

Digital Discovery & e-Evidence

BEST PRACTICES & EVOLVING LAW

Vol. 3, No. 3 | March 2003

Inside

- 1 **A Discovery Disaster of Operatic Proportions:** The Southern District of New York finds defendant's discovery abuses warrant entry of judgment for plaintiff.

- 1 **Talking Tech:** A Practical Guide for Avoiding *Metropolitan Opera* Mishaps: E-discovery expert Virginia Llewellyn sets out a plan.

- 5 **Litigator's Guide:** Mastering the Use of E-Discovery Special Masters: George Socha, complex litigation specialist, describes what to expect when a special master is appointed.

- 7-10 **Case Law & Regulation:** *McPeck II* Sets Out Additional Principles of Relevancy • California Appeals Court OKs Injunction Preserving E-Evidence, Giving Expert Access • No Reasonable Possibility Missing Hard Drives Contained Evidence of Theft of Trade Secrets • Warrant for Text Files Relating to One Crime Does Not Cover Image Files Relating to Another

- 11 **International Insights:** Hard Copies of E-Mails Not Hard Evidence: Dorothea Kettrukat reviews a recent decision from Germany.

- 12-13 **In Brief:** Practice Tip • Attorneys' Fees • Heightened Foreseeability of Criminal Act Not Evidenced by E-Mails

- 15 **Calendar**

A Discovery Disaster of Operatic Proportions

Metropolitan Opera Association, Inc. v. Local 100, Hotel Employees and Restaurant Employees International Union, 2003 WL 186645 (SD NY, decided January 28, 2003)

If District Judge Loretta A. Preska's opinion in this case were a libretto for an opera, it might well have been entitled "How to Lose a Civil Action Without Going Near a Courtroom." She sets forth in great detail the conduct of a defendant labor union that constituted such wholesale abuse of the discovery process as to warrant the ultimate sanction: entry of judgment in favor of plaintiff.

This was not a result the judge arrived at easily, as reflected by her observation that "in the ordinary course, lawsuits should not be resolved based on who did what to whom during discovery. Indeed, a result driven by discovery abuse is justified only on the rarest of occasions and then only after the miscreant has demonstrated unquestionable bad faith and has had a last clear chance to comply with the rules." The judge cited the union's total mishandling of discoverable electronic evidence as among its more egregious misdeeds.

continued on page 13

Practical Guide for Avoiding *Metropolitan Opera* Mishaps

By Virginia Llewellyn

Metropolitan Opera Ass'n, Inc. v. Local 100, Hotel Employees and Restaurant Employees Int'l Union, the focus of the lead story in this issue, and *Residential Funding Corp. v. DeGeorge Home Alliance, Inc.*, 2002 U.S. App. LEXIS 20422 (2nd Cir. Sept. 26, 2002) underscore just how crucial sound electronic discovery practices have become recently. These decisions vividly illustrate the potentially severe sanctions that may be issued for failure to understand the duties of electronic discovery, or failure to adopt a sensible electronic discovery response plan.

One of the most intimidating issues attorneys face today is how to carry out the obligations imposed by courts with regard to identification, preservation and potential production of information stored on clients' backup tapes. While natural instincts typically prevent attorneys from delving too deeply into technical matters, a basic understanding of the nature of information

continued on page 2

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

Managing Editor Carol L. Eoannou, ceoannou@pf.com
800/255-8131 ext. 269

Legal Editor Robert Emeritz, remeritz@pf.com
800/255-8131 ext. 258

News Editor Scott Sleek, ssleek@pf.com
800/255-8131 ext. 291

Contributing Editor Faith Ruderfer, fruderfer@pf.com
800/255-8131 ext. 288

Group Publisher Zachary Wheat, zwheat@pf.com
800/255-8131 ext. 229

Copy Editor Marie Unger

Layout and Design Manager Jennifer Andruzzi

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.

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.

Name _____

Title _____

Organization _____

Address _____

City _____ State _____ ZIP _____

Country _____ Phone _____

Fax _____ E-mail _____

Check enclosed (MD, NY and Canada: add sales tax; overseas: add \$33 for postage.)

Bill me (add \$20 for shipping)

Charge my: VISA AmEx Discover Diners

Card number _____ Exp. date _____

Signature _____

MAIL or FAX a copy to:
Digital Discovery, Pike & Fischer, 1010 Wayne Avenue,
Suite 1400 Silver Spring, MD 20910; 301/562-1521

continued from page 1

stored on backup tapes is essential to preparing an effective discovery response in nearly every case.

What Is a Backup Tape?

A backup tape (or any other form of backup media) is a copy of information generally made for the purpose of disaster recovery in the event of a system failure or natural disaster. Most companies back up computer files on a regular basis, and many computer networks utilize automatic backup software to make regular copies of some or all of the data that resides on the company's computer network.

Backups of computer data may be created with operating system commands or through use of a backup utility. Backup programs often compress data so that backups require a smaller amount of physical space on the backup media. The result of this compression is that unusually high volumes of files may be stored in a significantly smaller amount of space.

Backup tapes typically contain documents created by system users — e-mail messages, word processing documents, spreadsheets, database entries and the like — but also often include copies of the system files required to make the computer's operating systems function properly. Attorneys are almost always interested only in the actual documents created by the company's computer users. Understanding the nature of other types of files that may be present on a system backup is important to understanding the nature of information recovered from the backup media. A volume of information that may seem intimidating at first glance may actually contain a manageable amount of readable data for purposes of the discovery process.

An understanding of the volume of data contained on a backup tape must also consider what kind of backup was performed. Several common options include:

Full Backup—A complete backup of all information contained on the system.

This is the simplest type of backup and yields the most complete backup image.

Selective Backup—In a selective (or partial) backup, specific files and directories are selected for backup procedures. This provides more control over what is backed up. Selective backups are generally used to avoid backing up unnecessary program or system files and to focus on data files in known user directories, or when backup space is limited.

Incremental Backup—An incremental backup includes only those files that have changed since the last backup. It is like a selective backup, but the files are automatically selected based on whether they have changed recently, instead of an arbitrary selection based on directory or file names. This gives the time- and space-saving advantages of a selective backup while ensuring that all changed files are covered.

A mix of full and incremental backups is common in many companies. Any computer system is susceptible to occasional interruptions in service, but most users are fortunate enough to never experience a catastrophic system failure. Nevertheless, experts recommend that copies of important data be saved and stored in at least two separate locations.

Backup schedules and rotation of tapes can vary greatly from company to company, depending on the type and volume of files stored, the company's level of sophistication with regard to technical (and legal) matters, and numerous other factors.

What Should I Ask Clients About Their Backup Procedures?

In preparing any discovery response, an attorney must ask the client about information stored on backup tapes. The following questions will serve as a departure point for understanding the company's backup protocol, schedules, and volume and location of information stored that could be responsive in litigation.

- Does the company have a for-

malized backup protocol?

- If formalized in writing, obtain a copy.
- If set forth in writing, determine whether the written protocol is followed.
- If not set forth in writing, determine which company employee is responsible for backup procedures and immediately interview the employee to understand the backup protocol. This employee should also be prepared for the likelihood of a 30(b)(6) deposition.
- What is the company's backup schedule?
- A typical schedule might include a full backup once per week, with incremental backups made to capture new data on other days. At the end of each month, the weekly backups for the month might be replaced with one complete monthly backup. The tapes used to create the weeklies may then be put back into rotation (or "recycled") for storage of new data. This procedure is typically followed annually, so that a company would end each year with 12 full monthly backups and, ideally, no other incremental or partial backups.
- Determine whether the schedule is followed rigorously or whether variances are common.
- Does the company have a provision in its backup protocol for adhering to the company's document retention plan for electronic data?
- The IT department's definition of a "retention plan" (the period of history they want to keep on backups) is likely very different from the legal definition of "document retention." An early conversation between attorneys and the company's IT staff will help prevent breakdowns in communication on this vital issue.

While the rulings regarding duties related to the identification, preservation and production of information contained on backup tapes are not entirely consistent around the country, courts will generally apply a reasonableness standard in determining whether a party has met its discovery obligations. Unfortunately, the interpretation of "reasonable" varies from court to court.

- Determine whether the company has a formal document retention plan. If so, obtain a copy of any written guidelines and immediately determine whether they are being followed.
- If no document retention plan is in place, meet with the client's technical staff immediately to determine whether computer data is being overwritten or otherwise deleted in accordance with the company's backup protocol. Be sure procedures are in place to avoid any claims of negligent or intentional spoliation.
- A document retention plan will typically include a procedure for halting the rotation or recycling of backup tapes on the daily, weekly or monthly schedule. Consider the company's practices and immediately determine whether the company's usual procedures must be interrupted.
- Where is the company's backup data stored?
- Many companies store more than one copy of backup data. If this practice is followed, determine where each copy of the backup media is stored.

- Ideally, backups are kept in a locked place away from the company's primary place of business. Ask about offsite storage, as well as any "interim" storage facilities that may be used.

Preparing to Respond to Requests for Information Stored on Backup Tapes

Once you have a working knowledge of your client's backup practices, you are prepared to consider the legal issues relevant to discovery of information from the backup tapes. The case law surrounding the practice of electronic discovery is developing rapidly. While the rulings regarding duties related to the identification, preservation and production of information contained on backup tapes are not entirely consistent around the country, courts will generally apply a reasonableness standard in determining whether a party has met its discovery obligations.

Unfortunately, the interpretation of "reasonable" varies from court to court. For example, a company may have a longstanding "document retention and destruction policy" under which it regularly recycles backup tapes. One judge may find it reasonable for the company to continue to recycle backup tapes in the absence of a specific preservation order or discovery request, while another judge may determine that the usual procedures must be halted once the party is on notice of litigation. Preparing for the possibility of either ruling is critical.

Be Proactive—Prepare Early and Confer Often

The best way to avoid a discovery dispute concerning information on backup tapes is to prepare for all possibilities. With information about the client's backup protocols outlined in response to the questions above, an attorney is ready to confer with opposing counsel about the electronic discovery issues in the case.

While an attorney may initially be reluctant to raise the issue of backup data to opposing counsel (hoping that

the request for such data will never arise), the consequences of failing to address the issue early in the case can be disastrous. In fact, the “mandatory disclosure” provision in Fed. R. Civ. P. 26(a)(1) specifically requires parties to identify (in advance of a discovery request) any computer-based information that may be used to support the party’s claims or defenses in the case. In almost all cases, you will want to examine backup data for information to support your client’s position.

Sanctions for failing to preserve and produce data from backup tapes have ranged from monetary penalties to adverse jury instructions to judgment on the merits. In recent cases, attorneys have been required to demonstrate that personal attention was paid to the proper identification and review of information stored on clients’ computer systems.

Document Your Electronic Discovery Plan

Once the client’s backup procedures are understood, it is wise to document the electronic discovery protocol you intend to follow in the case. This plan should include an outline of the issues considered, client representatives consulted and conclusions reached. If you and your client determine that continuation of the company’s regular backup procedures (including recycling of tapes on a predetermined basis, etc.) is appropriate, be prepared to defend the decision. Likewise, if you determine that

While an attorney may initially be reluctant to raise the issue of backup data to opposing counsel (hoping that the request for such data will never arise), the consequences of failing to address the issue early in the case can be disastrous.

regular procedures must be halted, even temporarily, you should be armed with information about the potential costs to the company in so doing. You will be better positioned to seek relief from undue burden and extraordinary costs if you are well informed about the client’s backup protocols and can present opposing counsel with a proposed plan for handling electronic data in discovery. Securing agreement about electronic discovery protocols early in the case is the best-case scenario.

If You Foresee Difficulties, Ask the Court for Guidance

Discovery is contentious in many cases, and opposing counsel may be unwilling to agree to any plan set forth. If this situation arises, attorneys are wise to affirmatively seek guidance from the court rather than wait for a motion to compel. Courts routinely look with favor on a party that is well aware of its electronic discovery obligations and has taken necessary steps to educate ev-

eryone involved about issues that will be relevant to the case. The simple act of setting forth an electronic discovery plan and seeking approval from the court will make a significant difference in how your client is positioned should discovery disputes arise in the case.

Conclusion

Discovery of information from backup tapes is no different from discovery of information from any other source. Whether the documents originate from a file cabinet, a computer hard drive or media used to store data for backup procedures, the same rules of discovery apply. An attorney’s obligations are enhanced, however, by the need to understand the language of clients’ computer systems. Pleading ignorance to the issues surrounding electronic discovery will no longer suffice in any court. Conversely, attorneys who demonstrate a competent working knowledge of their clients’ computer systems and a sincere effort to address these issues in a proactive fashion will fare well in any jurisdiction.

Virginia Llewellyn, Esq., is director of Industry Relations for Applied Discovery, Inc. She can be reached at virginia.llewellyn@applieddiscovery.com. For further research on the topic of electronic discovery and production of information from backup tapes, visit the online Law Library at www.applieddiscovery.com.

Invitation to Authors

The publishers of *Digital Discovery and e-Evidence* invite attorneys, academics, and producers and vendors of litigation support products and services to submit for publication articles addressing the discovery, production, and presentation of evidence in the digital age. Good candidates for publication are articles on the best practices for: discovering electronic data, choosing forensic experts, and establishing efficient, cost-effective policies for maintaining and deleting electronic records in an organization.

Prospective authors may contact Carol L. Eoannou by telephone at (301) 562-1530 ext. 269, by fax at (301) 562-1542, or via the Internet at ceoannou@pf.com.

Mastering the Use of E-Discovery Special Masters

By George Socha

Special masters have been used in complex litigation since long before evidence began residing in electronic form. Rule 53 of the Federal Rules of Civil Procedure allows judges to appoint special masters in any pending action (F.R.C.P. 53(a)) and the appointment may be made on the court's own initiative or at the request of the parties. It's a safe bet that judges—and parties—will make increasing use of that authority now that e-discovery has become so integral to trial preparation.

Pursuant to F.R.C.P. 53(c), the court may delegate broad powers to the special master or limit them to a narrow scope of activities. Masters may be empowered, for example, to require the production of evidence, including evidence in electronic form, rule upon the admissibility of that evidence, examine witnesses under oath, and report to the court. *Id.*

Generally, however, the use of special masters is discouraged: "A reference to a master shall be the exception and not the rule. In actions to be tried by a jury, a reference shall be made only when the issues are complicated; in actions to be tried without a jury ... a reference shall be made only upon a showing that some exceptional condition requires it." F.R.C.P. 53(b).

Nonetheless, electronic discovery has been recognized as one of those areas where the use of a special master can be appropriate. See, e.g., *Playboy Enterprises v. Welles*, 60 F. Supp.2d 1050 (S.D.Cal. 1999); *Simon Property Group v. mySimon Inc.*, 194 F.R.D. 639 (S.D.Ind. 2000). Some familiarity with their function is therefore crucial for the litigator charged with seeking or producing electronic evidence.

Appointing an E-Discovery Special Master: Considerations for Courts

Courts should take the following factors into account in deciding whether to appoint an electronic discovery special master:

- How complex, arcane and technical are the electronic discovery issues in the case, and how steep will the learning curve be for the judge? Is the court technologically sophisticated enough to handle them just as it does the broad range of disputes laid at its door each day? Or are they issues which the court will understand only after study and training for which it has neither the time nor the financial resources?
- What level of expertise do counsel and their clients possess? Do the attorneys appearing before the court appreciate the distinctions between electronic media and electronic format? Do they grasp the challenges

In theory, a special master should bring to bear a more in-depth understanding of issues specific to electronic discovery. The special master also should have a better ability to cut through the other side's techno-babble. Finally, the special master should be able to suggest a broader range of realistically effective solutions.

faced by a large corporation trying to implement a hold on any destruction of electronic materials? Are they sufficiently versed in the operation of computer networks to distinguish between the client who really cannot find all e-mail messages to, from or mentioning any of a list of 50 former employees and the client's information services personnel who simply do not want to deal with temporary inconvenience and disruption to carry out a task whose value they do not understand and whose significance they do not appreciate?

- If the court does not refer those issues to a special master, how effective will the court, the attorneys and the parties be in resolving them in an expeditious, cost-effective manner?
- If the court does refer those issues to a special master, how likely will it be that a special master will be able to bring the parties to a point where they can agree on a process they can manage themselves?
- If the parties cannot agree on such a process, what is the likelihood that a special master will be better equipped than a judge to guide the parties to a solution?
- Are there so many electronic discovery issues that the court will have difficulty devoting sufficient time to understand and resolve them?
- How much electronic information is at issue and how potentially significant is that information for the defense or prosecution of the case?
- Will the costs of gathering and producing electronic information be great enough to justify the special master's fees and the costs of appearing before and possibly working under the direction of the special master?
- How interested are the parties in retaining and relying upon an electronic discovery special master?

Considerations for Parties

Parties considering whether to request an electronic discovery special master should perform a similar evaluation. In theory, a special master should bring to bear a more in-

depth understanding of issues specific to electronic discovery. The special master also should have a better ability to cut through the other side's techno-babble. Finally, the special master should be able to suggest a broader range of realistically effective solutions.

At the same time, engaging a special master means greater costs, such as paying a share of the special master's fees, and potentially arguing a position twice, once before the special master and a second time before the judge.

Making the Selection

When selecting an electronic discovery special master, consider the following attributes:

- Special master experience, in electronic or "regular" discovery; mediation or arbitration training.
- Experience as an electronic discovery or automated litigation support expert witness or court-appointed neutral.
- Familiarity with the litigation process: How well does the special master understand the litigation process, from initial investigations to final appeals? (Someone with extensive technical expertise but no appreciation of due process probably would be better used as a court-appointed neutral expert charged with carrying out forensic computer work based on guidelines agreed upon by the parties, suggested by a special master, or ordered by a court.)
- Experience with electronic discovery, from initial attempts at identifying and preserving relevant electronic information through presentation of digital information at oral arguments, trials, and the like. Experience with litigation does not in itself qualify one to serve as a special master focusing on electronic discovery issues; an understanding of electronic discovery is crucial.
- Temperament: Does the potential special master "play well with others?"
- Independence and neutrality: Does it matter to the parties, their counsel and the court whether the special master is associated with a law firm? What if the firm does primarily defense work, or, alternatively, principally plaintiffs' work? Is a connection with an electronic discovery vendor positive, problematic, or simply irrelevant? No matter how you come out on these issues, you must also ensure that the special master performs an adequate conflict search.
- Availability: Do you need someone who will be there in person, or is face-to-face contact only a minimal consideration? Will the engagement demand a substantial amount of the special master's time, and if so, for how long?

Engaging a special master means greater costs, such as paying a share of the special master's fees, and potentially arguing a position twice, once before the special master and a second time before the judge.

- Support: Is this a situation where a single person with in-depth expertise will suffice, or do you need someone with the backing of a larger organization?
- Cost: Rates will vary based on experience and background, degree of expertise, availability, overhead, geographical location, and the like. When considering costs, remember to factor in travel expenses, legal research charges, phone and fax charges, and other incidental costs.
- Reputation: For each of these areas, what type of reputation does the special master enjoy (or suffer from)?

Getting Started

If a court refers electronic discovery issues to a special master, it should issue a written order. The order should describe the degree of authority the court is delegating to the special master. Will the role of the special master be limited to hearing disputes involving electronic discovery and issuing rulings that the parties either follow or appeal to the judge? Will there be adversarial hearings intended to result in findings of fact by the special master? Will the special master be accorded a role more akin to a mediator, who tries to prevent the parties from simply locking horns and encourages solutions arrived at through consensus born of a common realization that neither side is as duplicitous nor as clueless as the other had thought and that each side had reasonable, if not ultimately correct, bases for the views it held going into the discovery dispute?

The order also should identify the scope of work the special master will perform. What issues will the special master consider? Will they be limited to ones explicitly raised by the parties? Will they also include issues of concern to the court? To what extent will the special master be involved in decisions such as who gathers electronic information, what procedures are used to gather the information, what means are used to process it, where it gets stored, who has access to it, and who pays the costs associated with each of these aspects of electronic discovery? Will the special master also have a role in less traditional areas such as developing electronic discovery protocols, not just endorsing but directing the selection and implementation of a repository of electronic information?

In addition, the order should set forth the procedures for the court's review of the special master's actions or decisions and include the standard for review. The order should also establish a mechanism by which the special master re-

ports back to the judge. Finally, the order should make specific provision for the special master's compensation.

Conclusion

If selected carefully and used effectively, an electronic discovery special master can be a powerful tool for court and parties alike. That special master should bring to bear a depth of expertise unlikely to be found among any but the most technologically advanced judges and magistrates. With that expertise, the special master should be able to help each party better understand the other party's positions and problems, cut through apparently convincing but technically

specious arguments, and pursue solutions that move the electronic discovery process along more expeditiously, more efficiently, and more justly.

George J. Socha Jr. is a shareholder at Halleland Lewis Nilan Sipkins & Johnson, in Minneapolis, Minnesota. His practice focuses on complex commercial, toxic tort, and products liability litigation. He has been selected as an expert witness on issues relating to automated litigation support and electronic discovery, including electronic discovery, data manipulation and complex information management. He can be reached at gsocha@halleland.com.

Case Law & Regulation

One Bite at the Backups

McPeek II Sets Out Additional Principles of Relevancy

McPeek v. Ashcroft, 2003 WL 75780 (D.D.C., decided January 9, 2003)

A Department of Justice (DOJ) employee claiming that he was the object of retaliation after accusing his supervisor of sexual harassment was not entitled to a second search of the DOJ computer backup system for evidence of retaliation. In light of the condition of the backup tapes and the small likelihood that another search would produce evidence relevant to the employee's claim, the time and expense of a subsequent search was not justified.

An earlier opinion arising out of the same dispute, *McPeek v. Ashcroft*, 202 F.R.D. 31 (D.D.C. 2001), *DDEE*, October 2001 (*McPeek I*) is considered to be among the most significant in the development of case law regarding allocating the costs of electronic discovery. In *McPeek I*, Magistrate Judge John F. Facciola permitted the plaintiff to search certain backup tapes to establish whether any further searches would be fruitful. After the initial search was completed, DOJ discovered that only certain backup tapes remained available.

Called into the fray once more, Magistrate Facciola begins from the premise that the appropriateness of an additional search depends on how likely it is that the word processing documents and e-mails residing on the available tapes will produce information that is relevant to the lawsuit. For purposes of a workplace retaliation suit, explains Magistrate Facciola, "relevant data" would have to mean data making it more likely than not that the true motive for the acts about which plaintiff complains was retaliatory.

Good News, Bad News

The good news is that the acts plaintiff complains of

occurred within a well-defined period: between October 1994 and July 1998 when the plaintiff experienced retaliation for complaining about being sexually harassed, and after July 2, 1998 (the date of plaintiff's formal letter complaint about the retaliation) until January 12, 2002, when plaintiff's counsel informed the defendant of his intention to file the instant lawsuit. It would therefore seem that crafting a discovery request regarding events so well-placed in time would be relatively straightforward, even if the documents sought existed only in electronic form.

Magistrate Facciola points out, however, that one characteristic of backup materials makes them frustrating from an electronic discovery perspective: they collect information indiscriminately, regardless of topic, making it impossible to reasonably predict what information is likely to be on a particular tape. "In this case," he adds, "there is the additional frustration that the tapes that do exist do not exist for clearly defined chronological periods but instead exist for certain days, without any rhyme or reason for their continued existence."

Plaintiff advocates searching all the tapes in existence for the relevant periods of time. Magistrate Facciola rejects that approach out of hand, cautioning that:

"The likelihood of finding relevant data has to be a function of the application of the common sense principle that people generate data referring to an event, whether e-mail or word processing documents, contemporaneous with that event, using the word 'contemporaneous' as a rough guide. Conversely, it is unlikely that people, working in an office, generate data about an event that is not contemporaneous unless they have been charged with the responsibility to investigate that event or to create some form of history about it."

Here, relevant data would consist of data that contains explicit references to the sexual harassment complaint, the letter dated July 2, 1998, or counsel's January 12, 2000 ex-

pression of intent to file suit, or data that bears on the justification for the actions plaintiff claims were retaliatory.

For all of the available tapes, Magistrate Facciola compares their dates with the dates pertinent to the development of the plaintiff's case. Finding little or no congruence among the dates, he denies the subsequent search.

Editor's Note: Read together, the two *McPeck* decisions provide an excellent primer on relevancy and cost allocation in the context of electronic discovery.

Preservation Order Upheld

California Appeals Court OKs Injunction Preserving E-Evidence, Giving Expert Access

Dodge, Warren & Peters Ins. Services Inc. v. Riley, Cal. Ct. App., 105 Cal. App. 4th 1414, 130 Cal. Rptr. 2d 385, 3 Cal. Daily Op. Serv. 1171, 2003 Daily Journal D.A.R. 1447, decided February 5, 2003

A trial court properly granted a preliminary injunction to preserve electronic evidence taken by departing employees, and requiring them to allow a court-appointed expert access to the files, a California Court of Appeal ruled Feb. 5.

Dodge, Warren & Peters Insurance Services Inc. in Ontario, Calif., fired four broker-agents and sued them for misappropriation of trade secrets, unfair business practices, breach of fiduciary duty, and breach of contract. The San Bernardino County Superior Court granted the firm's motion for a preliminary injunction barring the former employees from deleting or destroying any of the electronic files and requiring them to allow a court-appointed expert to copy the files and attempt to restore any deleted files.

Approving the injunction, the appeals court found Dodge, Warren & Peters is likely to prevail on its claim that it has a right to discovery of the electronic files, which may contain admissible evidence. Writing for the panel, Justice Manuel A. Ramirez found that, without the injunction, "Dodge could irretrievably lose evidence that otherwise would have been available to it," while any harm to the former employees would be negligible. Justices Thomas E. Hollenhorst and Betty A. Richli joined in the opinion.

Electronic Data Requested

James Riley and Garrison Gershon, while still employed by Dodge, Warren & Peters, began preparing in December 2000 to start their own firm. They discussed their plans with fellow employees Sandra McGovern, Patricia Anaya, and Parthena Yorke, who also decided to leave and join the new firm. They admit that they photocopied numerous documents and copied many computer files onto discs, which they took for use at the new firm.

Dodge fired the five employees on Jan. 21, 2001, when it

learned of their plans to open their own shop. Gershon subsequently returned to Dodge and told the firm about the copied documents and computer files. Dodge sued the other four former employees in February 2002, bringing various trade secret, contract, fiduciary duty, and unfair business practice claims.

The firm served the four former employees with requests for the production of documents, including computer files, and requested a preliminary injunction to "freeze" the electronic data. It argued that the former employees, by merely using the files, could accidentally destroy potential evidence. The superior court issued the injunction and denied the former employees' request for a protective order to limit the search.

Preventing Spoliation

An injunction may be granted when it appears that a party in a case is doing, or is about to do, something that would violate the rights of another party, including the right to discovery of relevant evidence, Ramirez explained. "We cannot conceive, as a matter of policy, given the broad discretion possessed of the trial court to ensure the effective administration of justice, why injunctive relief should not be available under circumstances such as these, should it otherwise be merited," he said.

The former employees argued an injunction is not necessary because Dodge has an adequate legal remedy under California's Civil Discovery Act of 1996. However, Ramirez found they "failed to establish that the Discovery Act provides any protection such as that sought by Dodge." That law does not provide any mechanism for the preservation of evidence and "does not specifically authorize the trial court to act on behalf of the party seeking evidence," the judge said.

In *Cedars-Sinai Med. Ctr. v. Superior Court*, 954 P.2d 511 (1998), the California Supreme Court declined to recognize a new tort claim for intentional spoliation, meaning destruction or alteration, of evidence. Although the Supreme Court acknowledged that trial courts can impose evidentiary and monetary sanctions for discovery abuse, the court "certainly did not suggest that a litigant could do nothing to prevent spoliation from occurring, but could only react after the fact," Ramirez said. Specifically, the state supreme court did not disapprove of injunctive relief as another non-tort alternative.

Dodge will likely prevail on its argument that it has a right to discovery of the electronic files to look for evidence to support its claims, Ramirez decided. He pointed out that the former employees admitted copying Dodge's paper and computer files. The Discovery Act specifically "authorizes inquiry into even irrelevant matters so long as their revelation may lead to the discovery of admissible evidence," Ramirez said.

Dodge showed it could irretrievably lose evidence and it has no other legal remedy that would provide adequate relief, Ramirez said. By contrast, he found any harm to the former employees would be "negligible" because the injunc-

tion requires that the copying be done in their presence and after working hours. “The copied material would be unavailable to anyone except upon agreement of the parties or order of the court,” Ramirez said. Finally, he pointed out that the injunction requires Dodge to pay for the cost to the former employees of reviewing the copied files to identify irrelevant or privileged documents.

Raymond A. Greenberg of Calabasas, Calif., represented Riley. Perry Fredgant of Woodland Hills, Calif., represented McGovern, Anaya, and Yorke. Trenton J. Hill of Jones, Bell, Abbott, Fleming & Fitzgerald in Los Angeles represented Dodge, Warren & Peters.

No Harm, No Foul

No Reasonable Possibility Missing Hard Drives Contained Evidence of Theft of Trade Secrets

Hildreth Mfg., L.L.C. v. Semco, Inc., Ohio App. 3 Dist., 2003 WL 359309, decided February 20, 2003

In the course of litigation stemming from the acrimonious dissolution of a manufacturing concern, the court was called upon to resolve an e-discovery dispute that arose from a temporary restraining order that prohibited the plaintiff and its employees from using any materials they obtained from the defendant. The restraining order also prohibited them from “destroying, concealing, or altering in any fashion any documents,” including those contained on the hard drives of their computers.

The Facts

The plaintiff corporation was headed by the son of one of the founding partners of the original company. He had worked at the defendant corporation almost since its inception, ultimately holding the positions of vice-president and plant manager. He started his own operation, manufacturing the same type of machine part, while his father was negotiating the sale of his stock in the original company to his partner, who continued in business. When several employees left the original company and went to work for the son, the remaining elder partner began to suspect that one of them had placed the company’s computer files on a magnetic tape and brought them to the son’s company in an effort to misappropriate trade secrets and private customer information. The son’s response to a letter memorializing these suspicions was to seek a declaratory judgment that the defendant had no trade secrets or confidential information prior to the date the father sold his stock, and that even if such information existed, the plaintiffs hadn’t misappropriated or improperly used it.

Shortly after discovery commenced, the defendant corporation filed a motion for contempt and for sanctions, alleging that the individually-named plaintiffs had willfully

destroyed the hard drives of their company computers in direct violation of the temporary restraining order, which was still in effect. The motion was based on defendant’s examination of plaintiff’s computers, undertaken in connection with efforts to copy their images in order to determine whether the allegedly misappropriated information was subsequently placed on plaintiff’s hard drives. The drives the defendants planned to image included “Mazak” hard drives, which were purchased after the temporary restraining order was issued and are used to operate lathe equipment.

Imaging of the desktop computers proceeded uneventfully, but plaintiffs objected to efforts to image the Mazak drives on the grounds that doing so could damage them and lead to employee injury if the lathe equipment subsequently malfunctioned. Before the court could rule on the objection, a representative of the Mazak supplier removed the Mazak hard drives and replaced them with different ones. Although plaintiffs did not protest this action, they were unaware that the supplier subsequently erased the Mazak drives and redistributed them to other customers.

Spoliation?

The erasure and redistribution was the basis of the motion for contempt for spoliation of evidence. The trial court found that the plaintiff failed to properly preserve the requested evidence but that there was not a reasonable possibility that the missing hard drives contained evidence that would have been favorable to defendant’s claims. In overruling the motion for contempt, the trial court determined that it was “nonsensical to believe that [plaintiff] would place purloined computer information on its Mazak computers, which were obtained after the issuance of the temporary restraining order, knowing that [defendant] sought to image these computer hard drives.”

The court of appeals agreed. Writing for the panel, Judge Stephen R. Shaw finds the trial court’s decision did not evidence “perversity of will, defiance of judgment, . . . the exercise of passion or bias” or an “unreasonable, arbitrary or unconscionable” attitude. Judge Shaw acknowledges that the defendant “may” have enjoyed a presumption that it was prejudiced by the destruction of the hard drives, but concludes that “the court was well within its discretion to determine that [plaintiff] adequately rebutted that presumption by showing that a reasonable possibility did not exist that access to the requested evidence would have produced evidence favorable to [defendant], which was otherwise unattainable.” The appeals court essentially endorsed the trial court’s finding that because downloading information known by the plaintiffs to be sought by the defendants would have been extremely foolish, they would not have done so and, accordingly, the evidence in question did not exist on the Mazak hard drives.

Also at issue was a machining database that one of the employees who joined the son in the new venture allegedly copied before resigning from the original company. Defen-

Case Law & Regulation

dant contended that the database of programs necessary to produce products to a customer's satisfaction was a trade secret. It attempted to prove the copying through the testimony of a computer consultant whom the employee had hired to create a backup tape of his computer hard drive, which contained the machining information. The consultant testified that he made a backup on one tape, showed the employee how to perform the operation, and then left the backup and an additional tape with the soon-to-defect employee. After the employee's departure, however, only one tape was found, which the defendant claimed demonstrated that the employee misappropriated information from his computer.

In rejecting this argument, Judge Shaw points out that no evidence was presented that the employee actually made a second backup or removed anything from the workplace that he was not supposed to. Moreover, the employee's computer did not require a password and others had access to the computer in question during the employee's tenure. That the consultant brought an extra tape that was never located—the only evidence conclusively presented—was insufficient to prove that the employee engaged in misappropriation.

Search and Seizure

Warrant for Text Files Relating to One Crime Does Not Cover Image Files Relating to Another

New York v. Carratu, 2003 WL 230674 (N.Y. Sup., decided January 23, 2003)

A criminal defendant's motion to suppress physical evidence raised the issue, novel in New York, of whether a warrant authorizing a search of the text files of a computer for documentary evidence pertaining to a specific crime will authorize a search of image files that appear to contain evidence of other criminal activity. The court ruled in favor of the defendant, granting his motion to suppress the image files.

After the defendant had been arrested for selling illegal cable television access devices, warrants were issued authorizing searches of a residence and a post office box. They authorized searches at both locations for devices capable of defeating the security and encryption system of a cable television, devices capable of de-scrambling telecommunications intended for use by cable television subscribers, and related parts and equipment, installation manuals, and computers and computer diskettes used in connection with the illegal cable scheme. In the course of executing the warrants, the police discovered physical materials which strongly suggested that the defendant was also engaged in an enterprise to manufacture phony identification cards. Among the items seized by the police were three computers.

The court describes the forensic examination of the computers as follows:

“The initial procedure was to make a copy of the hard drive for each of the systems. Since the Toshiba laptop was protected by a password, it was necessary to remove the hard drive from the Toshiba and attach it to a separate computer in order to copy the hard drive. Then the directory for each of the hard drives was displayed, and the folders for each hard drive were listed alphabetically. Finally, the detective opened each folder and examined each user-generated file to determine whether it contained evidence pertaining to the illegal cable box operation. Within the folders themselves, [the detective] observed web pages downloaded from a website for cable boxes. In a folder labeled ‘Fake I.D.’ on the Sony hard drive, the detective observed image files of driver's licenses, social security cards, inspection stickers, and registration certificates. Another driver's license image was also found in a folder called ‘My Documents.’ In another folder labeled ‘customers’ found in the Toshiba computer, the detective observed a file referring to Creative Alarms. In a folder labeled ‘DSS,’ the detective observed text files which appeared to relate to satellite television.”

The defendant claimed that the search of his computers exceeded the scope of the warrant because no effort was made to first examine the files or directories that by their name or nature might indicate some type of record or list. Nor was any attempt made to ascertain whether the files at issue contained graphic, data base, spread sheet or word processing product.

In ruling, the court relied on the particularity requirement of the Fourth Amendment, as interpreted in *United States v. Carey*, 172 F.3d 1268 (10th Cir. 1999), which held that a warrant authorizing the search of the text files of a computer for documentary evidence pertaining to a specific crime will not authorize a search of image files containing evidence of other criminal activity. Here, the warrant and supporting affidavit made clear the warrants authorized a search of the computers for documentary evidence relating to the defendant's illegal cable box operation. There was no ambiguity in the labeling of the “Fake I.D.” folder; it clearly indicated that it probably contained false identification documents rather than records of the sale of illegal cable boxes. Mere inspection of the folder name gave the detective probable cause to seek a further warrant authorizing a search of the Sony computer for evidence of possession of forged instruments. Moreover, since the name extenders of the files in the Fake I.D. folder made it likely they contained images, it was unlikely they were text files sought by the warrant. Finally, the state's reliance on the plain view doctrine was misplaced, since none of the image files containing false identification documents was inadvertently discovered.

Germany

Hard Copies of E-Mails Not Hard Evidence

By Dorothea Kettrukat

According to a recent decision of the Local Court of Bonn, the possibility that hard copies of e-mails may be manipulated prevents them from necessarily possessing evidentiary value in court (Case File 3 C 193/01).

Facts

The parties to a sales contract disagreed about whether they had resolved the issue of a commission for the plaintiff during their contract negotiations. In the hearing, the plaintiff introduced as evidence hard copies of e-mails allegedly sent by the defendant. The court held that, independent of the fact that the defendant denied having sent these e-mails, the hard copies themselves did not possess any evidentiary value. According to the court, it is commonly known that the content of e-mails is susceptible to manipulation. The court further argued that even if these e-mails actually had been sent by the defendant, there was still the chance that parts of the e-mail had been altered by a third party. Based on this reasoning, the court refused to accept the hard copies as sufficient evidence.

Evidentiary Value of Electronic Documents Under German Law

If the e-mails had been signed with a “digital signature,” the outcome of the case would probably have been different. Section 292a of the German Act of Civil Procedure (*Zivilprozessordnung*, hereafter “ZPO”) sets forth that electronic messages signed with a “qualified electronic signature” possess evidentiary value as *prima facie* evidence. The value of this category of evidence can only be diminished by presenting facts that are sufficient to cast serious doubt on it. If in this case the plaintiff had presented e-mails bearing qualified electronic signatures, they would not have been deemed inadmissible on defendant’s mere claim that the sender had been victim to the attack of a hacker or that a third party had gained unauthorized possession of the private signature key; such allegations would have had to be proven.

The qualified electronic signature is defined in Section 2 No. 3 of the German Signature Act (*Signaturgesetz*, hereaf-

ter “SigG”). It has to meet the requirements for an advanced electronic signature as stated in Section 2 No. 2 SigG, i.e., it

- is exclusively assigned to the owner of the signature code;
- enables the owner of the signature code to be identified;
- is produced with means which the owner of the signature code can keep under his sole control; and
- is so linked to the data to which it refers that any subsequent alteration of such data may be detected.

As stated in Section 2 No. 3 SigG, the qualified electronic signature is further based on a qualified certificate valid at the time of its creation and has been produced with a secure signature-creation device.

If, however, an electronic document has not been signed with a qualified electronic signature, its evidentiary value is judged according to Section 371 Para 1 ZPO. This provision sets forth the rules for the evidence by inspection, while the inspection procedure regarding electronic documents is specifically addressed by Section 371 Para. 1 Sent. 2 ZPO. The relevant part reads as follows:

“[...] If an electronic document is the object of the evidence, the submission of such evidence will have to be performed by either presenting or transferring the file.”

Such electronic documents do not qualify as *prima facie* evidence and provide only lesser evidentiary value. Their conclusiveness solely depends on the judge’s discretion when examining the document; therefore, the outcome of the evaluation may differ with each case. The Labor Court of Frankfurt, for example, had ruled that exchanged e-mails may be used as bases for determining whether the payment of a certain sum satisfied claims in the context of a labor contract (case file 7 Ca 5380/01).

In view of this uncertainty in jurisprudence, it is advised—especially in the context of large transactions or complex contracts—to agree on the use of qualified electronic signatures in order to ensure the evidentiary value of the exchanged electronic documents, unless the circumstances of the situation and/or the will of the parties demand the use of the traditional handwritten paper form.

The author is an attorney with Baker & McKenzie, Frankfurt. She may be reached by telephone at +49-(0)69-29908-616 or by e-mail at dorothea.kettrukat@bakernet.com.

Practice Tip

Plaintiff in an age discrimination in employment action sought discovery of a “computer diskette or tape copy of all word processing files created, modified and/or accessed by or on behalf of” five fellow employees over a two and one-half year period, which was roughly the length of plaintiff’s tenure with the defendant employer. Despite the time and source parameters plaintiff placed on his discovery request, the district court for the Northern District of Alabama denied it on the grounds of over-breadth, undue burdensomeness, and failure to make a reasonable showing of relevance. The Eleventh Circuit Court of Appeals affirmed this decision, characterizing plaintiff’s discovery request as “expansive.” Pointing out that “discovery in Title VII cases is not without limits,” the court suggests that the plaintiff should have (1) identified particular items rather than seeking all word processing files and (2) provided a theory of relevance to narrow the scope of his request. *Wright v. Amsouth Bancorp.*, ___ F.3d ___, 2003 WL 245588, 16 Fla. L. Weekly Fed. Cir 275 (11th Cir, 02/05/03).

Attorneys’ Fees

An Illinois trial court applied the correct evidentiary standard of proof when it accepted copies of computer-generated bills in an action to recover attorneys’ fees under ERISA. According to the attorney’s affidavit, he was unable to produce his original time records because they were “preliminary notes on scraps of paper,” the information from which was inputted into a computer that used software to generate a bill for each client. In this case, the court was not required

to follow Illinois precedent, which requires that when computer-generated documents summarizing the originals, such as time slips, are sought to be admitted, the original documents must either be presented in court or made available to the opposing party. Since the attorneys’ fees award was based on a federal statute, federal law governed the evidentiary decision. The federal common law provides that contemporaneous records are not required where the court finds that noncontemporaneous records accurately reflect amount of time actually expended by counsel. The documentation presented in support of the instant fee petition included affidavits from counsel and oral testimony presented at an evidentiary hearing on the petition. Accordingly, there was no abuse of discretion and the trial court’s decision to award fees is affirmed. *Cress v. Recreation Services, Inc.*, ___ N.E. 2d ___, 2003 W.L. 188128 (Ill. App., 2d Dist., 1/28/03).

Heightened Foreseeability of Criminal Act Not Evidenced by E-Mails

Two e-mails describing a potentially dangerous situation in Somalia were not sufficient evidence that the murder of an aid worker was a highly foreseeable act. Accordingly, under District of Columbia law, which emphasizes the foreseeability element of the required proof, the relief agency with whom the worker contracted could not be held liable for the worker’s death.

One month prior to her fatal trip, the worker sent her agency contact in the United States an e-mail in which she described some irregularities in the accounting of relief funds and expressed concern over the reception her investigation of the irregularities would receive. She wrote in part: “This could be a

Digital Discovery & e-Evidence Order Form

Mail: 1010 Wayne Ave., Suite 1400, Silver Spring, MD 20910-5600

Fax: 301-562-1521 • Tel: 800-255-8131 ext. 237 • E-mail: pike@pf.com

YES! I need the most current and comprehensive legal and technological information on digital discovery and electronic evidence. Begin my one-year subscription to Pike & Fischer’s Digital Discovery & e-Evidence at the introductory rate of \$449—a \$100.00 savings off the normal rate of \$549.

Payment Options: Visa MasterCard American Express Bill me Payment enclosed
Card Number _____ Expiration Date _____

Authorized Signature _____

(Please note: Your credit card statement will show a charge by Pike & Fischer, Inc., publisher of DDEE.)

Name _____ Organization _____
Address _____ City _____ State _____
ZIP Code _____ Telephone _____ E-Mail _____

(Add appropriate sales tax if located in Maryland or New York. In Canada, please add appropriate GST.)

very sensitive (not to mention dangerous) issue as we try to confirm some of these things . . . , particularly if the local people begin to suspect that they never received all of what . . . was supposed to [be] provide[ed]. They have told me that a hostage/kidnapping situation would not be farfetched, and I am sure you would be as unhappy receiving a midnight phone call for help as I would be if I had to make one.” The worker wrote a second e-mail to a longtime employee of the agency, which read, in part: “I feel like I am at the breaking point with no support system or release valve. The way things are going it wouldn’t surprise me if something happened in Somalia.”

The appeals court explains that in the District of Columbia, a defendant may be liable for harm caused by the criminal act of another only if the crime were particularly foreseeable. A demanding “heightened showing” of foreseeability

must be precisely proven. The court has rarely found evidence that satisfies this high standard.

The problem with the first e-mail is that it fails to demonstrate that the contingency that the worker feared might put her in danger, i.e., that the local people might begin to suspect that they hadn’t received all the aid to which they were entitled, ever materialized. The second e-mail fails because there was no evidence that the recipient was an agency employee at the time she received it, nor that its contents were ever conveyed to anyone at the relief agency. In short, the e-mail messages did not put the agency on notice of the danger that eventuated. *Workman v. United Methodist Committee on Relief of the General Board of Global Ministries of the United Methodist Church*, __ F.3d __, 2003 WL 431869 (D.C. Cir, 02/25/03).

continued from page 1

Sanctionable Actions

The underlying action was a fairly straightforward labor dispute: the opera company alleged the union distributed false, misleading, and defamatory leaflets and letters in an effort to unionize restaurant workers in the company’s employ. The discovery process, however, was “qualitatively different.” Judge Preska explains, “It presented the unfortunate combination of lawyers who completely abdicated their responsibilities under the discovery rules and as officers of the court and clients who lied and, through omission and commission, failed to search for and produce documents, and indeed, destroyed evidence, all to the ultimate prejudice of the truth-seeking process.” Specifically, the judge cited the union for the following:

- The union’s counsel repeatedly represented to the court that all documents responsive to the company’s document requests had been produced, when, in fact, a thorough search had never been made and counsel had no basis for so representing.
- Counsel knew the union’s files were in disarray and that it had no document retention policy but failed to cause a retention policy to be adopted to prevent destruction of responsive documents, both paper and electronic.
- Counsel failed to explain to the nonlawyer in charge of document production that “document” included drafts and other nonidentical copies and included documents in electronic form.
- The nonlawyer in charge of document production failed to speak to all persons who might have relevant documents, never followed up with those he did speak to, and failed to contact all of the union’s Internet service providers (ISPs) to attempt to retrieve deleted e-mails as counsel represented to the court

that he would.

- Shortly after the company’s counsel indicated it might seek permission to have a forensic computer examine the union’s computers in an effort to retrieve deleted e-mails, the union replaced those computers, without notice.

Although none of these discovery failures alone would not justify the imposition of the most severe sanction in the judicial arsenal, their combined effect impelled it, according to the court. The court intended the sanction to (1) remedy the effect of the discovery abuses, which consisted of prejudicing the company’s ability to plan and prepare its case, (2) punish the responsible parties, and (3) deter similar conduct by others.

The court was singularly unimpressed by the union’s evidently strenuous attempts to justify its conduct by accusing the company of comparable behavior. Judge Preska writes, “To the extent that there were failings by the [company] or its counsel, they were well within the normal hurly-burly of the discovery process and, in any event, were promptly addressed. The conduct of the union and its counsel, on the other hand, transcended the hurly-burly of the discovery process into gross negligence, recklessness, willfulness and lying.”

Reliance on Federal Rules, *Residential Funding Corp.*

Judge Preska finds support for her ruling in Fed. R. Civ. P. 26. She notes it provides a deterrent to discovery misconduct by “imposing a certification requirement that obliges each attorney to stop and think about the legitimacy of a discovery request, a response thereto, or an objection.”

In addition the court also referred to the Second Circuit’s recent decision in *Residential Funding Corp. v. DeGeorge*

Fin. Corp., 306 F.3d 99 (2d Cir. 2002), for guidance in exercising the court's broad discretion to issue discovery sanctions pursuant to Rule 37. The court looked to *Residential Funding* and other similar cases as confirmation of the court's discretion to invoke severe sanctions even when merely negligent conduct leads to the destruction of documents resulting in an imbalance in the availability of necessary evidence.

Onus Was on Counsel

If there is one lesson to be learned from this case, it is that in discovery, the buck stops with counsel, and that is true whether the information sought is in hard or electronic copy. The portion of the opinion subtitled "Electronic Documents" brings this point home. For example, when one lawyer charged with document production represented to the court that he never specifically instructed the union not to delete computer files and that no retention procedure had been instituted, the court thereafter directed him, rather than the union's non-lawyer document custodian, to insure that all documents relevant to the company's document requests were preserved, including, specifically, "all work done on computers and all information sent out or received through computers." The court also expressly admonished the lawyer for never having inquired of the non-lawyer custodian how he was discharging his discovery responsibilities.

Perhaps the lawyer's lapses, however, were as much a function of technological ignorance as they were of design. For example, he initially believed, erroneously, that e-mails are always automatically stored on a user's server. Upon learning that the union servers retained e-mail for only 30 days, his solution was to direct all union staff to make hard copies of all responsive incoming and outgoing e-mails and place them in a box for production. For those lost prior to the institution of this process, he directed union staff to contact the recipients of their e-mail and obtain copies which they

might have retained. Moreover, at least one union employee had a computer that was not connected to a printer. Her efforts to retrieve e-mails consisted of cutting and pasting them into a Word document, saving the new document to a disk, and inserting the disk in another computer to be printed out.

When a computer search was belatedly conducted by a union employee, it was limited to two of the three working computers and consisted of looking in the computer's "My Documents" folder or its hard drive (the searcher did not remember which) looking for document titles "that would say 'Met Opera.'" He didn't use the "Find" tool and only looked at document names. He was unable to recall whether the search produced any documents. And although his personal office practice was to save all documents to a single diskette from which he deletes as it fills up (without making a record of what he deleted), he never produced any diskettes in the course of discovery.

The court's delineation of the union's discovery failures continues in the same detailed vein for some 50 pages. This record supports the conclusion that union's counsel violated its affirmative duty under Fed. R. Civ. P. 26(g) to make a reasonable inquiry into the basis of their discovery responses and to "stop and think about the legitimacy of [those] responses." In addition, the record reflects ample evidence of willfulness and bad faith. And the union, along with counsel, was tarred with the brush of noncompliance for failing to set up an adequate system for document production, and dismantling computers that were the potential subject of a computer forensic sweep. The court concludes that the company was prejudiced by the union's behavior, which could only have been embarked upon for an improper purpose.

In addition to the entry of judgment as to liability against defendants, the court imposed additional sanctions in the form of attorneys' fees necessitated by the discovery abuse against the defendants and their counsel both.

The Court's Prescription

The *Metropolitan Opera* decision does set out what the union should have done, at a minimum, to properly discharge its discovery obligations. Essentially, the court avers that the union had a duty to "establish a coherent and effective system to faithfully and effectively respond to discovery requests." According to the court's discussion, elements of that plan should have included:

- a reasonable procedure to dis-

tribute discovery requests to all employees and agents of the defendant potentially possessing responsive information, and to account for the collection and subsequent production of the information to plaintiffs;

- a method for explaining to their client what types of information would be relevant and responsive to discovery requests;

- an inquiry into the client's document retention or filing systems, and implementation of a systematic

procedure for document production or for retention of documents, including electronic documents; and

- proper supervision of all elements of discovery that were to be carried out by non-legal personnel.

Virginia Llewellyn, who wrote this sidebar and contributed to the case study it accompanies, examines these principles in greater detail in the "Talking Tech" column that begins on page 1.

■ MARCH

6-7

16th Annual Advanced Computer and Internet Law Institute. Washington, D.C. Presented by Georgetown University Law Center.

Contact: tel: (202) 662-9890; fax: (202) 662-9890; e-mail: cle@law.georgetown.edu; Web: <http://www.georgetowncle.org>

13

23rd Annual Institute on Computer Law 2003. San Francisco, Cal. Presented by the Practising Law Institute.

Contact: tel: (800) 260-4PLI or (212) 824-5710; e-mail: info@pli.edu; Web: <http://www.pli.edu>

25

Document Management and Automation for the Federal Enterprise: Improving Performance Through Innovative Business Practices (Session 1). Arlington, Va. Presented by Market*Access International, as part of its Market*Access Government Best Practices Series™.

Contact: tel: 703-807-2748

27-28

Evidence Issues in Employment Cases: A View from the Bench. The Yale Club, New York City. Presented by Pike & Fischer, Inc. for the Bureau of National Affairs, Inc.

Contact: tel: (301) 562-1530; e-mail: pf@pf.com; Web: <http://www.pf.com>

■ APRIL

1

E-Discovery: Tips, Tactics & Technology. Washington, D.C. Presented by Kroll Ontrack.

Contact: tel: 800-347-6105

1-4

13th Annual Conference on Computers, Freedom & Privacy. New York City. Presented by the American Civil Liberties Union.

Contact: e-mail: feedback@cfp2003.org; Web: <http://www.cfp2003.org>

17

Document Management and Automation for the Federal Enterprise: Improving Performance Through Innovative Busi-

ness Practices (Session 2). Arlington, Va. Presented by Market*Access International, as part of its Market*Access Government Best Practices Series™.

Contact: tel: 703-807-2748

24-25

Complex Litigation V. Sedona, Ariz. Presented by the Sedona Conference. Focus on discovery of electronic information documents; critique of principles to govern e-discovery proposed by Sedona Conference Working Group.

Contact: tel: (866) 860-6600; Web: <http://www.thesodonaconference.org>

■ MAY

1-2

2003 BNA Litigation Forum: Electronic Discovery and Records Management. The Princeton Club, New York City. Presented by Pike & Fischer, Inc. for the Bureau of National Affairs, Inc.

Contact: tel: (301) 562-1530; e-mail: pf@pf.com; Web: <http://www.pf.com>

6-8

InfoToday 2003: The Global Conference & Exhibition on Electronic Information and Knowledge Management. New York Hilton and Towers, New York City. Presented by Information Today, Inc.

Contact: tel: (609)-654-6266; fax: (609) 654.4309; Web: <http://www.infotoday.com/it2003>

8-9

The Internet: Digital Privacy & Security. Sedona, Ariz. Presented by the Sedona Conference.

Contact: tel: 1-866-860-6600; Web: <http://www.thesodonaconference.org>

SEPTEMBER

17

Document Management and Automation for the Federal Enterprise: Improving Performance Through Innovative Business Practices (Session 3). Arlington, Va. Presented by Market*Access International, as part of its Market*Access Government Best Practices Series(tm).

Contact: tel: 703-807-2748

The publishers of *Electronic Commerce & Law Report* and *Digital Discovery & e-Evidence* proudly present:

Third Annual BNA Litigation Forum Electronic Discovery and Document Retention 2003

MAY 1-2, 2003
The Princeton Club
15 West 43rd Street
New York City
212-596-1200
www.princetonclub.com

Our distinguished faculty of judges, veteran litigators, and technology experts will share with you cutting-edge trends and best practices in electronic discovery!

FEATURED SPEAKER
Hon. James C. Francis IV
Magistrate Judge,
U.S. District Court,
Southern District of New
York

FEATURED SPEAKER
Eric Dinallo
Bureau Chief,
Investor Protection and
Securities Bureau,
New York State Office of
the Attorney General

Attend This Forum to:

- **Implement** the courtroom strategies and records management practices that can slash your production costs.
- **Learn** new sources of electronic evidence to include in discovery motions—including some the other side often overlooks!
- **Understand** how Enron and other corporate scandals have highlighted the focus on electronic evidence in litigation.
- **Discover** the crucial steps you must take to keep privileged information out of the files you hand over to your opponent.
- **Find** the precise type of technical assistance you need to enhance your digital discovery and electronic records management.

And Much More!

Hosted by:



The Bureau of National Affairs, Inc.



Pike & Fischer, Inc.

Sponsors:

- Applied Discovery • Evidence Exchange
- Fast Track • PriceWaterhouseCoopers

Register Online: <http://conferences.pf.com/ediscovery> • Phone: 631-368-2082 • Fax: 631-368-2947