to be overwritten. And this unintended consequence, which affected the e-mails sought by the defendant, was not recognized by UnumProvident or IBM until mid-January.

Too Much Delay, Not Enough Communication

While the court acknowledges that the erasures were inadvertent, it nonetheless chastises the plaintiff for its missteps. First, observes the court, the people making critical decisions about how much and what e-mail to preserve in order to meet UnumProvident's legal obligations were not only ill-equipped to handle the task, they were left largely unsupervised to do so.

The court points out that no formal instruction regarding data preservation was issued until sometime in the first week of January 2003, but there is no written confirmation or independent corroboration that this occurred. For example, no instruction was given to identify the backup tapes containing the e-mails for the six crucial days and remove those tapes from circulation. Indeed, no instruction regarding the preservation of e-mails for the six specific dates was given at all.

UnumProvident compounded the problem by never articulating to the court that it would have any difficulty in preserving the six days of e-mail, to the extent that they still existed as of the date of the December 27 order. The court explains, "The fact that the backup tapes had a set expiration schedule was understood by all, and a subject of exten-

sive discussion with the court. Counsel for UnumProvident believed that the expiration protocol may have been as short as 30 to 60 days. It was, therefore, incumbent on the defendants to act promptly to preserve as much as possible. If they had done so, the backup tapes overwritten between approximately December 28 and January 15 would have been preserved. If the retrieval of tapes from off-site storage and overwriting had occurred only on December 24, 26 and 27, then an estimated 90 tapes would have been overwritten, instead of 881."

The court also criticizes UnumProvident's conduct once it realized that the e-mails had been lost. It should have promptly investigated what had gone wrong and reported the results of its investigation in a forthcoming manner to the plaintiffs and the court. It should also have ascertained the extent of the loss months before it actually did, and reported the results with dispatch. This would have saved all parties—and the court—significant resources, and perhaps even more importantly, prevented UnumProvident from losing credibility with the judge.

The issue of sanctions is reserved until the extent of the loss, the possibility of retrieval, and the resulting prejudice to the plaintiffs are determined.

— *C. Eoannou*

District Courts Slowly Embracing Electronic Case Management

The Associated Press recently reported on the progress the 94 U.S. district courts have made in migrating their case files to an electronic environment. As of October 11, the 26 district courts listed below maintain at least a portion of their case files on an electronic case management and filing system that gives lawyers and the public access by computer over the Internet. Sixteen of them allow lawyers to file cases initially with the court over the Internet; they are so designated in the list with the word "filing." According to the administrative office of U.S. Courts, eventually all 94 districts will offer all these services over the Internet.

Alabama, Southern District
California, Northern District, filing
District of Columbia, filing
Indiana, Southern District, filing
Iowa, Northern District
Kansas, filing
Kentucky, Eastern District
Kentucky, Western District
Maine
Maryland, filing
Massachusetts
Michigan, Western District, filing
Missouri, Western District, filing

Nebraska, filing
New York, Eastern District, filing
New York, Western District
Ohio, Northern District, filing
Ohio, Southern District, filing
Oregon, filing
Pennsylvania, Eastern District, filing
Pennsylvania, Middle District, filing
South Dakota
Texas, Northern District
Washington, Western District, filing
Wisconsin, Eastern District, filing
Wyoming

Book Review

Primer, Reference

Electronic Discovery by the Book

By George Socha

This year brings two excellent new books on electronic discovery. Joan Feldman's *Essentials of Electronic Discovery – Finding and Using Cyber Evidence* is a quick and readable primer on computer forensics and electronic discovery, useful for newbies and old hands alike. Michael Arkfeld's *Electronic Discovery and Evidence* serves as a solid digital discovery reference resource, packed full of detailed information and replete with case citations. Anyone working with electronic discovery should consider adding both books to their libraries.

Essentials of Electronic Discovery – Finding and Using Cyber Evidence

Joan Feldman specializes in forensic computing, discovery and risk management. One of the pioneers of computer forensics, she founded Computer Forensics Inc. (www.forensics.com) in 1994 and worked in records management before that.

Based on Ms. Feldman's experience and expertise, *Essentials of Electronic Discovery* offers newcomers to the world of electronic discovery an overview of what they must contend with. Fortunately, it also provides a series of pointers for dealing with the myriad issues raised by this relatively new aspect of discovery. In addition, it is an effective set of refresher materials for those of us who have been laboring in the electronic discovery fields for years.

The book is laid out in 12 chapters whose titles go a long way toward explaining the focus of the book:

1. Why Computer Based Discovery
2. Nuts and Bolts of Computers: Data Within Computer Systems and Storage Media
3. Everything You Wanted to Know About Email Discovery, But Were Afraid to Ask
4. Discovery of Databases in Litigation
5. Data and Equipment Security
6. Planning and Conducting Electronic Discovery
7. Determining the Completeness of Discovery
8. Forensic Collection, Analysis, and Preservation
9. Discovery on the Internet
10. Electronic Risk Management
11. Can New Technology Solve the Problems in Electronic Discovery?
12. Special Issues for Attorneys

The book also contains 13 short appendices ranging from "Frequently Asked Questions" to an "Exit Inventory for Data Preservation" form to a sample declaration.

The strength of *Essentials of Electronic Discovery* lies in its apparent simplicity. Assembled in a three-ring binder, the book can be read—or at least skimmed—in one sitting. Although it is 253 pages long including appendices and index, it has small pages, large print, and few footnotes. Most importantly, the text is direct and simple, containing little technical jargon.

Should you prefer, you can tackle the book one chapter at a time. Averaging just over 16 pages, the chapters do not take long to go through. For the most part, each chapter can be treated as an independent piece, so that it is not necessary to have read the first chapter, on why one needs to deal with

Most importantly, the text is direct and simple, containing little technical jargon.

electronic discovery, before diving into the sixth chapter, which focuses on how to plan for and conduct electronic discovery.

I said "apparent" simplicity, because the book really is packed with practical advice borne of years of hands-on experience in the field. Many of the chapters can serve as sound checklists. For example, the seventh chapter, "Determining the Completeness of Discovery," offers the following advice: determine where electronic data really came from; look for under-represented categories of information such as people, drafts of importation documents, date ranges, and topics; be specific in text searches your expert runs; follow through; and make the other side commit to having complied completely with your discovery requests.

Light on Legal Authority

Because it was written by an expert in computer forensics, not by an attorney, the book offers only slim guidance for those seeking legal authority. For example, as far I as could tell, there are no references to the Federal Rules of Evidence and only seven references to the Federal Rules of Civil Procedure—four general, one setting out the text of Rule 26(c), one relating to questions to ask during a Rule 30(b)(6) deposition, and one briefly discussing Rule 37 as a potential source of sanctions.

Essentials of Electronic Discovery is published by Glasser LegalWorks, Inc. It can be ordered by phone (1-800-308-1700, ext. 101), by email (orders@glasserlegalworks.com), or through the Internet (www.glasserlegalworks.com). Inside the front cover is a CD-ROM containing a searchable PDF version of the book. The book costs \$195 plus tax, shipping and handling, and comes with a 30-day free trial.

Electronic Discovery and Evidence

An Assistant United States Attorney in Arizona and an ardent user of legal technology for nearly two decades, Michael Arkfeld has focused on law office and courtroom technologies for the past 11 years. In an earlier book, *The Digital Practice of Law*, Mr. Arkfeld examined legal technology applications for law offices and litigation. With *Electronic Discovery and Evidence*, Mr. Arkfeld turns, not surprisingly, to the field of electronic discovery.

Three years in the making, *Electronic Discovery and Evidence* is a compendium of information about electronic discovery, from overviews to minutia, replete with case citations. It makes an excellent reference resource for attorneys and their support staff. It also is of value to the forensic service bureaus catering to those attorneys.

The book is divided into eight chapters:

1. Electronic Information in Litigation
2. Creation and Storage of Electronic Information
3. Structure and Type of Electronic Information
4. Computer Forensics, Experts and Service Bureaus
5. Collecting, Processing and Searching Electronic Information
6. Discovery and Production Process
7. Court Procedural Rules and Case Law
8. Admissibility of Electronic Evidence

A 13-page glossary of technical terms appears at the end of the book.

Strengths and Weaknesses

Electronic Discovery and Evidence is at its best as a resource to turn to when you have a specific issue to address. At 437 pages of tightly-packed text and chapters averaging nearly 55 pages, this is not a book to curl up with in a deep chair in front a hot fire. If, however, you need to research the risks and penalties associated with failing to adequately preserve electronic evidence, §7.09[E], *Spoliation*, offers 12 pages covering the topic in great detail. By my count, there are 77 case citations in that section alone, many including commentary.

I do have one nit to pick, which has to do with ease of use. The book is divided into chapters, sections, and subsections, and the table of contents at the beginning of the book reflects that structure. The page numbering and the section listings at the beginning of each chapter do not.

If you want to go to §1.04[D][8], which is about the evidentiary value of electronic information in trademark cases, the table of contents directs you to page 1-19. Flip through the pages and fairly quickly you can find that page. If, however, you go to the section listing at the beginning of Chapter 1, you will not find any page numbers, just section numbers and names. The same holds true with references within the text. Thus, the discussion at page 1-11 about Fed. R. Civ. P. 26(a)(1)(B) sends you to §7.07[B], “Document” – Defini-

Electronic Discovery and Evidence is at its best as a resource to turn to when you have a specific issue to address.

tion for further information, but does not indicate which page between 7-1 to 7-100 you need to turn to.

The three-ring binder also, a glossary and an index. Purchasers of the book get a six-month subscription for content updates and access to a “members-only” password-protected web site that contains practice forms, case summaries, and other electronic discovery resources.

Electronic Discovery and Evidence is published by Law Partner Publishing and can be ordered by phone (602-993-1937), by e-mail (sales@arkfeld.com), or through the Internet (www.arkfeld.com). The book costs \$149.99 plus shipping of between \$6.95 and \$40.

Complementary Texts

Essentials of Electronic Discovery and *Electronic Discovery and Evidence* both make useful additions to any library on electronic discovery. They serve very different roles and should be viewed as complementary rather than competitive sets of materials. Ms. Feldman’s book is a quick read that provides an overview of the world of computer forensics and electronic discovery as well as insights into strategies and techniques. Mr. Arkfeld’s publication is a reference resource densely packed with practice pointers and case citations, definitely not intended as armchair reading.

George Socha is an attorney and consultant whose business, Socha Consulting LLC, helps inform digital discovery decisions. He is a frequent contributor to Digital Discovery & e-Evidence and can be reached at 651-690-1739 or george@sochaconsulting.com.

Electronic Format Clearly Superior for E-mail Production

By Gregory L. Fordham CPA, CIA

Electronic messaging in the form of e-mail continues to be a significant focus for litigators during discovery. Remarkably, after resolving issues related to cost and scope, litigators still face their most important decision: should the e-mail be produced in paper, image or electronic format.

The formats differ from one another considerably. The paper option typically involves printing the e-mail message (sender, recipients, subject, message and date) onto a paper medium. The image format typically involves capturing that same data in Tagged Image File Format (TIFF) or Portable Document Format (PDF). The electronic format involves retaining the e-mail message or even the entire data store in a digital format, the attributes of which can then be displayed or printed.

The digital format has three advantages over the typical paper and image-based formats. First, the electronic format is the only complete original. Printing the standard message, in whatever format, only reveals the sender, the “to” and “cc” recipients, subject, message body and the sent date attributes of the e-mail, even though many more attributes exist.

The second shortcoming of the traditional paper and image formats involves the requirements for authentication and identification. Simply stated, the paper and image format messages cannot be reliably authenticated without an electronic original or at least access to all the data contained in the electronic original.

The final flaw of the traditional paper and image formats is that they present fewer cost efficiencies than the electronic format. For cost conscious litigators, the electronic format offers more advantages than its paper or image-based counterparts.

Methodology

To illustrate these points, this article compares and contrasts the typical paper and image-based formats to the electronic version from a MAPI compliant messaging system. MAPI is assumed because it is probably the most widely-used messaging system architecture. It exists in every Microsoft operating system since Windows 95. It is also employed in the most widely used messaging systems, Microsoft Exchange and Microsoft Outlook. Finally, it has been adopted by most messaging system vendors, including IBM in its Lotus Notes product and Novell in its

Groupwise product. In fact, Microsoft touts the MAPI architecture as the only true industry standard messaging specification, since it was developed with the participation of more than 100 software vendors.

Requirement for Original

Rule 1001 of the Federal Rules of Evidence requires that an original be used to prove the content of a writing, recording or photograph. With respect to e-mails, the question becomes what constitutes an original. The most likely response would be the printed message itself (date, sender, recipients, subject and message), but that would simply be an original of those *attributes* and not the entire message.

Like all electronic data, e-mail contains more data than ever appears on paper. A MAPI compliant system contains more than 50 standard properties related to messages, recipients and message attachments of which the message sent date, sender, subject and message body are but four. In addition to the standard properties, a MAPI compliant system can contain additional vendor specific properties.

Properties Unique to Electronic Format

What, then, is missing from the printed version of the e-mail, whether in paper or image format? Some of the more significant data contained in the original electronic version but not appearing on the printed message include the following:

- **Transport Header** — The transport header is a text-based property that is part of the electronic message. It contains an audit trail of the message’s journey from the sender to the recipient. Captured in the audit trail are the IP addresses of each server encountered along the way, including date and time stamps of each encounter. Another potentially useful piece of information contained in the header is the sender’s computer name, which, along with the sender’s IP address, can be used to authenticate the message sender. Although there is a MAPI option that allows client applications to place the transport header in the message body, usually this option is not invoked and so this data never appears on the printed message.
- **Recipient List** — The recipient list is contained within a table that is part of the electronic message. All message recipients are contained in this table, including direct recipients, carbon copy recipients, blind carbon copy recipients and resend recipients. (A resend recipient is someone who could not receive the message initially, necessitating its retrans-

mission.) Blind carbon copy recipients and resend recipients do not typically appear on the printed message; they are only available in the original electronic format.

- **Create and Last Modified Date/Time Stamps** —

All of the message objects and sub-objects include fields that capture the object's create and last modified date/time stamps. Thus, the message itself and the attachment list contain create and last modified date/time stamps. These values are populated based on the last issuance of a "save changes" command. So, if there were ever a dispute about differences between a sender and receiver's message or their attachments, these date/time stamps could be inspected to determine whether one was changed at a time subsequent to the message's sent date/time or its received date/time. Of course, neither the create nor last modified date/time stamps for any of the message's objects or sub-objects appears on the typical printed message; they are only available in the original electronic format.

- **Original Author and Sender** —

The original author and sender are also properties contained within the message. In the case where replies have occurred and the respondents have deleted the reply chain, a litigator could at least know the name of the original author and sender of a message. Based on the message's create and last modified date/time stamps, the litigator could also determine the elapsed time from initial message creation and the latest reply. Of course, none of this data appears on the typical printed message; it is only available in the original electronic format.

- **Representing Sender and Receiver** —

In some cases, a superior may delegate the actual process of sending or receiving an e-mail to a subordinate or other agent. The representing sender and representing receiver functions help to differentiate these individuals. The person actually pushing the send button appears as the message sender while the representing sender is the person for whom the message is sent. Of course, the difference in personnel does not appear on the typical printed message; it is only available in the original electronic format.

- **Folder Name** —

Each message is contained within a folder. Although the folder name is not attached to the message itself, the parent entry ID that relates to the particular folder is a property of the message. With this data alone and with the other messages in a popu-

lation, a litigator could evaluate whether there were other folders in which incoming and outgoing messages were stored other than the inbox, sent items and deleted items folders. This information could be useful if the user retained messages in special subject matter-based folders. If the litigator also had the entire message store such as a PST or EDB file in addition to the electronic message, he could also identify the name of the particular folder in which a message resided. Of course, none of this information appears on the printed message; it is only available in the original electronic format.

The lesson from this analysis is that the typical printed message is not a complete original, since it does not display all of the data contained within the original electronic message. Furthermore, since the MAPI architecture allows for vendor specific properties as well, it is probably unrealistic to think that a litigator could formulate a document request for paper or imaged-based formats that would contain all of a messaging system's attributes until after he has received the electronic original.

Authenticating the Original

The gap between the contents of the typical paper and image format versus the electronic format also raises another significant point under the Federal Rules of Evidence.

Some of the more significant data contained in the original electronic version but not appearing on the printed message are the transport header, complete recipient list, create and modify date/time stamps, original author and sender, representing sender and receiver, and the folder name where the message resides in the user's messaging system.

Rule 1001(3) provides, "If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an 'original.'" Clearly, with regard to electronic compilations there is nothing magical about the printed format and none is prescribed.

In addition, Article IX of the Federal Rules of Evidence imposes a requirement for authentication and identification. With regard to e-mails, the easiest way to satisfy this requirement is by self-authentication under Rule 902(7). However, if the only tools for self-authentication are the typical paper or image formats, an erroneous result could ensue.

Although the e-mail contains the sender's name and sometimes e-mail address, this information is easily forged. Through a practice known as spoofing, any sender can conceal his true identity. The only requirement for the sender's e-mail address is a valid domain name. Accordingly, the only effective way to determine a phony sender is by examining other message properties, like the transport header. Similarly, if there are disputes about message contents or attachment contents, the details necessary to authenticate what was received or what was sent simply do not exist in the typical printed message. Again, that capability only exists with the original electronic message, or through other testimony and observation.

For those who favor the image format because it is less likely to be changed or altered after production than the original electronic format, there is a solution. Since each electronic file has its own unique digital fingerprint, this value can be included with any electronic production and then used as a baseline to subsequently prove authenticity of produced data.

The bottom line is that electronic data is highly perishable and easily changed. The best way to authenticate an electronic message is by using its electronic format coupled with proper chain of custody procedures and digital fingerprints.

Cost and Economy Issues

In discovery, every litigator wants to cast a wide net. The secret to successful fishing is landing the catch and processing it as quickly and inexpensively as possible. The greatest efficiency in producing e-mails is provided by the electronic format, since it eliminates the need for intermediate conversion processes and because it is able to narrow the population of documents to be examined.

Nowhere is this more apparent than in the area of deduplication. The image format is not as efficient for deduplication because attachments are typically appended to the e-mail message and not separated. Accordingly, the deduplication process is applied to the entirety of the e-mail message, including its attachments. Thus, if the same attachment is sent in different e-mails at different times or to different recipients or with different collections of attachments, there is no way to identify that the collection contains a duplicate attachment, since all of those attributes would be used to identify a duplicate. This means that the duplicate original would be reviewed with every unique collection in which it resides. It also means that locating every instance of a particular attachment would likely be impossible.

Even word searching an image file cannot locate identi-

cal attachments if their names have been changed in the attachment list of the e-mail or if it contains no truly distinguishing features or phraseology. Simply, when combined with all parts of the message, it is impossible to positively

The bottom line is that electronic data is highly perishable and easily changed. The best way to authenticate an electronic message is by using its electronic format coupled with proper chain of custody procedures and digital fingerprints.

identify a particular attachment within an image file. Even searching for particular attachments, particularly images, could be impossible when their true identity is obscured by the message sender and then the litigator merges it with the entire message collection.

By contrast, when the original electronic message is used, distinctions can be made between the entire message, including attachments and the message itself, or the attachment itself. Once separated, digital fingerprinting can be used to uniquely identify attachments instead of just their file names.

In sum, the electronic format is the best choice for the production of e-mail because it is a complete copy of a multi-part original and has superior authentication capability. Litigators who continue to use the traditional printed message should recognize the significant limitations of that format: it does not display all of the data contained within an electronic message and will never provide the cost efficiencies that can be obtained through the use of the original electronic format. Electronic format has yet to achieve universal acceptance because legal professionals persist in applying traditional paper document concepts to the discovery, presentation and management of e-mails. E-mails and their related data must be recognized as hierarchical databases where the message, attachments and other related data are limbs and leaves on an intricate tree structure. Consequently, the format preference for e-mails should be the same as any other database, the electronic format.

Mr. Fordham is a Principal in the Atlanta, Ga. office of K&F Consulting, Inc. For nearly 20 years, he has assisted contractors and attorneys from around the United States and overseas with a myriad of systems issues, including recovery and analysis of electronic data, electronic data discovery, and computer-based auditing. He can be reached at 770-642-0311 (voice), 770-642-9913 (fax), or greg@knfcon.com.

Kroll-Ontrack Offers Certification Course

Kroll Ontrack Inc., a wholly-owned subsidiary of Kroll Inc. (NASDAQ: KROL) that provides electronic evidence and data recovery software and services, is sponsoring a certified e-discovery specialist course, designed exclusively for litigation and law practice support professionals. Certification acknowledges litigation support professionals who meet the industry's high standards for managing the e-discovery process and assisting attorneys in making digital evidence decisions as they arise in litigation and regulatory compliance matters.

"With the ever increasing amount of electronic data being requested and produced in litigation, it is crucial for litigation and practice support managers to have a firm understanding of electronic discovery," Kristin Nimsger, director of the Electronic Evidence Product Line for Kroll Ontrack, said in a statement announcing the course. "This certification also will allow litigation and practice support managers to have a full understanding of the technology and complex decisions associated with e-discovery. It will help them to be acknowledged as a vital resource within the law firm or corporation, and to the clients they represent." The certification course will be offered December 8 and 9, 2003, at Kroll Ontrack's corporate headquarters in Eden Prairie, Minnesota. Prerequisites for the course include a solid background in large-scale document review and production practices and a cursory understanding of e-discovery issues. The course will address crucial topics to e-discovery projects, including:

- how to identify the key characteristics of a matter where e-discovery should be undertaken;
- the current electronic evidence case law;
- what a litigation support professional needs to know;
- options for collecting data;
- important criteria in the data conversion and filtering processes;
- options for reviewing and producing electronic evidence;
- key decisions for each stage of the electronic discovery process; and
- managing timelines for e-discovery projects.

Course faculty include Hampton Coley, Technical Litigation Support Manager, Cravath, Swaine & Moore; Kimberly Ford, Litigation Support Coordinator, Kirkland & Ellis LLP; Nancy Robertson, PMP, Director of Electronic Evidence Project Management, Kroll Ontrack; and Mike Rands, Director of Electronic Evidence Technology, Kroll Ontrack, among other highly credentialed e-discovery experts. Tuition for the course is \$1,500 and enrollment is limited to 35 people. For more information on how to enroll, visit www.krollontrack.com.

Invitation to Authors

The publishers of *Digital Discovery and e-Evidence* invite you to submit for publication articles addressing the discovery, production, and presentation of evidence in the digital age. Prospective authors may contact Carol L. Eoannou at (301) 562-1530 ext. 269, by fax at (301) 562-1542, or at [ceoannou@ pf.com](mailto:ceoannou@pf.com).

Calendar

NOVEMBER

5

Electronic Evidence Thought Leadership Series CLE Program: E-Discovery: Tips, Tactics, & Technology. Houston, Texas. Presented by Kroll Ontrack.

Contact: Web: <http://www.krollontrack.com/redirect/Tcaselaw1003upevents.asp>

14

7th Annual Electronic Discovery and Records Retention Conference. Chicago, Ill. Presented by Glasser LegalWorks.

Contact: Web: <http://www.legalwks.com>

21-22

The Business Response to the New CyberSecurity Threats and Terrorism. Washington, D.C. Presented by the American Bar Association and the Center for Continuing Legal Education.

Contact: tel: 800-285-2221; fax: 312-988-5850; Web: <http://www.abanet.org/cle/programs/n03brn1.html>.

DECEMBER

4

Electronic Evidence Thought Leadership Series CLE Program: Ask the Experts: E-Discovery Advanced Topics. New York City. Presented by Kroll Ontrack.

Contact: Web: <http://www.krollontrack.com/redirect/Tcaselaw1003upevents.asp>

5

7th Annual Electronic Discovery and Records Retention Conference. San Francisco, Cal. Presented by Glasser LegalWorks.

Contact: Web: <http://www.legalwks.com>

8-9

E-Discovery Specialist Certification Course. Eden Prairie, Minn. Presented by Kroll Ontrack.

Contact: Web: <http://www.krollontrack.com/redirect/Tcaselaw1003upevents.asp>

9

E-Discovery Conference. San Francisco, Cal. Presented by Mealey Publications.

Contact: tel: 800-MEALEYS or 610-768-7800, fax: 610-768-0303; postal service: Mealey Publications, P.O. Box 62090, King of Prussia, PA 19406-0230; e-mail: mealeyseminars@lexisnexis.com; Web: <http://www.mealeys.com>

2004

FEBRUARY

2-4

LegalTech 2004. New York City. Features Litigation Technology and Electronic Data Discovery tracks. Presented by LegalTech, a division of American Lawyer Media.

Contact: Web: <http://www.legaltechshow.com>

MAY

24-26

National Conference on Managing Electronic Records (MER). Chicago, Ill. Presented by Cohasset Associates, Inc.

Contact: tel: 800-200-7667; Web: <http://www.cohasset.com>

