Published by Pike & Fischer, A BNA Company

Digital Discovery & e-Evidence

BEST PRACTICES & EVOLVING LAW

http://ddee.pf.com

Vol. 6, No. 3 | March 2006

FRE Committee To Consider Remedy for Privilege Problem Discussed in *Hopson*

The Advisory Committee on Evidence Rules will meet on April 24, at Fordham University Law School, to consider a new evidence rule. Proposed Federal Rule of Evidence 502 is intended to address various privilege issues that the revisions to the Federal Rules of Civil Procedure do not completely eliminate. They were most recently examined in *Louis H. Hopson v. The Mayor and City Council of Baltimore*, (232 F.R.D. 228, D. Md., November 22, 2005; *DDEE*, December 2005, page 1).

Magistrate Judge Paul W. Grimm, author of the *Hopson* opinion, has referred to the Fordham meeting as "a mini-conference convened on *Hopson*." In that opinion, Judge Grimm explained that protecting privilege has become difficult and expensive because the data to be reviewed is voluminous and unorganized.

The solution of various jurisdictions – and the one adopted in the proposed revisions to Federal Rules of Civil Procedure 16, 26, 33, 34, and 37 – is to encourage parties to enter into agreements to disclose privileged materials (provided the disclosure is not taken to entail waiver as to all privileged matters), and have the court include those agreements in a case-management or other order.

It has been noted that this approach does not address the substantive questions of whether privilege or work product protection has been waived or forfeited, but merely allows the responding party to assert a claim of privilege or of work-product protection after production, with the answer dependent on the law of privilege that the particular jurisdiction applies. Within the Fourth Circuit, no case provides definitive guidance on this issue.

Judges' Viewpoints

Discussing *Hopson* at an ALI-ABA/Georgetown University Continuing Legal Education Program on February 10, Magistrate Judges John M. Facciola (D. D.C.) and Ronald J. Hedges (D. N.J.) agreed with Judge Grimm that there are three specific problems associated with the use of non-waiver agreements. First, they may not be enforceable as to the parties that enter into them. Second, their effectiveness against third parties is even more doubtful. Finally, case law from the Fourth Circuit suggests that the court may be inclined to adopt a strict liability approach to inadvertent waiver, meaning that waiver would be broad subject matter waiver, rather than waiver limited to the contents of the disclosed documents.

Court Orders Are Key

Hopson's proposed solutions to these problems entail the courts issuing scheduling orders under Fed. R. Civ. P. 16, protective orders under Fed. R. Civ. P. 26(c), or discovery management orders under Fed. R. Civ. P. 26(b)(2), that incorporate procedures under which electronic records will be produced without waiving privilege or work-product protection that the courts have determined to be reasonable given the nature of the case, and that have been agreed to by the parties. This approach will succeed in avoiding waiver only if it is compelled by the court, rather than accomplished solely by the voluntary act of the producing party, and if it reflects the taking of reasonable measures to protect against privilege and work-product protection.

continued on page 2

Inside

Proposed Rule 502 echoes the *Hopson* holding, providing that "a voluntary disclosure does not operate as a waiver if …the disclosure is inadvertent and is made during discovery in federal or state litigation or administrative proceedings — and if the holder of the privilege or work product protection took reasonable precautions to prevent disclosure and took reasonably prompt measures, once the holder knew or should have known of the disclosure, to rectify the error, including (if applicable) following the procedures in Fed. R. Civ. P. 26(b)(5)(B)." It further provides that "a court order concerning the preservation or waiver of attorney-client privilege or work product protection governs its continuing effect on all persons or entities, whether or not they were parties to the matter before the court" and that "an agreement on the effect of disclosure is binding to the parties to the agreement, but not on other parties unless the agreement is incorporated into a court order."

Lingering Concerns

While acknowledging that *Hopson* and the proposed new evidence rule represent a laudable effort to rectify a serious problem, Judge Hedges expressed some reservations about its ultimate success. Specifically, he questioned the authority of a court to bind parties outside of its jurisdiction, and predicted that due process objections would be lodged to such an approach. The full text of Proposed Rule 502 is available at http//:ddee/pf.com.

– C. Eoannou

Editor's Note

The *Hopson* opinion was the topic of a 90-minute audio conference presented by Pike & Fischer on January 11. The author of *Hopson*, **The Honorable Paul W. Grimm**, was joined by **Magistrate Judges John M. Facciola** (D. D.C.) and **Ronald J. Hedges** (D. N.J.) in sharing judicial perspectives on the important issue of how best to preserve privilege when producing electronically stored information. Well-known D.C. attorney **Jonathan M. Redgrave**, of Redgrave, Daley, Ragan, & Wagner LLP. moderated the program.

To order a CD recording of the event, which was entitled **Privilege in Peril: Judges' Perspectives on Privilege Problems Associated With Electronically Stored Information**, go to http://www.pf.com/eventDetail.asp?id=47&type=2.

Regualtory Developments

NARA Publishes Final Rule on Short Term E-mail

According to a notice in the February 21 Federal Register (71 FR 8806), the National Archives and Records Administration's (NARA) Final Rule pertaining to the disposition of electronic mail records with short retention periods will become effective on March 23, 2006. The Rule is intended to provide for the appropriate management of very short-term temporary e-mail by allowing agencies to manage these records within the e-mail system.

The Rule sets out the following standards:

Agencies may elect to manage electronic mail records with very short-term NARA-approved retention periods (transitory records with a very short-term retention period of 180 days or less … or by a NARA-approved agency records schedule) on the electronic mail system itself, without the need to

Digital Discovery
& e-Evidence
http://ddee.pf.com

Managing Editor, Carol L. Eoannou ..... 800-255-8131 ext. 269 (ceoannou@pf.com)
Senior Director, Legal and Regulatory Products, Robert Emeritz ..... 800-255-8131 ext. 258 (remeritz@pf.com)
President, Meg Hargreaves ..... 800-255-8131 ext. 229 (mhargreaves@pf.com)
Pike & Fischer Customer Care ..... 800-255-8131 ext. 248 or 301-562-1530 ext. 248
Pike & Fischer Customer Care Online ..... Email: customercare@pf.com Web: www.pf.com

Published monthly. ISSN: 1537-5099 Subscription rate: $559

POSTMASTER: Send address changes to: *Digital Discovery & e-Evidence*, Pike & Fischer, 1010 Wayne Avenue, Suite 1400, Silver Spring, Maryland, 20910.

PUBLISHER: Pike & Fischer, a division of IOMA, Inc., 1010 Wayne Avenue, Suite 1400, Silver Spring, Maryland 20910

copy the record to a paper or electronic recordkeeping system, provided that:

(i) Users do not delete the messages before the expiration of the NARA approved retention period, and

(ii) The system's automatic deletion rules ensure preservation of the records until the expiration of the NARA-approved retention period.

For all other electronic mail records:

(i) Agencies must not use an electronic mail system to store the recordkeeping copy of electronic mail messages identified as Federal records unless that system meets certain criteria;

(ii) If the electronic mail system is not designed to be a recordkeeping system, agencies must instruct staff on how to copy Federal records from the electronic mail system to a recordkeeping system.

The full text of the Rule is published at http://ddee.pf.com under Proposed & Enacted Rules, United States Administrative Agencies. *— C. Eoannou*

Current Literature

Call for Comments on 2006 *Sedona Principles*

In light of the proposed revisions to the Federal Rules of Civil Procedure, which most observers predict will become effective on December 1, 2006, and the continued development of case law, The Sedona Conference Working Group Addressing Electronic Document Retention and Production announces that it is undertaking a project to review and update its groundbreaking work, *The Sedona Principles*® (available for free download for personal use at www.thesedonaconference.org).

Richard Braman, Executive Director of The Sedona Conference, emphasized the process that gives rise to Sedona publications. He explained, "The Working Groups of The Sedona Conference were conceived as ideal settings to create living, breathing and iterative guidance in important areas for the bench and bar. Consistent with that origin, the decision of this Working Group to undertake this timely review will ensure that *The Sedona Principles* has continued vitality as an important resource to harmonize the law in a way that rules changes, cases and other commentary simply cannot do."

Jonathan Redgrave, chair of the Working Group and Editor-in-Chief of *The Sedona Principles*, added, "Consistent with our approach to solicit the comments of the bench and bar on other draft work product of Sedona Working Groups, we welcome the suggestions, edits, and contributions of the public on the existing version of *The Sedona Principles*. The comments from observers from all perspectives are invaluable to help the editorial board address the anticipated changes in the rules of civil procedure and other new developments in the law and technology involved in the production of electronic data and documents in litigation to make *The Sedona Principles* an even more valuable resource."

The Working Group expects that a revised version of *The Sedona Principles* will be published in December of 2006, and will be accompanied by a 2006 annotated version of the document. The latter builds upon the current annotated version of *The Sedona Principles* that distills and organized the most important cases and developments in this area. *The 2005 Annotated Version of the Sedona Principles* is currently available from Pike & Fisher (http://www.pf.com/sedonaPrincPD.asp).

Comments should be faxed to The Sedona Conference at 928-284-4240, using the form on the "Publications" page of its website, www.thesedonaconference.org. Comments should be received no later than June 1, 2006.

— Special from The Sedona Conference

New Sources of Evidence

Company Using Implantable Employee ID Tags

Two employees of CityWatcher.com, a video surveillance company based in Cincinnati, recently had glass-encapsulated radio frequency identification (RFID) devices placed under their skin. Sean Darks, CityWatcher.com's chief executive officer, explained that the "VeriChip" microchips implanted into the employees' arms are imprinted with 16-digit numbers that are read when the employees approach special scanners that control access to secure rooms. The employees volunteered to accept the devices, he said. The microchips can contain individuals' complete medical records.

VeriChip, based in Delray Beach, Fla., developed the microchips for implantation into hospital patients suffering from illnesses that might cause them to lose consciousness or wander away. At least 65 hospitals across the United States have purchased the technology, according to VeriChip spokesman John Procter. Procter said that the chips, which are made of medical grade glass about the size of a grain of rice, can easily and safely be injected with a needle into the receiver's arm in a doctor's office. When the wearer wants the chip removed, he or she can undergo a "simple outpatient procedure," which Procter likened to "removing a large splinter." *— Special from BNA*

COURTS & PROCEDURES

NCSC Publishes Proposed Guidelines for State Trial Courts Regarding Discovery of Electronically Stored Information

By Courtney Ingraffia Barton, Esq.

In September of 2005, a Working Group of the Conference of Chief Justices of the state courts (CCJ), working through the National Center for State Courts (NCSC) published a series of Proposed Guidelines for State Trial Courts Regarding Discovery of Electronically Stored Information (guidelines). These guidelines were open for comment until December 15, 2005.

According to Richard van Duizend from the NCSC, 11 organizations and individuals commented on the guidelines, with varying degrees of specificity. Comments were submitted by vendors, individuals, and groups from both the plaintiff and defense bar. The comments are now being compiled and will be submitted to the Working Group in a series of conference calls over the next few weeks. The public will not have an opportunity to comment further or to see the comments unless the Working Group determines that substantial revisions are necessary.

If revisions are not necessary, the guidelines will be submitted to the entire CCJ for approval at the CCJ's July meeting. If revisions are needed, there may be an opportunity to comment further at that time.

The guidelines will not be binding on the state courts, although each court may use them to address electronic discovery as they see fit. The purpose of the guidelines is to help reduce the uncertainty of how to address electronic information in the state courts. Although the state courts have not seen a large number of electronic cases thus far, the CCJ Working Group recognized that the reliance on electronic information almost certainly assures that the courts will need to address these issues in the near future.

Developing the Guidelines

Drawing heavily from an electronic discovery presentation to the National Workshop of United States Magistrate Judges on June 12, 2002 given by Ken Withers, who at the time was the Senior Judicial Education Attorney at the Federal Judicial Center, the CCJ Working Group noted in its introduction to the guidelines that there are three essential differences between conventional documents and electronic documents:

- differences in degree;
- differences in kind; and
- differences in costs.

Differences in degree relate to the sheer volume, number of locations and the data volatility of electronic documents versus paper documents. Differences in kind relate to the fact that often no permanent document is created with digital transactions, and that electronic documents contain certain types of "non-traditional" information such as metadata, system data, and deleted data. Differences in costs can include the higher costs of restoring backup tapes and hiring experts, and the lower costs associated with greater search functionality.

Recognizing these differences between electronic discovery versus paper discovery, the CCJ Working Group looked to the following sources in order to craft the guidelines, which address 10 areas of electronic discovery:

- the proposed Federal Rules of Civil Procedure on Electronic Discovery,
- the Electronic Discovery Guidelines issued by the U.S. District Court for the District of Kansas,
- the American Bar Association *Standards Relating to Civil Discovery* (August 2004),
- *Zubulake v. UBS Warburg LLC,* 2003 U.S. Dist. LEXIS 12643 (S.D. N.Y. July 24, 2003) (*"Zubulake III"),*
- a proposed rule for California prepared by Richard Best, which was never adopted, and
- the Default Standard for Discovery of Electronic Documents promulgated by the U.S. District Court for the District of Delaware.

The Guidelines

Although similar to the proposed amendments to the Federal Rules of Civil Procedure which are currently pending before the Supreme Court, the guidelines do contain some substantial differences.

The guidelines are summarized and discussed below:

1. Definition of Electronic Information.

The guidelines pose a very broad definition of electronic information. Unlike the proposed federal rules, the guidelines define "accessible information" based on *Zubulake III,* as "electronically stored information that is easily retrievable in the ordinary course of business."

2. Duty of Counsel to be Informed about Client's Electronically Stored Information.

This guideline is also different than the proposed federal rules, which do not explicitly state an affirmative duty

to be informed. However, the Federal Rules do implicitly require such knowledge in preparation for the Rule 26 meet and confer.

3. Pre-Conference Order.

This guideline would apply in cases where issues regarding electronic discovery are raised and the parties have not reached an agreement on how the issues should be handled. The guideline suggests that the judge order the parties to meet and confer and discuss the following: persons most knowledgeable about electronic systems, records custodians, lists of electronic systems and the relevant information they contain, accessibility, location of electronically stored information, and the form of production preferred. In addition, the guideline encourages the naming of an electronic discovery liaison, who would be the person coordinating the e-discovery efforts. The comments to this guideline suggest some general qualifications for this person, such as sufficient familiarity with the party's electronic systems and capabilities to explain these systems, and the ability to be prepared to participate in e-discovery disputes. The guidelines also suggest that the parties submit an agreement about information to be exchanged, and/or an agreed-upon schedule of compliance with deadlines.

4. Initial Discovery Hearing or Conference.

This guideline would encourage a hearing to discuss issues similar to those in the pre-conference order, such as form of production, preservation procedures, and allocation of costs.

5. The Scope of Electronic Discovery.

This guideline is similar to proposed Federal Rule 26(b)(2)(B), which addresses the production of accessible information, although it does not use those terms. The guideline provides the factors a judge should take into account when determining whether information must be produced.

The first inquiry is relevance (which is not defined) and then a balancing test weighing the burdens and expense of production. The factors are derived from the American Bar Association *Standards Relating to Civil Discovery*, Standard 29 (August 2004).

6. Form of Production.

This guideline states that in the absence of an agreement among the parties, a judge should ordinarily require electronically stored information to be produced in no more than one format and should select the form of production that, at a minimum, preserves the substantive information of the relevant data. This is similar to the proposed Federal Rules in that only one format is required. However, it is different in that the Federal Rules do not contain requirements about preserving substantive information of the documents. The Federal Rules base form of production on how information is maintained ("ordinary course of business") and used ("reasonably usable"). The comments to this guideline also address native file production, noting that producing in native format is undesirable because it would be "difficult to search without the word-processing, e-mail or database software need[ed] to organize and present the information in a coherent form." Moreover, with respect to metadata, the guidelines do not establish "a rebuttable presumption against the production of metadata, rather it sets the rendition of the substantive information (such as a .tif or .pdf file) as a floor, leaving open specification of a format revealing non screen information." Thus, the production of metadata may be required, but no form of production for metadata is specified in the guideline.

7. Reallocation of Discovery Costs.

This guideline follows the cost shifting principles set forth in *Zubulake III,* including the factors judges should follow when determining whether cost-shifting is appropriate.

8. Inadvertent Disclosure of Privileged Information.

Similar to the proposed Federal Rules, this guideline addresses the fact that due to the sheer volume of electronic information being produced by parties, information considered privileged may be inadvertently produced to an opponent. This guideline is different than the proposed Federal Rule in that it sets forth four factors for a judge to consider in determining whether a party has waived the attorney-client privilege in the absence of an agreement between the parties. By contrast, the proposed Federal Rule does not address the substantive law of privilege but rather puts forth a procedure for the return of inadvertently produced information so that a judge can then apply the substantive law of the state.

9. Preservation Orders.

This guideline sets forth the factors judges should consider when evaluating a motion for preservation of electronic evidence. The guideline states that preservation orders should be narrowly tailored and should consider factors drawn from *Capricom Power Co., Inc. v. Siemens Westinghouse Power Corp.* 220 F.R.D. 429; 2004 U.S. Dist. LEXIS 10016 (W.D. Pa. April 21, 2004), including: the threat to the existence and integrity of the information in question; whether any irreparable harm is likely to result to the requesting party absent a preservation order; the capability of the responding party to maintain the information sought in its original form; and the physical, technological, and financial burdens created by ordering preservation of the information.

10. Sanctions.

Considerations for sanctions under this guideline, based on *Residential Funding Corp. v. DeGeorge Fin. Corp.,* 306 F.3d 99, 2002 U.S. App. LEXIS 20422, 53 Fed. R. Serv. 3d (Callaghan) 1105 (2d Cir. Conn. Sept. 26, 2002), give more guidance than the proposed Rule 37(f). The guideline sets forth three factors for judges when considering sanctions because of the destruction of electronically stored information.

Although the comments have not been made public, because of the differences between the guidelines and the proposed Federal Rules, some parties may have had difficulty with this inconsistency. Others, however, may have appreciated that the guidelines provide more direction. Nevertheless, it will be interesting to see what next steps the CCJ will take.

For more information and updates, interested parties can go to the NCSC website: www.ncsconline.org. The Guidelines, in their entirety, are posted at http://ddee.pf.com under "Proposed and Enacted Rules, Other Advisory Bodies."

Courtney Ingraffia Barton *is Vice President of Industry Relations of LexisNexis® Applied Discovery®. In this role, she works with law firms, government organizations and industry notables to educate the legal community on the continually evolving case law and technology of electronic discovery.*

Prior to joining Applied Discovery, Ms. Barton was a trial attorney with the United States Department of Justice where she oversaw a docket of multimillion dollar environmental enforcement cases. She also worked as a senior associate with Arnold & Porter in Washington, D.C.

PROFESSIONAL RESPONSIBLITY & ETHICS

Client E-files May Be Stored on Remote Servers under Third-Party Control

A law firm may store its electronic client records on a remote server under the control of a third party so long as the firm selects with care a company that promises to keep the information confidential, according to a recent opinion from the Nevada Bar Associations's ethics committee (Nevada State Bar Standing Comm. on Ethics and Professional Responsibility, Formal Op. 33, February 9, 2006).

When these precautions are taken, an off-site electronic storage arrangement may be used without client consent despite the risk that an employee of the company or someone else might gain unauthorized access to the files, the panel concluded.

Online Records Storage

A lawyer asked the ethics committee about the propriety of using an outside agency to store electronically formatted client information. The lawyer's electronic client files, containing confidential information and communications, would be kept beyond the lawyer's direct control on a server maintained by a third party.

For purposes of its analysis, the committee assumed that the lawyer will be able to insist—as part of his service contract with the third party—that all reasonably necessary means be used to preserve the confidentiality of the information and to prevent unauthorized access and disclosure. The panel also assumed, however, that employees of the agency will have access, both authorized and unauthorized, to the confidential data.

After reviewing the ABA's evolving views on lawyers' use of electronic communications, the committee concluded that an attorney does not violate the duty of confidentiality by storing electronic client records on a remote computer not under the lawyer's dominion, so long as the attorney takes precautions similar to those used when arranging for confidential paper files to be warehoused.

ABA Opinions

Lawyers must act competently to safeguard confidential information in any context, the committee noted. It added that although lawyers are not strictly liable for a breach of client confidentiality, they must take reasonable precautions to prevent both inadvertent and unauthorized disclosure.

Finding a scarcity of up-to-date ethics opinions from other states on applying the duty of confidentiality to electronic data, the panel traced the history of the ABA's advice on the issue. It found that although a 1986 ABA report counseled lawyers to be wary of using an electronic communication system without first obtaining informed client consent or assuring themselves of the system's security, the ABA's ethics committee subsequently supported a different approach.

First, in ABA Formal Ethics Op. 95-398 (1995), the committee advised that the duty of confidentiality is not breached by giving a computer maintenance company access to a lawyer's confidential records, so long as the lawyer is reasonable and competent in creating and maintaining the arrangement with the outside contractor.

More recently, ABA Formal Ethics Op. 99-413 advised that a lawyer's use of unencrypted e-mail does not violate the duty of confidentiality, although particularly sensitive information may require extraordinary security measures.

The Nevada opinion notes that nearly all state bar associations addressing the issue have adopted the ABA's approach to e-mail communications, although some commentators have suggested that advances in technology will require, or may already require, that lawyers take additional steps to safeguard electronic communications.

New Comments

Continuing its survey of the ABA's views, the commit-

tee noted that as part of the ABA Ethics 2000 Commission's amendments to the Model Rules of Professional Conduct, two new comments were added on the subject of a lawyer's duty to guard against unauthorized and inadvertent disclosures. Comments [16] and [17] to Model Rule 1.6 indicate that traditional rules of confidentiality generally apply to new forms of communication, the committee said.

From the ABA opinions and the new comments to Model Rule 1.6, the Committee gleaned the following policy: Electronic client information is treated according to existing confidentiality rules, and an attorney is not responsible for a breach of client confidentiality, or for storing client information in a way that makes possible a breach, so long as the attorney:

- exercises reasonable care in selecting a third-party contractor that can be trusted to keep the data confidential;
- reasonably expects that the information will be kept confidential; and
- instructs and requires the contractor to keep the information confidential and inaccessible.

If these precautions are taken, a lawyer does not violate the rule on client confidentiality simply by contracting with a third party to store information, even if an unauthorized or inadvertent disclosure should occur, the opinion makes clear.

The committee said that if these precautions are taken, client consent to the storage arrangement is not mandatory, even though ethics rules "generally would prefer that the lawyer obtain the client's informed consent before transmitting confidential information to third parties in any case."

New Hampshire

E-records Must Be Turned Over to Successor Counsel

E-mails and other electronic materials relating to a former client's representation must be retrieved from a law firm's computer network and given to a departing lawyer who has requested the file in order to represent the client at a different firm, the New Hampshire Bar ethics committee advised in a January opinion (New Hampshire Bar Ass'n Ethics Comm., Op. 2005-06/3, January 2006).

The committee decided that a client's file necessarily includes electronic as well as paper forms of materials pertaining to the client's representation. The possible cost of locating and compiling electronic records has no bearing on a lawyer's duty to turn over a client's file upon request, the opinion makes clear.

Ex-Client's Right to File

A law firm asked the committee about its obligation to relinquish electronic communications and documents concerning former clients to an attorney who is leaving the law firm and will continue to represent the clients at another firm.

The law firm plans to turn over all of the paper files pertaining to the former clients, including paper copies of e-mails that had been placed in the files. The departing lawyer has also requested, however, that the firm provide copies of all e-mail communications and electronic documents pertaining to the clients on the firm's computer network.

The firm asked whether it could avoid organizing thousands of electronic items in the lawyer's inbox and instead provide only the hard copy items in the client's file. The committee's answer was no.

The New Hampshire Supreme Court has held that the contents of a client's file belongs to the client and that, upon request, a lawyer must provide the client with the file, the committee noted.

Moreover, the committee pointed out that in the words of New Hampshire Rule of Professional Conduct 1.16(d), a lawyer must, when a representation ends, take steps to the extent reasonably practicable to protect a client's interests, such as surrendering papers and property to which the client is entitled.

E-materials Too

Assuming that the departing lawyer has requested a file on the client's behalf, the committee continued, the law firm must include in what it turns over electronic communications and documents within the firm's computer network. "[T]he contents of a client's file would necessarily include both paper and electronic forms of communications, documents and other records pertaining to the client," the committee explained.

In reaching this conclusion, the panel relied on ABA Model Rule 1.0, which defines writing as a tangible or electronic record of a communication or representation, including e-mail.

The committee said that this model rule, although not adopted in New Hampshire, reflects that with increased reliance on electronic communications and records in the practice of law, it is reasonable to assume that a client's file can include electronic communications, such as emails, as well as electronic versions of documents filed on behalf of a client.

Thus, the committee concluded, the mere existence of a paper file does not necessarily allow a firm to exclude electronic materials from the client's file.

Burden Is Irrelevant

The committee also advised that if a client requests a copy of her file, the firm has an obligation to provide all files pertinent to representation of that client, regardless of the burden that it might impose upon the firm to do so.

In any event, the committee said, the firm can manage the burden by using computer search functions or other

means routinely used for discovery. As in the discovery process, the panel added, it is incumbent upon law firms to manage their files in such a way that allows for release of a file to a client without releasing other information that might harm a third party.

Firms should also consider whether they have adequately notified former clients of any file destruction policies with regard to electronic and paper records, the committee advised.

The full text of the Ethics Opinion is posted at http://ddee.pf.com. – *Special from BNA*

CASES

Southern District of New York Offers Guidance on Rule 37(a) Preservation Orders

A securities analyst's claims of defamation, tortious interference with prospective economic advantage, prima facie tort, and civil conspiracies have given rise to a magistrate judge's opinion that reviews the current state of preservation orders. *Treppel v. Biovail Corporation*, 2006 WL 278170, S. D. N.Y., February 6, 2006.

The Dispute

The e-discovery phase of *Treppel* began approximately four months after service of an amended complaint, when plaintiff's counsel sent a letter to defendants' counsel demanding that all information relevant to the claims and defenses in the action, including electronic evidence, be preserved. Counsel for defendants (the corporation and some named individuals), returned a comparable demand. Approximately six weeks later, plaintiff's counsel circulated a proposed Stipulation and Order Regarding Electronic Data Preservation and Discovery Protocols, which reflected a detailed and comprehensive approach to e-discovery, proposing, *inter alia*, an information swap regarding each party's document retention policies, depositions of witnesses familiar with the parties' respective information systems, the preservation of relevant data in a variety of specifically described media and storage devices, according to a highly detailed protocol, production in native format of all relevant information maintained in accessible form, and the identification of information contained on inaccessible media. Defendants' counsel made no reply.

Undeterred, plaintiff then extended to defendants' counsel an invitation to confer about the proposed order, which the defendants declined, claiming they were "aware of their preservation obligations under the Federal Rules of Civil Procedure, and would abide by them." Plaintiff's First Request for Production of Documents met with a slightly more favorable reception, although defendants filed some relevancy objections.

With respect to some of the documents that defendants *agreed* to produce, a separate dispute arose when their counsel sought an agreement about which electronic files were to be searched and what search terms were to be used. Plaintiff's counsel responded, "[I]t is defendants' obligation to simply search its records and respond to those demands. Plaintiff has no obligation to assist defendants in the process by providing search terms or any other guidance."

The plaintiff then filed a motion pursuant to Rule 37(a) of the Federal Rules of Civil Procedure, for an order compelling the defendants to: (a) preserve all potentially discoverable data, whether maintained in electronic or paper form; (b) answer a range of questions concerning their electronic data management practices by filling in a Document Retention Questionnaire; and (c) produce all accessible data and documents responsive to the plaintiff's First Request for Production of Documents, including documents responsive to three specific requests (i.e. "All documents concerning the decision by or on behalf of Biovail to subpoena or otherwise obtain Treppel's personal account statements and trading records in the Florida Lawsuit," "All documents concerning the termination of Biovail's investment banking relationship with Banc of America Securities (BAS)," and "All documents reviewed, referred to or relied upon by Biovail and [defendant] Melnyk in the preparation of their respective Answers to the Second Amended Complaint in this action.").

Approaches to Preservation Orders

Magistrate Judge James C. Francis IV begins his discussion of preservation orders by admonishing the defendants for previously refusing to enter into a stipulated preservation order on the grounds that the case was too narrow to warrant one. He writes, "Such reasoning is shortsighted. Even litigation that concerns relatively precise issues, statements and timeframes may nevertheless involve information, including electronic documents, that may be in danger of destruction in the absence of a preservation order. Further, a preservation order protects the producing party by defining clearly the extent of its obligations. In the absence of such an order, that party runs the risk of future sanctions if discoverable information is lost because it has miscalculated." (Internal quotations omitted.) He also points out, citing *Pueblo of Laguna v. United* States, 60 Fed. Cl. 133 (2004); *DDEE,* May 2004, p. 10, that while not automatic, such orders are "increasingly routine in cases involving electronic evidence, such as e-mails and other forms of electronic communications." The question of the

circumstances under which a preservation order should be issued is at the heart of his opinion.

Injunctive Relief Test

While some courts take the position that the standards for obtaining a preservation order are the same as those for obtaining injunctive relief (irreparable injury and either likelihood of success on the merits, or sufficiently serious questions going to the merits and the balance of hardships in the movant's favor), Magistrate Judge Francis finds this approach problematic. He observes that applying those requirements in the context of a request for a preservation order requires the court to "evaluate the merits of the litigation even before evidence has been gathered, let alone produced to the opposing party or submitted to the court."

He turns, instead, to a balancing test like that set forth in *Capricorn Power Co. v. Siemens Westinghouse Power Corp.*, 220 F.R.D. 429 (W.D. Pa. 2004), requiring the application of the following three factors:

1) the court's level of concern for the continuing existence and maintenance of the integrity of the evidence should a preservation order not issue;

2) any irreparable harm likely to result to the requesting party absent a preservation order; and

3) the capability of an individual, entity, or party to maintain the evidence sought to be preserved, not only as to the evidence's original form, condition, or contents, but also the physical, spatial, and financial burdens created by ordering evidence preservation.

Danger of Destruction

Determining the likelihood of whether evidence has been destroyed requires ascertaining when the duty to preserve attaches and what evidence must be preserved. The parties take predictable positions regarding the onset of the duty: the plaintiff attempts to tie it to February 2002, when the events that gave rise to Treppel's claims occurred; the defendants, on the other hand, claim the duty did not attach until the plaintiff's formal demand for preservation efforts was made, by letter dated December 3, 2003.

The court explains that both views are erroneous: "On the one hand, the mere existence of a dispute between Mr. Treppel and Biovail in early 2002 did not mean that the parties should reasonably have anticipated litigation at that time and taken steps to preserve evidence." The court points out, however, that Biovail made a public comment on May 1, 2003, describing the suit — which had been filed but not served — as being "without merit," and reported the fact of the pending litigation to the Securities and Exchange Commission some three weeks later.

This places Biovail's awareness of the suit in the May 2003 timeframe, although it didn't make any preservation efforts until December 12, 2003.

All that that establishes, according to the court, is that "Biovail was tardy in establishing a preservation program." According to the court, it cannot be inferred that the delay led to the loss of any evidence. And Biovail convincingly outlined the steps it took beginning on December 12, 2003, to minimize the threat of future litigation.

The court concludes, "While Biovail's failure to recognize promptly its preservation obligation is cause for concern, the plaintiff has demonstrated neither that evidence has been lost nor that the steps Biovail has now taken are inadequate to preserve existing documents."

(Among the steps that Biovail ultimately took were creating back-ups of its central servers and images of hard drives of the laptops of certain employees, which the court describes as freezing information "so that in the future it would be neither destroyed beyond recovery nor downgraded from an accessible format to an inaccessible one." In an interesting footnote, Magistrate Judge Francis takes issue with *Quinby v. Westlab AG,* 2005 WL 3453908 (S.D. N.Y., December 15, 2005), where the court declined to sanction a party for converting data to an inaccessible format, and held that there is no obligation to preserve electronic data in an accessible form, even when litigation is anticipated. Judge Francis argues that under *Residential Funding Corp. v. DeGeorge Financial Corp*., 306 F.3d 99 (2d Cir. 2002), conduct that hinders access to relevant information is sanctionable, even if it does not result in the loss or destruction or evidence. Judge Francis puts the "downgrading of data to a less accessible form which systematically hinders future discovery by making the recovery of the information more costly and burdensome" into the category of conduct prohibited by *Residential Funding*.)

Content of Destroyed Documents

The court points out that plaintiff's failing to demonstrate that any documents were destroyed establishes, by extension, that he has also failed to identify the content of such documents. While identification of specific documents isn't necessary, plaintiff failed in his obligation to demonstrate that certain types of relevant documents existed and were necessarily destroyed by the operation of Biovail's routine document retention program.

Burdens

The plaintiff's application for a preservation order ultimately fails because of his failure to articulate the extent of the burden that would be occasioned by the imposition of the order.

Plaintiff sought the preservation of "electronic data, including e-mail data, whether on back-up tapes, computer hard drives, servers, PDAs, Blackberries, or other physical media and network back-up tapes." His error was in failing to demonstrate that his request for preservation is not unduly burdensome.

The court acknowledges that the defendants were par-

tially responsible for the plaintiff's inability to make the burdensomeness argument successfully – they were not forthcoming with the basic information about the operation of their electronic document system that plaintiff sought. The court therefore orders that the plaintiff's Document Retention Questionnaire and supplementary inquiries contained in letters from the plaintiff be treated as interrogatories, despite the fact that plaintiff has already propounded the 25 interrogatories allotted by operation of Fed. R. Civ. Pro. 33.

Search Protocol

The court admonishes the plaintiff for refusing to stipulate to a search methodology, suggesting that plaintiff both misunderstood the scope of the defendants' obligation to respond and missed an opportunity to convince the defendants to broaden their search to uncover the greatest number of responsive documents and avoid subsequent disputes. The court also chastises the defendants for failing to produce any documents whatsoever, despite having suggested a protocol (searching key players' computers using specified search terms). Absent an agreement, the court says, defendants should have proceeded unilaterally, producing all responsive documents that the search they designed covered.

Finally, the plaintiffs requested that production be made in native form. Since defendants failed to provide a substantive basis for its objection to native production, that is the form the court will require.

The full text of the opinion is posted at http://ddee.pf.com. — *C. Eoannou*

Technology

'Appearance' at Hearing Via Speakerphone Inherently Invalid

Voicing concern over the encroachment of technology on criminal representation, the Seventh Circuit has held that a criminal defense attorney who, with the court's permission, "appeared" at a client's plea hearing by way of a speakerphone offered inherently substandard services, so that the client need not show prejudice in order to vacate his plea (*Van Patten v. Deppisch,* 434 F.3d 1038, (January 24, 2006).

Counsel's performance in such a situation is necessarily so "perfunctory" that prejudice should be presumed pursuant to *United States v. Cronic*, 466 U.S. 648 (1984), the court decided.

Disembodied Voice

Defense counsel James B. Connell arranged for a change of plea proceeding in which his client, Joseph Van Patten, who was charged with intentional homicide, would plead no contest to reckless homicide.

Because Connell had court appearances in other counties that day, the judge allowed him to provide assistance to his client by speakerphone broadcast in the courtroom. Van Patten was not asked whether he consented to this procedure. Later, Van Patten sought to withdraw his plea on the ground that his lawyer's failure to appear in person at the hearing violated Van Patten's right to counsel.

The state court analyzed the claim as a complaint of ineffective assistance under *Strickland v. Washington*, 466 U.S. 668 (1984), and rejected it. The district court on *habeas* review likewise found no basis for relief.

Strickland v. Cronic

Claims of ineffective assistance of counsel are generally evaluated under *Strickland*, which requires a defendant to show both that his attorney's performance fell below an objective standard of reasonableness and that he suffered prejudice as a result. *Cronic*, however, established that prejudice may be presumed when counsel "entirely fails to subject the prosecution's case to meaningful adversarial testing." The Supreme Court has made clear that a change of plea proceeding is a critical stage of a prosecution in which counsel's assistance is crucial.

The Seventh Circuit, in an opinion by Judge Terence T. Evans, decided that *Cronic* rather than *Strickland* governed this case. The court observed that although the trial judge took pains to ensure that permitting Connell to participate in the plea hearing by way of a telephone connection did not violate Van Patten's rights, "the arrangements made it impossible for Van Patten to have the 'assistance of counsel' in anything but the most perfunctory manner."

Van Patten "could not turn to his lawyer for private legal advice, to clear up misunderstandings, to seek reassurance, or to discuss any last-minute misgivings," the court pointed out.

Furthermore, the court said, the speakerphone alternative prevented the lawyer from being able to "detect and respond to cues from his client's demeanor that might have indicated he did not understand certain aspects of the proceeding, or that he was changing his mind." It added that any discussion between Connell and his client could have been overheard by anyone else in the courtroom.

In essence, the court explained, Van Patten's complaint was directed at a structural defect in the proceedings, not merely the effectiveness of his lawyer's performance. Quoting from *Satterwhite v. Texas*, 486 U.S. 249 (1988), it said: "When a defendant is denied assistance of counsel at a stage where he must assert or lose certain rights or defenses, the error 'pervades the entire proceeding.' " Allowing the hearing to go forward with counsel and client unable to see each other or communicate privately was just such a violation of the Sixth Amendment, Evans concluded.

Technology Isn't a Panacea

"Getting the attorney on the speakerphone may have been better than nothing," the court said, but an accused is entitled to more than "formal compliance" with the Sixth Amendment. "[W]e think it problematic to treat assistance of counsel as a formality to be overcome through creative use of technology so that everyone can keep their calendars in order," the court commented. The court added:

"Physical presence is necessary not only so that counsel can keep an eye on the client and the prosecutor, but so the court can keep an eye on counsel.... Over a phone line, it would be all too easy for a lawyer to miss something. For example, she might prejudice her client by failing to make some important point during the proceedings and later claim it was a tactical decision (in which case *Strickland* mandates a large benefit of the doubt), when in reality she wasn't paying attention. Or an attorney might realize he had neglected to inform the client of some crucial piece of information but be tempted to let it pass rather than broadcasting the issue to everyone in the room.... Even assuming that counsel could hear and understand every word (and how many people who have experienced speakerphones or conference calls would stake their liberty on that assumption?), the client or the judge might never know whether the defense attorney was hanging on every word, reading documents in another case, surfing the web, or falling asleep."

If defense counsel were allowed to phone in representation as occurred here, the court wondered, "what might we be asked to accept next? Offshore defense-counsel call centers? Letting the defendant confer with counsel via Blackberry?"

Having decided that the *Cronic* presumption of prejudice applied, the court went on to emphasize that structural errors of this sort that "contaminate[ ] the entire proceeding" are not subject to harmless-error analysis.

The state court unreasonably applied established federal law in analyzing the defendant's complaint under *Strickland*, the court concluded, and therefore Van Patten is entitled to *habeas* relief from his conviction.

Linda T. Coberly of Winston & Strawn, Chicago, argued for Van Patten. Christopher Wren of the U.S. Attorney's Office, Madison, Wis., argued on behalf of the state.

CFFA

Use of Memory Stick, Hotmail to Export Pricing Data Supports Claim

Damages arising from the unauthorized transfer of pricing data from a secure database to an outside computer using a USB memory stick and Hotmail e-mail account support a civil claim under the Computer Fraud and Abuse Act, according to a recent district court ruling. *HUB Group, Inc. v. Clancy*, 2006 WL 208684, ED Pa, January 25, 2006.

Jeffrey Clancy worked as a sales executive for the plaintiff's shipping and logistics company, which maintained a password-protected database with detailed pricing information. Clancy left to join a competing firm. Forensic analysis of his company computer indicated some unusual activity on his computer shortly after he resigned. Clancy had attached a device to the computer's USB port, which the company theorized was a memory stick. He also sent several e-mails with attachments to his wife's Hotmail e-mail account. The e-mails contained confidential pricing data, gleaned from the database, which Clancy admitted taking for use in his new job.

Judge Lawrence Stengel concluded that the employer's allegation of damage to the integrity of its database was sufficient to plead a cause of action for violation of the Computer Fraud and Abuse Act.

However, the court declined to issue a preliminary injunction because the pricing data was no longer valuable. Clancy said he never used the data, and it is now too stale to be of use to anyone. "[T]he pricing data taken by Clancy is already obsolete due to fluctuating fuel prices and other general rate changes," the court said.

Glenn Beard of Pepper Hamilton LLP, Philadelphia, represented Hub Group, Inc. John Fitzpatrick of Mylotte, David & Fitzpatrick, Broomall, Pa., represented Clancy.

Full text of the decision is available at http://ddee.pf.com.

Production

Employee Not Required to Produce All E-mail in Account

A civil rights plaintiff must turn over some 400 e-mails from her America Online account to her former employer because they are relevant to her claims that her former supervisor sexually harassed her and then hacked into the account and stole the e-mails, a federal magistrate in New York ruled Jan. 20 (*Rozell v. Ross-Holst*, 2006 WL 163143 (S.D.N.Y. 2006).

Mary Rozell sued ANDCO LLC, its principal, and her former supervisor in the U.S. District Court for the Southern District of New York under Title VII of the 1964 Civil Rights Act, state and local employment discrimination laws, the Electronic Communications Privacy Act, and the New York Penal Law.

Rozell turned over the approximately 400 e-mails she claimed her supervisor had hacked from her AOL account, but she redacted the text of each document, leaving only its transmission history. Moreover, she otherwise refused to comply with the defendants' discovery demand for all mail accrued in the account after ANDCO started to pay for it when she joined the company, apparently to serve as a backup to her work e-mail.

Only Hacked Documents Held Relevant

On their motion to compel production, the defendants argued that every e-mail transmitted to or from the account during the period ANDCO paid for it was relevant to Rozell's sexual harassment, computer hacking, and physical and emotional distress claims, and should be produced, or at least reviewed *in camera*, rather than letting Rozell serve as the final arbiter of relevance. Privileged documents, they said, should be listed on a privilege log, and e-mails of a personal nature protected by a confidentiality order.

Rozell countered that she already had produced all responsive e-mails in the account. *In camera* review of the account was unnecessary, she contended.

The court granted the defendants' motion in part. The e-mails allegedly hacked from the account must be produced without redaction, the court said, because they are plainly relevant to her claims of illegal interception of electronic communications. The relief available on that claim includes compensatory and punitive damages, and if the subject matter of a communication is innocuous and the disclosure of it is unlikely to cause embarrassment to the victim, then the finder of fact might be justified in assessing only modest damages, the court said. But if it concerns a highly personal matter, a more significant award could be warranted, according to the decision.

Otherwise, the defendants are not entitled to discovery of the account, the court found. The other e-mails are not relevant to Rozell's hacking or sexual harassment claims, and counsel represented that all relevant documents in the account already were turned over, the court said. Review by the court to assess the relevance of the other e-mails would be improper, because the producing party has a duty to honestly and accurately respond to discovery requests and the requesting party has remedies for its failure to do so, the court wrote.

The full text of the opinion is available at http://ddee.pf.com.

Web-based Testimony

Reliance on Post-Incident Internet Data Disqualified Expert

An expert cannot claim familiarity with the local standard of care based on information the attorney downloaded from the Internet four and a half years after plaintiff's surgery, the North Carolina Court of Appeals ruled Jan. 17 (*Purvis v. Moses H. Cone Memorial Hospital,* 624 S.E.2d 380 (2006)).

The expert's familiarity with the hospital was solely based on Internet material supplied by the plaintiffs' counsel. Because that material was produced about four-and-one-half years after the incident at issue, the appeals court said it does not demonstrate the expert was familiar with the standard of care as it existed at the time of the incident, as required under North Carolina law (N.C. Gen. Stat. §90-20.12).

Because the expert testifying on behalf of plaintiffs in a medical malpractice lawsuit failed to demonstrate that he was familiar with the resources available to a hospital at the time of the incident at issue, a trial court properly granted the defendant-doctor summary judgment.

The matter stems from neurological damage suffered in February 1999 by a male fetus prior to delivery at the Women's Hospital of Greensboro. When delivered, Aeron Purvis had the umbilical cord wrapped around his neck.

Purvis' parents and guardian filed a medical malpractice lawsuit in the North Carolina Superior Court for Wake County against the hospital and three physicians, claiming their negligence caused Aeron's injuries. The trial court granted summary judgment for two of the defendant doctors, and the plaintiffs had voluntarily dropped their claims against the remaining physician and the hospital.

The plaintiffs appealed the ruling, claiming the trial court improperly granted summary judgment by finding the plaintiffs did not provide sufficient evidence to counter such a motion. Dr. Bernard A. Marshall, the mother's regular obstetrician/gynecologist, and Dr. McArthur Newell, the supervising physician on call when the mother was admitted, were the two defendants subject to the appeal.

Untimely Internet Information

The appeals court found that the trial court was correct in granting summary judgment to Marshall, as the plaintiffs failed to provide sufficient evidence regarding the standard of care at the hospital.

According to the appeals court, the plaintiffs' sole standard-of-care expert, Atlanta-based Dr. Alphonzo Overstreet, failed to adequately meet state standards regarding such testimony. "Review of Dr. Overstreet's deposition reveals that he had never been to Greensboro, had no colleagues there, had reviewed no demographic information regarding Greensboro, and was relying solely on the Internet materials supplied by plaintiffs' counsel as the source of his information about Women's Hospital," the court said.

Because the material provided to Overstreet was dated August 2003, it gave information about the hospital's resources more than four years after the incident at issue, according to the appellate court. "We cannot assume—as we would have to do in order to deem Dr. Overstreet competent to testify—that the resources and standard of care remained unchanged at Women's Hospital for a period of more than four years," the court said.

As Overstreet was the only expert testifying on behalf of the plaintiffs and he did not meet state competency requirements, sufficient evidence was not provided to counter the motion for summary judgment and the trial court's ruling, the appeals court said.

BEST PRACTICES

The Exhumation of Corpses and Digital Data: Insights into Conducting Forensic Examinations of Information Systems

Jeffrey B. Ritter and Daniel C. Garfinkel

Destroying or tampering with potentially relevant evidence is considered to be one of the most hostile affronts to the function of justice in the United States. A central foundation of our judicial system is the principle that documents and things with evidential value will be preserved and made available in the discovery process. When there is a contrary result, a judicial finding of spoliation or misconduct can fundamentally alter the outcome of a case. This reality is not new to our view of civil or criminal justice. However, the types of documents and things leading to judicial findings of spoliation and/or misconduct have evolved in recent years with the increasing prevalence of discoverable digital data. Indeed, the case law of the last two years provides a resounding roll call of the ease with which courts have confirmed that the spoliation of digital data is equally repugnant to how justice will be administered.[1]

Currently, lawyers and their clients are working hard to adjust traditional case management practices to the realities of e-discovery. Existing procedures to preserve "documents and things" often include asking tough questions to determine whether there has been any historic destruction or tampering. However, for electronic records (known as "electronically stored information" in the proposed revisions to the Federal Rules scheduled to become effective in December 2006), those procedures (and the questions) are generally not yet in place.

To locate evidence of the destruction or alteration of electronic records requires different types of tools, procedures and investigations. Essentially, counsel and client must conduct an "autopsy" of the available records and systems, examining the systems data and records in order to reconstruct the occurrence of events (such as file deletion) that could impact the credibility of specific records or testimony.

It is not surprising, therefore, that the professional technical services involved are called "forensics." Digital forensic experts are attempting not only to identify and locate potentially relevant records; they are also searching for evidence of whether relevant records have been altered, lost or destroyed. Forensic examiners are often regular members of the team in complex litigation and their services are becoming indispensable in many types of cases.[2]

However, many questions persist as to how digital forensic services can be conducted:

- When can an "autopsy" of an information system be performed?
- Can a digital forensic examination of specific systems or records be performed after a lawsuit has been filed (e.g., to determine whether particular employees have attempted to delete relevant files)?
- What risks exist that the examination may itself be viewed as tampering with the available records (particularly metadata and other internal systems data that can heavily influence the credibility of specific records) and potentially judged as spoliation?
- What steps should parties take to assure that the results of forensic investigation activities by adverse parties are themselves preserved?
- Should parties, as a part of their discovery plans, negotiate and agree upon the conditions under which their forensic examinations are conducted?
- How can the attorney-client or work product privilege be relied upon to protect from disclosure information learned from digital forensic activities?

As suggested by *Fosse v. Pensabene*, 838 N.E.2d 258, 2005 Ill.App. LEXIS 1095, 297 Ill. Dec. 771 (App. Ct. 2005), many of the answers to these questions may arise, quite literally, from the grave. This recent decision contributes to a substantial collection of statutes and case law in Illinois relating to the exhumation and examination of corpses, much of which is carefully reviewed by the court. In doing so, the *Fosse* court carefully considered the relevant legal standards of the discovery process, and it is this analysis that may well provide valuable insight into the practical strategies to be considered in conducting case-related digital forensic services.

The Facts of *Fosse*

Under Illinois' Wrongful Death Act, Fosse, as the executor for the decedent, brought a medical malpractice action against Dr. Pensabene, who had been providing cardiac care to the decedent. After the action was initiated, the defendant's interrogatories requested that the estate disclose information regarding the performance of any autopsy. In response, Plaintiff accurately stated that "an autopsy was not performed."

However, two weeks later, without notice to the defendant (and perhaps inspired by defendant's request itself), the decedent's body was exhumed and an autopsy was performed by the county coroner (at which plaintiff's counsel was in attendance and for which a videotape was produced

and photographs taken). Plaintiff obtained the coroner's written report (which attributed death to hemorrhagic shock) and made the report, the videotapes and photographs available to the defendant. The coroner was identified as an expert witness, and information about the autopsy was disclosed, in supplemental interrogatory responses, within seven days.

Eight months later, the defendant sought dismissal of the case, arguing that (1) advance notice of the exhumation and autopsy was required and (2) the autopsy constituted destructive testing of relevant evidence, for which the sanction of dismissal of the lawsuit was appropriate. The court observed that (a) an autopsy had not been requested or performed by the defendant, though that right existed under Illinois law, (b) there was no discovery order in place at the time of the autopsy prohibiting an autopsy from being performed, and (c) there was no separate law (other than the rules of discovery) imposing a duty to provide advance notice that an autopsy would be conducted. Defendant failed to prevail on any point—the plaintiff's right to conduct the autopsy without prior notice was affirmed, plaintiff was free to use the evidence gained from the autopsy and no sanctions would be imposed.

The Discovery Questions

The court was required to confront a number of intriguing questions in its analysis. The analysis of these questions will be considered and then their possible lessons for digital discovery strategies will be presented.

Does a party have a right to employ "discovery methods" after a lawsuit is commenced?

The court analyzed Illinois' law very carefully. Court Rule 201(a) identifies the physical examination of a person (albeit a dead person) as an appropriate "discovery method." That rule identifies the methods that may be employed to obtain information which is to be the subject of discovery and includes the "physical examination" of persons.[3] The court concluded that an autopsy may be employed to obtain information relevant to the subject matter of the pending action. However, the court did not rule that, just because a lawsuit has commenced, a party is forbidden from employing discovery methods on its own behalf.

Plaintiff also argued that records of the autopsy performed in the presence of counsel represented work product subject to protection against disclosure. However, because plaintiff was offering those records for review, the court concluded there was no reason to reach a determination on the applicability of the work product privilege.

Does an autopsy performed without prior notice to the defense constitute an "abuse of discovery rules"?

Illinois law actually addresses the rights of parties to participate in autopsies for various types of cases, including workers' compensation claims and insurance claims in which the autopsy will be necessary to resolve the related claim or gain relevant information. But such claims were not in question in *Fosse*.

The governing local rules expressly allowed that the court, on the motion of a party, could order a physical examination. However, as noted earlier, the defendant had never made a motion for the autopsy to be performed, even though the physical condition of the decedent was clearly relevant. The court concluded that, having had, and waived by its inaction, the opportunity to secure an autopsy under court supervision, the defendant was not otherwise entitled to prior notice.

Does an autopsy constitute "destructive testing" of material evidence, for which advance notice was required?

Defendant argued that the autopsy altered or partially destructed the decedent's body and therefore represented destructive testing in violation of the discovery rules. An earlier Illinois Supreme Court decision was cited in which a party's disassembly and metallurgical examination of a power-steering mechanism prior to the filing of a lawsuit was determined to constitute improper destructive testing.[4] In that case, the plaintiff's testing was determined to have unduly prejudiced the rights of the defendant, but not sufficiently to justify the trial court's earlier dismissal of the entire case.

By contrast, in *Fosse*, the court was influenced by several factors. First, the autopsy was not the only alteration of the decedent's body—it had already been embalmed and buried. Second, the entire record of the autopsy (video tape and photographs) was being made available to the defendant. Third, nothing indicated that the decedent's remains could not be re-autopsied by the defendant (and, in fact, certain internal organs had been separately preserved by the coroner). Under these circumstances, the plaintiff was determined to have taken "reasonable measures to preserve the integrity of relevant and material evidence".

The court took time to emphasize that a substantial burden rests on a party claiming discovery abuses where the incident that is the basis of that claim (i.e., the autopsy without notice) could have been avoided if the party had diligently exercised its rights to seek a protective order. The *Fosse* court stressed that the doctor defendant had the right to request an autopsy, or otherwise protect the evidence, from "any time after defendant filed its appearance." Moreover, since the interrogatories requested only historical autopsy reports (and did not make, but could have made, reference to future autopsies), the court declined to impose any obligation on the plaintiff.

Since a request for autopsy information was included in the original interrogatories, did the performance of the autopsy without advance notice constitute a "knowing concealment"?

The court was asked to evaluate as controlling authority an earlier case from Nebraska in which discovery sanctions were imposed based on the occurrence and disclosure of an autopsy without prior notice.[5] The analysis focused on three timing variables—the point in the case at which the autopsy was conducted, the timeliness of the disclosure of the autopsy and the proximity to trial.

In the Nebraska case, the autopsy was performed less than a month before trial and only disclosed two weeks before trial. In *Fosse*, the autopsy was performed very early in the litigation, was disclosed promptly and long before trial was on the horizon. As a result, the court easily distinguished *Fosse* as lacking the indicia of concealment that would appear to have been intended to prejudice the adverse party's rights.

Lessons for Managing Digital Forensics

The *Fosse* decision is only one case within a substantial body of law that relates to exhuming corpses and conducting autopsies.[6] But, the court's analysis suggests some practical considerations for how digital forensics should be incorporated into case management strategies. Much like the law of exhumation and autopsies has evolved, it is likely that litigants and judges will need to develop and apply suitable standards for digital examinations. Nevertheless, here are some of the factors to be considered, particularly with a view toward how to minimize possible claims of spoliation.

Pre-lawsuit Forensic Services.

Digital forensic services are often performed by companies in the ordinary course of internal quality control, enforcement of employment policies and the investigation of possible legal risks. It is entirely foreseeable that the facts giving rise to an internal investigation requiring digital forensics may later form the basis of a lawsuit.

- For example, a hospital wishes to evaluate access log data in order to determine if a specific nurse was logging onto pharmaceutical records in order to fraudulently obtain drugs for personal use outside of regularly scheduled work hours.
- Following a review of the access log data, the hospital does not create a record of the review and then permits the access data to be deleted and the records overwritten by more current access log records. Subsequently, the employee files a discrimination action, indicating he was falsely accused of fraudulent drug use based on his sexual preference.

In those instances, companies should evaluate whether the basis for the investigation gives rise to a duty to preserve evidence.[7] If that duty arises, then the records relating to the forensic activities should be preserved as fully as one might otherwise preserve relevant evidence. With reference to how the *Fosse* autopsy was documented, a company should consider what steps should be taken to assure that the forensic examination does not create a fact pattern that might later be viewed as evidence of tampering itself.

Interrogatories and Production Requests.

The *Fosse* defendant's interrogatories may very well have provoked the plaintiff to exhume the decedent and conduct the autopsy. The additional failure of the defendant to specify a request for advance notice of any future autopsy further handicapped the defendant's subsequent argument for discovery sanctions. How then should a litigant structure interrogatories and production requests when digital forensics may be important to determining the integrity of case-related records, or the occurrence of events recorded by a party's computer systems?

Electronically stored information ("ESI") is recognized as the most dominant form in which business records are created and maintained.[8] The scope and meaning of ESI is not limited to electronic versions of traditional business records, such as agreements, invoices, or prescription records. ESI also includes the type of data that is invaluable to digital forensics. Access logs, file directories, metadata, and records of file properties (collectively, "systems data") are all useful in determining the integrity of specific events or records.

In preparing production requests, counsel should anticipate that systems data might be important as relevant evidence, or as information leading to the discovery of relevant evidence. If those records have potential value, the production requests should specify what systems data is to be produced. Those requests, of course, must be rationally related to the nature of the case or other electronic records that are sought.

While digital forensic "autopsies" will not always be performed in every case, *Fosse* encourages litigants to consider the strategic value of requesting the related records of digital forensic investigations as a matter of course. However, a party must be cautious as to whether making the request will lead the adverse party to do something they may not have previously considered. Of course, as *Fosse* also makes clear, if a party does seek production requests for the records of digital forensic investigations, the requests should be crafted to include the records of investigations that may be conducted in the future. (For example, the hospital employee makes a production request of all systems data relating to the management of access to the pharmaceutical applications. While such systems data is not regularly retained, the employee's request prompts the hospital to secure the data before scheduled destruction occurs and the data provides nearly irrefutable evidence of the employee's misconduct.)

By deferring on making a pro-forma request for forensic records, an adverse party may be able to improve its position later if there is reason to question the integrity of specific records or events. Systems data is increasingly being

viewed as relevant by the courts to determine the truth regarding events relevant to a lawsuit.[9] If other information or evidence suggests that systems data may be useful to discovery, an adverse party's awareness of how to pursue that information may prove to be valuable. An early "fishing" request pursuant to initial production requests may increase the burden on a party to demonstrate that a subsequent forensic investigation is justified.

Requiring Advance Notice or Protective Orders.

One of the distinctions between digital forensics and forensics involving corpses (or the testing analysis of mechanical equipment) is that digital forensic services generally do not require the alteration of the records or any physical thing (such as a magnetic media device). Unlike the physical destruction involved with autopsies or engineering testing, digital forensics generally involves the recovery and analysis of systems data or the restoration of files otherwise still accessible. Digital forensics, when properly performed, does not involve electronic equivalents of cutting, dissecting, grinding or other physical acts that forever alter physical evidence. While some forensic activities involve the restoration of deleted or overwritten data, those services rarely put any data at risk since the media are fully duplicated before the performance of the forensic services. Following digital forensics activity, the data and magnetic media can be retained and, like the decedent's body in *Fosse*, retained for future review or examination (including by an adverse party).

As a consequence, the potential undue prejudice to an adverse party that may result from digital forensics conducted without notice (or in the absence of counsel's presence) is significantly diminished. Thus, if one party were to conduct digital forensic activity on its own, without notice, it is unlikely such activity would support a later objection or motion for discovery sanctions. However, that analysis is subject to an important caveat: as in *Fosse*, any digital forensics activity conducted after a lawsuit is filed and without prior notice to, or the involvement of, adverse party counsel, should be carefully documented and the results (and original media) suitably preserved. The overwriting (or other reuse) of media that has been subject to forensics analysis would, of course, provide a tremendous advantage to any adverse party on a future motion for sanctions; at that point, the destruction of the analyzed data or media would provoke claims of undue prejudice more likely to be sustained.

Whether a litigant should routinely seek a protective order against digital forensic activities by adverse parties presents a different set of considerations. Since any party is subject to a general duty to preserve potentially relevant evidence, and digital forensics generally do not put electronically stored information at risk, there is clearly a question of whether a party could persuade a court that a protective order against digital forensic activity could be justified. The better course in most circumstances would be to serve the opposing party with a well-constructed preservation request demanding that advance notice be provided prior to the initiation of any forensic activity, and making clear the serving party's desire to be present during any such activity, or at least be notified of such activity. Such a request could also be utilized to alert the opposing party to employ "reasonable measures to preserve the integrity of relevant and material evidence."[10]

Timing.

The *Fosse* decision highlights the need for adverse parties to act with due respect for the trial process. Although, in the end, the court did not object to the timing of the plaintiff's autopsy or the subsequent disclosure, the court did give serious consideration to defendant's timing objections. To the extent a party believes that digital forensics may be useful, the procedures should be pursued earlier rather than later and, as appropriate, the results disclosed promptly, particularly if those results tend to impact the relative merits or credibility of specific claims or related evidence.

What the *Fosse* court did not resolve, of course, is whether a party has any obligation to disclose digital forensic services (or the related records) if the adverse party has not requested the production of those records, sought a protective order or requested advance notice. For example, if digital forensics of a party's systems data produces records in contradiction of the adverse party's position in a case, is there any obligation to disclose that data prior to trial? Similarly, as in *Fosse*, if the services are performed in a manner that includes the party's counsel and seeks to protect the results as privileged work product, will those efforts be recognized by a court? These issues are topics on which the *Fosse* decision provides no insight.

The Future

In what direction will the law governing digital forensics evolve? Obviously, there can be no early predictions worth betting on. But, the standards governing the exhumation and autopsy of corpses confirms that the law of discovery already has many precedents on which to rely, whether in support or in opposition, when performing or challenging specific litigation tactics.

As a practical matter, perhaps the valuable lesson learned from the *Fosse* analysis is to be prepared. As the 21st century continues, the integrity and reliability of electronic records will be challenged with increased frequency. Digital forensics of information systems, the use of systems data and the introduction of the results of system autopsies into evidence will require dynamic and significant lawmaking as the judiciary seeks to craft acceptable norms regarding what constitutes persuasive and reliable electronically

stored information. Digital forensic services will present abundant opportunities for conflict and litigants should be mindful of those possibilities when structuring and executing their case strategies. The plaintiff in *Fosse* navigated between the existing legal boundaries effectively, seizing the opportunity to use discovery methods without the presence of opposing counsel while acting responsibly to preserve the integrity of the relevant evidence. Parties who pursue a similar path in employing digital forensics on their own are likely to be able to do so without significant opposition.

Endnotes

[1] See *E*Trade Sec. LLC v. Deutsche Bank AG*, No. 02-3682 RHK/AJB, No. 02-3682 RHK/AJB, 2005 U.S. Dist. LEXIS 3021 (D. Minn. Feb. 17, 2005) (recommending an adverse inference instruction where defendants failed to properly preserve computer hard drives, telephone recordings, and e-mails); *Zubulake v. UBS Warburg LLC*, 229 F.R.D. 422 (S.D. N.Y. 2004) (granting plaintiff's motion for costs and an adverse inference instruction where defendant failed to properly produce e-mails); *Mosaid Technologies Inc. v. Samsung Electronics Am., Inc.*, 348 F. Supp. 2d 332 (D. N.J. 2004) (affirming a spoliation inference and monetary sanctions where defendants failed to properly preserve e-mails); *Metro. Opera Ass'n, Inc. v. Local 100, Hotel Employees & Rest. Employees Int'l Union*, 212 F.R.D. 178 (S.D. N.Y. 2003) (granting judgment as to liability and costs where party failed to properly produce paper and electronic records); *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc.*, No. CA 03-5045AI, 2005 WL 674885 (Fla. Cir. Ct. March 23, 2005) (granting partial default judgment where defendant failed to properly produce e-mails).

[2] Regulatory authorities have also recognized the importance of forensic examinations. In late 2004, the U.S. Securities and Exchange Commission posted a new job description for a digital forensics examiner, responsible for assuring the integrity of the systems of regulated entities. *See also* Jack Seward & Daniel A. Austin, *E-Sleuthing & the Art of Electronic Data Retrieval: Uncovering Hidden Assets in the Digital Age* (pts. 1-3), 23-1 AM. BANKR. INST. J. 14 (Feb. 2004), 23-1 AM. BANKR. INST. J. 14 (Mar. 2004), 23-1 AM. BANKR. INST. J. 14 (Apr. 2004) (addressing the use of digital forensic technology with regard to bankruptcy litigation).

[3] Illinois Court Rule 201(a) reads as follows: "**(a) Discovery Methods.** Information is obtainable as provided in these rules through any of the following discovery methods: depositions upon oral examination or written questions, written interrogatories to parties, discovery of documents, objects or tangible things, inspection of real estate, requests to admit and physical and mental examination of persons. Duplication of discovery methods to obtain the same information should be avoided." ILL. CT. R. 201(a), *available at* http://www.state.il.us/court/SupremeCourt/Rules/Art_II/ArtII.htm#201.

[4] *Shimanovsky v. General Motors Corp.*, 181 Ill. 2d 112, 692 N.E.2d 286 (1998).

[5] *Schindler v. Walker*, 256 Neb. 767, 592 N.W.2d 912 (1999).

[6] *See generally* Annotation, *Disinterment in Criminal Cases*, 63 A.L.R.3d 1294 (1975); W.R. Habeeb, Annotation, *Power of Court to Order Disinterment and Autopsy or Examination for Evidential Purposes in Civil Cases*, 21 A.L.R.2d 538 (1952).

[7] *See, e.g., Barsoum v. New York City Hous. Auth.*, 202 F.R.D. 396, 400 (S.D. N.Y. 2001) (stating that, a "party has a duty to retain evidence that it knows or reasonably should know may be relevant to pending or future litigation."); *U.S. ex rel. Koch v. Koch Indus., Inc.*, 197 F.R.D. 463, 484 (N.D. Okla. 1998) (noting that, the "obligation to preserve evidence that is potentially relevant to imminent or ongoing litigation is an affirmative duty that rests squarely on the shoulders of senior corporate officers.").

[8] *See The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production* (The Sedona Conference Working Group Series, January, 2004), available at http://www.thesedonaconference.org/publications_html (noting that, "at least 93 percent of information created today is first generated in digital format, 70 percent of corporate records may be stored in electronic format, and 30 percent of electronic information is never printed to paper.").

[9] *See In re Priceline.Com Inc., Sec. Litig.*, No. 3:00CV01884(DJS), 2005 U.S. Dist. LEXIS 33636 (D. Conn. Dec. 8, 2005) (requiring the production of searchable metadata databases); *Williams v. Sprint/United Mgmt. Co.*, 230 F.R.D. 640 (D. Kan. 2005) (requiring the production of electronic spreadsheets' metadata, as well as requiring the spreadsheets to be produced with "unlocked" cells and data).

[10] *Fosse v. Pensabene*, 838 N.E.2d 258, 297 Ill. Dec. 771, 2005 Ill. App. LEXIS 1095, at *25 (App. Ct. 2005).

Jeffrey B. Ritter *is a partner of Kirkpatrick & Lockhart Nicholson Graham, resident in their Washington office, and* ***Daniel Garfinkel*** *is an associate with the firm, resident in their Pittsburgh office. Both are active in the firm's Records Management and E-discovery practice group.*

CALENDAR

MARCH

8

b-Discovery Meeting. Les Halles de Paris, 1201 Pennsylvania Ave NW, Suite 100, Washington, D.C.

Contact: dregard@lecg.com.

23-24

Advanced E-discovery Certification Course. Eden Prairie, Minnesota. Presented by Kroll Ontrack®.

Contact: http://www.krollontrack.com/upcomingevents.

27-29

E-Discovery Preparedness For the Pharmaceutical Industry: Building Teams, Controlling Costs, and Developing Compliant Retention Strategies. New York City. Presented by American Conference Institute.

Contact: http://www.americanconference.com

The Legal and Strategic Guide to E-Discovery West: Best Practices for Corporate Counsel. San Francisco, Cal. Presented by Marcus Evans Ltd. and Media Partner Digital Discovery & e-Evidence.

Contact: http://www.marcusevans.com

28-29

The Legal and Strategic Guide to E-Discovery: Proactively Preparing for the Challenges of Electronic Discovery. Toronto, Ontario. Presented by Marcus Evans Ltd.

Contact: http://www.marcusevans.com

30

E-mail Discovery & Retention Policies Conference. New York City. Presented by LexisNexis Mealey's.

Contact: http://www.mealeys.com/conferences

30-31

3rd National In-House Counsel Conference on Defending & Managing Complex Litigation. Atlanta, Ga. Presented by American Conference Institute.

Contact: http://www.americanconference.complexlit

APRIL

7

Attorney E-discovery Training Course. Eden Prairie, Minnesota. Presented by Kroll Ontrack®.

Contact: http://www.krollontrack.com/upcomingevents.

28

Electronic Discovery and Digital Evidence Institute. Houston, Texas. Presented by the State Bar of Texas.

Contact: craig@ball.net

MAY

16-18

Document Retention & Electronic Discovery: Practical Solutions and Best Practices. Toronto, Ontario, Canada. Presented by Legal IQ, a division of International Quality & Productivity Centre.

Contact: http://www.iqpc.com/LegalIQ

18-20

Electronic Records Management and Digital Discovery: Practical Considerations for Legal, Technical, and Operational Success. Chicago, Ill. Sponsored by ALI-ABA with the cooperation of the Federal Judicial Center.

Contact: http://www.ali-aba.org

22–24

The 14th Annual National Conference on Managing Electronic Records. Chicago, Illinois. Presented by Cohasset Associates.

Contact: http://www.merconference.com

JUNE

13-14

The Legal and Strategic Guide to E-Discovery: Optimizing Your Protocols for Effective E-Data Management and Discovery. New York City. Presented by Marcus Evans Ltd.

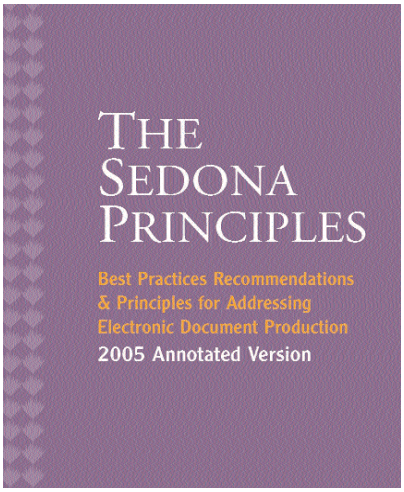
Contact: www.marcusevansto.com/ediscoveryny

The Sedona Principles

ORDER NOW!
800-255-8131
ext. 248

Best Practices Recommendations & Principles for Addressing Electronic Document Production

2005 Annotated Version



Pike & Fischer is pleased to present the 2005 annotated edition of *The Sedona Principles.* Crafted by some of the nation's finest lawyers, consultants, academics, and judges under the auspices of the highly regarded Sedona Conference®, *The Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Production* was the first formal attempt to provide a common approach for managing discovery practice as it changes with technology. The first annotated version, published in 2004, quickly became the "must-have" resource for both the bench and the bar.

E-discovery's evolution in the past year is chronicled in our new publication. The *2005 Annotated Edition* not only explains the policy underlying the 14 Principles that state and federal judges continue to rely on to resolve contested discovery disputes, it also contains citations to and analysis of their latest orders and opinions - including the obscure and hard-to-find ones, in addition to those with higher profiles.

Fax Order Form • fax to: 301.562.1521 • call: 1.800.255.8131 • e-mail: customercare@pf.com

❑ **Send me** _____ copies of *The Sedona Principles* at $129* each. (Shipping $5/copy; $12 multiple copies)

Total $ _____

Name _____ Title _____

Organization _____

Street Address _____

City _____ State _____ Zip _____

Telephone _____ E-mail Address _____

❑ **Please charge my** ❑ VISA ❑ MC ❑ AMEX Acct. No. _____

Signature _____ Expiration Date _____

**Your credit card statement will show a charge from Pike & Fischer, publisher of* Digital Discovery & e-Evidence.

1010 Wayne Ave. - Suite 1400, Silver Spring, MD USA 20910-5600 - Telephone (301) 562-1530 or (800) 255-8131, Fax (301) 562-1521

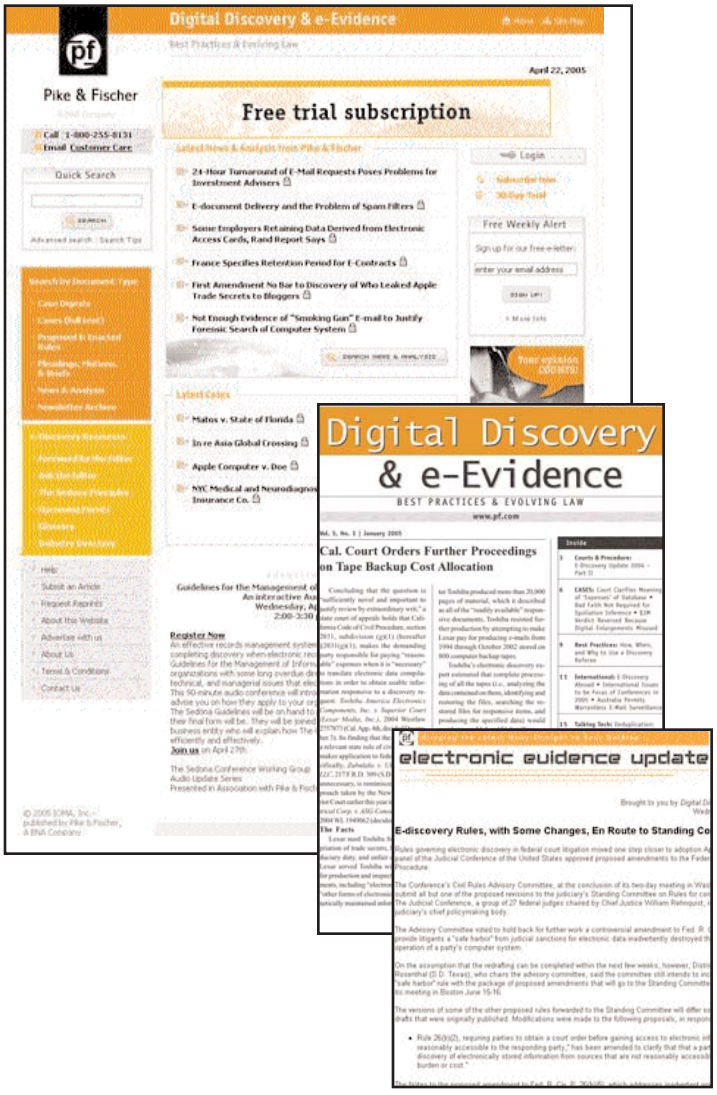
New Web Reference Service

Digital Discovery & e-Evidence

http://ddee.pf.com

Pike & Fischer's new *Digital Discovery & e-Evidence* web reference service provides 24.7 access to all the information you need relevant to electronic evidence and discovery. Consult the new DDEE website for:

- Full text of all Relevant Decisions
- Case Digests
- Proposed & Enacted Rules
- Pleadings, Motions & Briefs
- Complete News & Analysis Archive
- Glossary
- Industry Directory
- Upcoming Events



An easy-to-use interface provides quick and easy searching of documents, decisions, and articles.

"Your new product is a brilliant and effective upgrade to your offerings. I accessed it easily and quickly found myself immersed in the web based cases and the articles, all of which came up smoothly and were easy to read. It will save me valuable hours - as well as capturing things I do not normally see."

Thomas Allman, Special Counsel
Mayer Brown Rowe & Maw
Chicago

For More Information:
Call: 800-255-8131, ext 248
301-562-1530, ext. 248
Email: customercare@pf.com
Visit: http://ddee.pf.com

Pike & Fischer, A BNA Company, 1010 Wayne Ave, Suite 1400 Silver Spring, MD 20910 www.pf.com