

# Digital Discovery & e-Evidence

BEST PRACTICES &amp; EVOLVING LAW


<http://ddee.pf.com>

Vol. 5, No. 12 | December 2005

## Maryland District Court Gives Guidance on Privilege and ESI

A motion to compel responses to a broad discovery request for electronically stored information (ESI) in an employment discrimination action provided the opportunity for a federal magistrate to weigh in on a widely-perceived deficiency of the proposed amendments to the Federal Rules of Civil Procedure: how to protect privileged information when producing ESI. (*Hopson v. The Mayor and City Council of Baltimore*, 2005 WL 3157949, D. Md., November 22, 2005.)

The underlying action included putative class and individual claims against the City of Baltimore and its police department asserting that the department engaged in racial discrimination against African Americans in connection with the administration of the disciplinary system for Baltimore police officers.

As soon as the discovery period commenced, plaintiffs sought information on the “nature, extent, and location of electronically stored records, the defendants’ IT capabilities, the nature of archived data, e-mail, and records retention policies — in short, all of the computer generated information that is the subject of so much discussion these days.” The defendants filed numerous general objections, including burdensomeness and the expense of performing pre-production privilege review of the records, which the court criticized as too vague and lacking in detail.

After receiving augmented but still deficient support from defendants for their opposition to the motion, Magistrate Judge Paul W. Grimm ruled on some of plaintiff’s requests but ordered the parties, after consultation with the defendants’ IT manager, to present a reasonable discovery plan for ESI to the court within 30 days. He specifically ordered the parties to “discuss the Rule 26(b)(2) factors in connection with the procedures that defendants reasonably should take to perform a review for privilege and work product claims, given the nature of the litigation, the long time period for which the records were sought, and the resources of the parties.”

### Uncertainty

However, he also wrote the extensive Memorandum under consideration because the case “highlights significant unresolved issues relating to the nature of privilege review that must be performed by a party producing electronically stored information, whether non-waiver agreements entered into by counsel to permit post-production assertion of privilege are permissible and effective for their intended purpose, as well as the application of principles of substantive evidence law related to the waiver of privilege by inadvertent production.”

Judge Grimm frames the issue succinctly as “how properly to conduct Rule 34 discovery within a reasonable pretrial schedule, while concomitantly

### Inside

3	Justice Department Abandons Prosecution of Arthur Andersen
4	<b>Regulatory Developments:</b> SEC Relaxes Policy on Routine E-mail Inspection
5	<b>Conference Reports:</b> Judges Speak Candidly About E-discovery Expectations; 6 SEC G. C. Recommends an Expansive View of Technology
7	<b>Best Practices:</b> Managing Litigation Holds in the New Era of Compliance Duties
9	<b>Cases:</b> Specifications for Orders for ‘Pen Registers,’ Tracing Devices; VA Ethics Opinion on Paperless Files
12	<b>Talking Tech:</b> Legal Defensibility of E-Signatures Tested in Simulated Trial
14	<b>Calendar</b>

insuring that requesting parties receive appropriate discovery, and that producing parties are not subjected to production timetables that create unreasonable burden, expense, and risk of waiver of attorney-client privilege and work product protection.”

As with so many ESI issues, Judge Grimm explains, protecting privilege has become difficult and expensive because the data to be reviewed is voluminous and unorganized. The solution of various jurisdictions – and the

continued on page 2

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.

As the Advisory Committee noted, this approach does not address the substantive questions 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.

**Enforceability Problems**

The first problem with the use of non-waiver agreements is that they may not be enforceable as to the parties that enter into them. Second, their effectiveness against third parties is even more doubtful. Moreover, 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.

If these considerations lead to the conclusion that no production of ESI can be accomplished in civil cases absent a comprehensive privilege review and particularized assertion of privilege and work product claims, the costs, in terms of both money and time, would be prohibitive.

**Court Orders Are Key**

Judge Grimm’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 waiver. It implicates both Fed. R. Evid. 501 and the doctrine of compelled disclosure encompassed by Proposed (but not enacted) Rule of Evidence 512, which Judge Grimm argues can be considered a “standard.”

The import of the Rule, the standard, and cases like *Transamerica Computer Co. v. IBM*, 573 F.2d 646 (9th Cir. 1978) is that a party that is compelled to produce privileged material, or erroneously produces it, does not waive privilege. That case involved voluminous documents, an accelerated discovery schedule, and “Herculean efforts” on the part of the producing party to comply, circumstances that led the court to conclude that production was “made without (adequate) opportunity to claim the privilege,” and that the production of some of the privileged material had occurred as a result of the trial court’s discovery order. The *Transamerica* approach can even be extended to third party

**Digital Discovery**  
& e-Evidence  
[www.pf.com/digitaldisc.asp](http://www.pf.com/digitaldisc.asp)

**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: [customer care@pf.com](mailto:customer care@pf.com) Web: [www.pf.com](http://www.pf.com)

Published monthly. ISSN: 1537-5099 Subscription rate: \$559  
 Copyright © 2005 IOMA, Inc. Published by Pike & Fischer

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

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

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

Routine or systematic photocopying of this publication or portions thereof is a violation of Federal copyright laws. To ensure compliance with copyright regulations or to inquire about licensing any Pike & Fischer content, contact Pike & Fischer Customer Care at [customer care@pf.com](mailto:customer care@pf.com) or call us at 1-800-255-8131 x 248/301-562-1530 x 248. While no copyright is claimed in any materials obtained from official United States Government Sources, including text of statutes, rules, or regulations, all other rights are reserved.

claims if: “(a) the party claiming privilege took reasonable steps given the volume of electronically stored data to be reviewed, the time permitted in the scheduling order to do so, and the resources of the producing party; (b) the producing party took reasonable steps to assert promptly the privilege once it learned that some privilege information inadvertently had been disclosed, despite the exercise of reasonable measures to screen for privilege; and importantly (c) the production had been compelled by court order that was issued after the court’s independent evaluation of the scope of electronic discovery permitted, the reasonableness of the procedures the producing party took to screen out privileged material or assert post-production claims upon discovery of inadvertent production of privileged information, and the amount of time that the court allowed the producing party to spend on the production.”

### Pre-production Privilege Review Unavoidable

The biggest lesson of Judge Grimm’s analysis: even with non-waiver agreements in place, reasonable pre-production privilege review cannot be eliminated or replaced with a cursory screening. As he notes in Footnote 39: “Reviewing appellate courts are unlikely to accept the doctrine of compelled disclosure under Proposed Rule 512 if it is offered to justify transparently inadequate pre-and post-production privilege review and assertion. . . . Similarly, absent any clear signal from the appellate courts that they should do other-

wise, district courts called upon to ‘bless’ the production procedures agreed upon by counsel with a court order should independently satisfy themselves that full privilege review reasonably cannot be accomplished within the amount of time the court has allowed for production. The court also should satisfy itself that the procedures agreed upon by counsel regarding privilege production are in fact reasonable and that more could not be accomplished with the production period given the scope of electronic records production permitted by the court.”

— C. Eoannou

### Editor’s Note

The *Hopson* opinion will be the topic of a 90-minute audio conference on January 11, from 2:00 to 3:30 p.m. est. The author of the opinion, **The Honorable Paul W. Grimm**, will be 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 will moderate our program. Details and registration information will be available shortly at <http://ddee.pf.com>.

## Justice Department Abandons Prosecution of Arthur Andersen

Government prosecutors will not retry Arthur Andersen LLP for shredding documents related to the collapse of Enron Corp. in late 2001 (*United States v. Arthur Andersen*, 5th Cir., No. 02-21200, November 22).

In a motion filed with the U.S. Court of Appeals for the Fifth Circuit in New Orleans, the Justice Department’s Enron Task Force requested that the court remand the case to the U.S. District Court in Houston to vacate the conviction and dismiss the indictment with prejudice.

“The government has determined that it is in the interests of Justice not to re-prosecute Andersen on the pending charge,” the motion said.

In a responsive statement, Andersen said it was “pleased with the decision by the Department of Justice to request the Fifth Circuit to remand the case to trial court for the expressed purpose of having the case dismissed.”

“This represents an important step in removing an unjustified cloud over the professionalism and integrity of the people of Arthur Andersen,” the company said.

The Chicago-based accounting firm had served as Enron’s long-time auditor.

### Supreme Court Had Reversed Verdict

The U.S. Supreme Court unanimously overturned Arthur Andersen’s conviction in May and remanded the case for further proceedings consistent with its opinion. (See *DDEE*, June 2005, p. 3.) The court held that the trial judge in Houston erred when she told jurors they could convict Arthur Andersen even if employees did not know that shredding Enron documents was illegal.

Counsel for Andersen argued that Andersen employees were merely following a legal document retention policy when they shredded documents immediately prior to receiving a Securities and Exchange Commission subpoena related to an investigation of the collapse of Enron.

The trial judge, Judge Melinda Harmon of the U.S. District Court for the Southern District of Texas, imposed a maximum \$500,000 fine and sentenced the accounting firm in June 2002 to five years probation after jurors found the company guilty of obstructing justice by altering and shredding documents. The U.S. Court of Appeals for the Fifth Circuit upheld the conviction.

In March 2002, a federal grand jury in Houston indicted Arthur Andersen on charges that it destroyed documents to keep them away from federal investigators. The jury returned a guilty verdict against the accounting firm.

# REGULATORY DEVELOPMENTS

## SEC Official Says Agency Relaxing Policy on Routine E-mail Inspection

Gene Gohlke, associate director of the Securities and Exchange Commission's Office of Compliance Inspections and Examinations, Nov. 8 said that about six months ago, the Commission staff stopped asking registered investment advisers in routine inspections for all of their e-mails for the past three months. Instead, he said, the staff is targeting e-mail when they have specific suspicions of wrongdoing.

### Blanket Requests

Speaking at the SEC-sponsored CCO Outreach National Seminar in Washington, Gohlke said blanket requests for e-mail were used extensively in the wake of the market timing and late trading scandals that broke in 2003, but that "in the last year or so" the approach began turning up less and less information. "That's in part why perhaps we've changed our policy for e-mails," he said.

Gohlke also explained that suspected wrongdoers began to evolve their tactics. The sweeps and requests for e-mail as evidence "have been in the news extensively, so people are smart and may get the idea" to use the telephone or another method of communication to further a scheme, he said.

In 2004, representatives of the Investment Counsel Association of America—now called the Investment Adviser Association—met with several SEC commissioners and staff seeking guidance or a rule on e-mail inspection policy. ICAA could not be reached for comment on Gohlke's remarks.

Current protocol, Gohlke said, calls for SEC examiners to review information on compliance programs and then, "if we identify areas that seem to warrant more in-depth review," to make a secondary request that includes e-mails.

### Problem Areas

Once such a request is made, he continued, "We try to target our e-mail requests to areas where we think there are potential problems." Gohlke amplified that such targeted requests may be centered on communications related to a person or group of persons, or an activity.

Gohlke meanwhile encouraged companies that receive e-mail requests to contact the commission staff in an effort to narrow the petition. "Talk with the examination staff," he implored. "We don't want to create any more burden [than] necessary. To the extent there's another way to get us the information, we're ready to listen."

### Privilege

Appearing on a panel with Gohlke, Andrew Beagley, chief compliance officer of Citigroup Asset Management, explained

how his firm tries to comply with SEC e-mail requests while protecting sensitive attorney-client information. Beagley said that after Citigroup retrieves the electronic communications, it sends them to its outside counsel to judge whether any of them are privileged. Wendy Fox, chief compliance officer of Ariel Capital Management who was the third panelist, said the procedure is the same at her firm.

"[The outside counsel] will typically come back to us with a list of e-mails they have questions on," Beagley explained. For example, "Who was this lawyer you were talking to? What was the nature of the discussion?" Based on that, we will come up with a list of e-mails we consider privileged."

Gohlke stated sympathy with the question of privilege, but asserted nonetheless "advisers also have the duty to promptly produce records that are requested by the staff." He expressed dismay that sending e-mails—sometimes 500,000 to 1 million per request—to counsel for review could slow the turn-over process by weeks or even months. The disparate mandates of SEC examinations and corporate privilege, he said, "grind on each other."

To offset the dueling priorities, Gohlke suggested that certain sensitive e-mails contain key words in the subject lines to indicate their status. A key-word search would then net those particular communications. Such a protocol, he suggested, would "make production more quick and reduce what I would assume would be a heavy legal bill."

While not agreeing or disagreeing with the suggestion, Fox wondered whether such a system is feasible given the disparate training and backgrounds of staffers using e-mail. "I have to be trained to know to give the cue word" to signify privilege information, she said. Because not everyone is trained in legalisms, "it might be difficult for people in the business units to know they are passing on privileged information," Fox said.

### Request Relief

In response, Gohlke acknowledged, "Perhaps there isn't any easy way of identifying those documents, [but] you would think ways could be found." Beagley, meanwhile, expressed that the SEC's cessation of e-mail sweeps has relieved his firm of a logjam of e-mails being inspected for possible delivery to the agency, making the process that much more efficient. "Now we're in a different period, and if we're dealing with an exam on a case-by-case basis, it's much easier to focus on that one request," he said.

On a related subject, Beagley said Citigroup Asset Man-

agement allows its staffers to utilize instant messaging technology. He cautioned, however, “There’s always a concern that when people start getting more creative with the different media they’re using, how are we going to keep up with retention?” Fox said Ariel Capital Management does not allow instant messaging.

Finally, Gohlke explained that monitoring e-mails—what Plaze called looking out for “bad apples”—is at the discretion of individual companies. He recounted, however, “more and more information is flowing via e-mail, and there can be a lot of suspect e-mails that compliance people might like to be aware of.”

He continued: “Think of it this way. Suppose there are a couple of people at the firm that are running some scheme that is systematically ripping off clients of the firm, but it’s not really obvious unless you really dig in and read their e-mails.” After a while, for some reason, the scheme unravels.

“The SEC comes in,” Gohlke said, “takes a look, requests e-mails and, wow, it’s right there. Nobody at the firm had bothered to look at the e-mails, and I suspect the CCO

and others at the firm would be a bit embarrassed: ‘Gee, it was here under our noses, and we didn’t see it.’ ... It would seem in many cases to be prudent [to] monitor e-mails in some way.”

### Higher Risk

To mitigate monitoring costs and effects—mainly a negative connotation about Big Brother-like snooping—Gohlke suggested firms could sample e-mails. “Why wouldn’t it be feasible to identify people in the firm that are perhaps at higher risk for abusing e-mails or at higher risk of being able to participate in some sort of scheme or arrangement that could harm clients, and then on a sample basis monitor those persons’ e-mail?”

Even if a firm randomly monitors e-mail traffic to and from a particular individual, “I would think just having that notion out there at a firm, that somebody in the compliance area can [read e-mails randomly], can have a deterrent effect,” he said.

— *Special from BNA by Richard Hill*

## CONFERENCE REPORTS

### Judges at Georgetown Conference Speak Candidly About Their E-discovery Expectations

Three jurists pulled no punches at the November 17-18 Advanced E-discovery Institute presented by Georgetown University Law Center Continuing Legal Education, bluntly responding to questions about what they expect from litigants during e-discovery.

The Honorable Randall T. Shepard, Chief Justice of the Indiana Supreme Court, posed provocative inquiries that elicited stern advice from Magistrate Judge John M. Facciola (D.D.C.) and U.S. District Judge Barbara J. Rothstein (W.D. Wa.). They were unanimous in their view that whenever a case implicates electronically stored information, lawyers must be able to present their judges with an early, realistic, and detailed assessment of the issues arising from it.

#### Be Prepared to Talk Technology

Invoking the specter of Morgan Stanley’s backup tapes that, forgotten in Brooklyn, contributed to record-setting sanctions, Judge Rothstein urged the 150-member audience to familiarize themselves with their client’s systems prior to the Rule 26(f) meeting. She posited that knowing what information is stored electronically, where it is located, and how it is kept is crucial intelligence that must be shared at the meet and confer. Such information will, among other things, enable the judge to “get hold of the discovery” and thus be able to move towards a trial date, she explained.

Judge Facciola emphatically agreed with Judge Rothstein’s admonition not to be “the one in the room who knows the least about what you’re talking about” and cautioned the audience not to underestimate the technical expertise of the federal bar. He pointed out that magistrate judges run criminal dockets that require them to issue orders for evidence from such technically sophisticated devices as pen registers and geographic positioning systems. Similarly, the electronic filing systems that have been a mainstay of federal courthouses for several years required federal judges to become among the most technologically savvy members of the legal profession.

From this perspective, the meet and confer emerges as the perfect opportunity to either win or lose the judge’s credibility. “When the judge asks a question, be sure the judge can trust the answer,” warned Judge Rothstein.

She urged the audience to realize that if their technological explanation of why certain data cannot be recovered is inaccurate, the judge is likely to recognize the inaccuracy, which will lead him to doubt the accuracy of all future representations.

#### Know Thy Judge

Judge Rothstein pointed out that there nonetheless remains a “range of knowledge” about e-discovery among the judiciary, and no case assignment process exists that will ensure the expertise of the judge hearing your techno-

logically complex matter. Accordingly, it is incumbent upon counsel to make an effort to assess the judge's technical acumen prior to the meet and confer.

Judge Rothstein suggested that the attorneys from both sides approach the judge's clerk jointly with a diplomatic inquiry along the lines of "when we make our presentation on e-discovery, how much detail does the court want?"

Judge Facciola added that a Lexis or Westlaw query using the judge's name and "e-discovery" as search terms, or a quick check of web sites for the judge's participation as an e-discovery CLE panelist can provide the information needed.

### Pointers on Preservation

Acknowledging that having multiple information technology managers can complicate the process, Judge Facciola advised the audience to get input from the IT department on the scope of preservation. He suggested that the one significant lesson of the recent case law is that sanctionable behavior appears to derive from either "over promising or under promising" on what will ultimately be produced.

Echoing those sentiments, Judge Rothstein emphasized the importance of talking about preservation realistically,

identifying the actions that can be taken immediately, and those that must be deferred. It is crucial to have a plan that furthers the goal of preserving the data necessary to the presentation of the case without destroying the business in the process, she said.

### Calling on a Neutral

How do you resolve battles between IT experts? Judge Rothstein advocates calling in a neutral IT person. She explained that doing so has three advantages: the neutral will be able to explain which party's expert is correct and why, the neutral can come up with suggestions to move the parties beyond impasse, and, since both sides will share the cost of the neutral, they might be more motivated to resolve their dispute.

Judge Facciola has found holding a hearing on IT issues, replete with examination of experts and issuance of findings of fact, to also be effective.

Sometimes, Judge Rothstein added, the particularity of a request for information can be an indicator of genuineness of the party's need for it. All of these strategies are necessary, concluded Judge Facciola, for preventing e-discovery from becoming "a play thing of the rich," and forcing settlements inappropriately — *C. Eoannou*

## SEC General Counsel Recommends an Expansive View of Technology

Securities and Exchange Commission General Counsel Giovanni Prezioso Nov. 18 told an American Bar Association gathering that while technology is constantly advancing, it is important to study the big picture rather than focus on incremental developments.

"Technology issues frequently are framed, I think, too narrowly as a special subset of issues that deal only with the particular practical problem that emerging technology can raise," Prezioso said.

He cited relatively recent issues that were given birth by emerging technology—questions about posting information on the Internet, using e-mails, the creation and retention of electronic records—and acknowledged the import of settling issues raised by their advent. Prezioso added, however, that "over time, as we address those issues piecemeal, I think there's a risk of losing sight of some of the larger possibilities that wholesale technological changes can bring about."

He urged ABA members to use their "unique positions" "to help the commission fully recognize some of the potential benefits of technological change," especially as those changes can reduce costs and increase information outreach to investors.

Prezioso observed that by not focusing on technological advancements on a case-by-case basis and instead looking long-term, "the future actually holds the potential for

many more beneficial regulatory changes that can really harvest the benefits of new technology."

### Information Delivery

Emerging technology as a whole, Prezioso predicted, will have its greatest impact in the way information is delivered to investors as well as the quality of that data. He also observed that technology will help the SEC take on problems that hitherto had been impractical, citing 1934 Securities Exchange Act Regulation FD (Fair Disclosure) as an example.

"Not many people think of Reg FD as a technology rule," Prezioso said. "But in a very practical sense, Regulation FD is a product of communications technology changing because it simply couldn't be implemented in a world without Webcasts, universal conference calls, and other techniques that let management get in touch with [the investment community] on essentially a real-time basis."

Prezioso also cited proposed rules on point of sale disclosure. "Those rules wouldn't just rely upon the ability of technology to get information out quickly. What they do is enable investors to get the information before they make their investment decisions." He called such a change "a pretty dramatic step in the history of securities laws," especially as compared to the postal era of prospectus and sales confirmation delivery.

Prezioso further discussed proxy reform as a potential beneficiary of new technology. After watching the television program “American Idol” and its real-time voting format, Prezioso said he wondered, “If tens of millions of pre-teenagers can essentially vote simultaneously to choose the best singer, you would think that maybe we would have the technology to let the country’s largest companies have real-time, online voting of their shareholders.”

### New Language

On another level, Prezioso wondered about the changes that might accompany interactive data, specifically XBRL [extensible business reporting language], a communications initiative being studied by the commission. In thinking about XBRL, he said, “What needs to be considered is more than the technology involved. The decisions that are made

have a lot of potential collateral ramifications” that could reach into accounting standards and even generally accepted accounting principles. It is a matter, Prezioso said, “that needs to be thought through.”

Finally, regarding Edgar, the commission’s database of corporate filings, Prezioso noted, “We’re at the point where the potential for rethinking Edgar can create a lot of new possibilities for rethinking the kinds of data that we want investors to have and the mode we want them” to receive the information in.

— *Special from BNA by Richard Hill*

### Editor’s Note

The Securities and Exchange Commission announced Nov. 30 that General Counsel Giovanni Prezioso is leaving the agency to return to the private sector.

## BEST PRACTICES

### Managing Litigation Holds: Best Practices for the New Era of Compliance Duties

By Stacy O’Neil Jackson

Prior to *Zubulake v. UBS Warburg LLC*, 229 FRD 422 (SD NY 2004) (*Zubulake V*), the litigation hold letter was just one item among many on the general litigation checklist. In the post-*Zubulake V* era, the rules have changed for paper, as well as electronic data. (Hereinafter, paper and electronic data will be referred to collectively as data.)

The litigation hold letter can no longer be just an item on the checklist. It demands an entire checklist all its own.

Indeed, the proposed changes to the Federal Rules have reinforced the post-*Zubulake V* litigation hold duties. Several of the proposed amendments to the Federal Rules are geared to force the parties to pay attention to electronic discovery issues early in the game.

It is no longer acceptable to “stick your head in the sand” and pretend your case does not have e-data issues.

Specifically, proposed amended Rule 26(f) requires parties to discuss any issues relating to preserving discoverable information. Additionally, proposed amendment to Rule 37(f) will protect a party from sanctions for data deleted during the routine, good faith operation of its computer systems.

“Good faith” may require that a party suspend certain features of its computer system, and the steps taken to implement an effective litigation hold will determine if a party acted in good faith.

Here are the areas to address when considering your duties with regard to litigation holds.

### Review Document Retention Policy and Mechanisms for Enforcement

In the late 1980’s, document shredding conjured up images of Fawn Hall and Ollie North at the shredding machine during the Iran-Contra Affair. Today, we have a different imagery: the specter of Arthur Andersen employees shredding documents while they were on notice of a federal investigation involving Enron. Since that time, Congress enacted the Sarbanes-Oxley Act, which makes it easier for the government to prosecute wrongful document destruction. Judge Scheindlin brought all of this home to us when she advised counsel to “become fully familiar with her client’s document retention policies, as well as the client’s data retention architecture.” *Zubulake V* at 432.

But how do you get familiar with “data retention architecture”? At first blush it sounds painful, but really, the most painful part is learning the lingo and accepting the fact that maybe you don’t know everything.

First, get a copy of your client’s document retention policy, if they have one. It is estimated that only 59 percent of companies have e-mail retention policies. Sue Reisinger, *Electric Company, Corp. Couns.*, October 2005, 100 at p. 104. Review the policy before there is even the faint aroma of litigation, for what it does and does not cover. Pay special attention to electronic data. Most corporate retention policies do not currently address electronic data, and if they do, they do not do so adequately. If there is no ongoing or anticipated litigation, help your client improve upon their document retention policy with an eye toward how it

will affect you during the discovery phase of any future cases.

Second, find out if a litigation hold has been instituted since the policy was written. Interview major stakeholders to see what went right and what went horribly wrong with the implementation of the litigation hold. Were there recalcitrant employees, were there technical difficulties, or were there cost issues? If you have the time and the money, you might try and implement a mock litigation hold and test what the company already has in place. Painful as it may be, in the end it may become a valuable learning tool for exactly how things will happen in a real world scenario.

Third, you will need to sit down with the major business units that may be affected by the litigation hold. Departments like Human Resources, Accounting, Purchasing, departmental managers, or the company executives will need to explain to you how they create data, where they store the data, and how they destroy their data. Make sure they have seen the document retention policy and operate their business unit in accordance with that policy. Often, you will encounter employees who have read and understand the company's document retention policy but whose implementation of that policy at the daily operations level of the company is vastly deficient.

Understanding the data flow, storage devices, and retention issues will give you a running start if the new Federal Rules amendments become effective in December 2006, as anticipated. The Committee Note to the proposed amendment to Rule 26(f) states that it may be important for the parties to discuss their systems and for counsel to become familiar with the systems before the Rule 26 scheduling conference. Taking all of the above steps will allow you to effectively implement a litigation hold.

### Assess Your Data

In a post-*Zubulake* and amended Federal Rules era, we have to assess our data and determine its accessibility. When a party reasonably anticipates litigation, it must issue a litigation hold to ensure the preservation of relevant data. This general rule, as enunciated in *Zubulake IV*, *Zubulake v. UBS Warburg, LLC*, 220 FRD 212 (SD NY 2003), applies only to accessible data. Accessible data is defined as data that is stored in a readily useable format that does not need to be restored or manipulated to be useable. *Zubulake v. UBS Warburg LLC*, 217 FRD 309 (SD NY 2003).

A real-world, albeit paper, example of accessible data would be the trash can, dumpster, and landfill analogy. A piece of paper that is thrown into the office trash can is an accessible data item. Once that trash can is emptied into the office building's dumpster—and becomes commingled with other office waste—it becomes near-line data. Near-line data is data that is between accessible and inaccessible data, but it is definitely recoverable. After the dumpster is emptied into the landfill, it becomes inaccessible data.

In the electronic world, the analogy would flow as follows: an e-mail is read and deleted into the "deleted items" folder. That e-mail is considered on-line and accessible data. If the user copies the e-mail to a CD-ROM for future use, the e-mail becomes near-line data. If that same e-mail remains in the "deleted items" folder overnight and is copied to the nightly disaster recovery backup tape, and is then deleted from the "deleted items" folder, it has become inaccessible data. But take note that data from tapes *can* be considered accessible if corresponding accessible data has been destroyed after notice of the litigation, *or* if the backup tapes are used for purposes other than disaster recovery, *i.e.*, recovery of data from backup tapes occurs regularly.

Sit down with the Information Technology people. First assess whether they have ever seen the document retention policy and what it means to them in their daily lives. Then ask them how they implement and track the policy. Ask them to explain to you, in easy terms that a fifth grader could understand, how information is processed through their system. Send your IT "dude" an e-mail and then have him explain how that particular e-mail flows through the system. Have him show you the servers that e-mail resides on, the backup tapes that it will be copied to, the off site storage area where the tapes are housed in case of disaster.

While the IT person explains this to you, create a flow chart and record how information—both e-mail and electronic documents—flows through the system, and identify all of the storage points. Once the storage points are identified, inquire as to how long the item will reside on that particular tape, server, CD-ROM, etc.

Once you've gone through the tutorial with one or more of the IT people, ask yourself who would be the best witness for the 30(b)(6) deposition. It's usually the person that made the subject matter easiest for you to digest in the initial stages of your IT education.

### Issue and Reissue the Preservation Letter

Even in a pre-*Zubulake* world, we all issued litigation hold letters. More often than not, they were boilerplate letters. Today's litigation hold letter is vastly different.

The litigation hold letter should be specifically tailored to the facts and circumstances of the case. It should educate the data custodian about the records retention policy of the company, the types of data that must be preserved, how it will be preserved, and the ramifications for the failure to preserve. Most importantly, the preservation letter should provide contact information if the data custodian has any questions or requires assistance. More than likely, you will need two points of contact: an attorney contact for the legal and subject-matter issues, and a technical contact to assist with hardware or software issues. The preservation letter should be reissued periodically as the issues or key players in the case change.

## Oversee Compliance and Monitor Efforts

Monitoring the efforts of those actually implementing the litigation hold takes several forms. First, you must educate the masses. You must ensure that the everyday data custodians who are creating and storing data understand what the litigation hold is. It also helps to educate them on the ramifications of their actions for failing to preserve the data, *i.e.*, the company could be sanctioned millions of dollars.

For instance, sit down with the IT person who actually runs the backup tapes. Address any specific labeling issues with them and make sure the label contains enough data that would make a search or restoration of that tape more economical. Make sure they have enough tapes to ensure they won't have to reuse tapes. Often, there is a set amount budgeted for backup tapes and if you cannot recycle tapes for a certain timeframe, this could increase that budget exponentially. Most day-to-day IT people aren't aware of the IT budget, much less how it will be impacted.

Second, follow up. In order to capture day-forward e-mails, we once set up a special mailbox, and whenever a key player had certain key words in their e-mail, a copy was automatically forwarded to the special mailbox. However, this required all of the key players to turn on some Outlook rules. After a month, we ran a report, only to discover that there were some key players who never had any mail sent to the special mailbox.

It turns out that some of them had hardware problems that had required a new install of Outlook; but they forgot to reset their special rules. Had we not followed up with these key players, we would have lost relevant day-forward e-mail.

Often, requiring a person to sign a form stating that they have read, understand, and will comply with the rules of your request to the best of their ability will tend to make them take their role in data preservation a little more seriously. These forms can serve as backup documentation of your good faith effort to enforce the litigation hold.

## Document, Document, Document

Finally, if you have done all of the above, don't let it all go to waste! Remember to document your good faith efforts to implement and monitor the litigation hold. Create trip reports that record who you spoke with, the topics you discussed, and the documents and educational materials that were provided to each key player or data custodian. Finally, make sure to keep all of this data in one centralized location.

In the modern era of litigation holds, counsel's duty to implement and monitor the litigation hold is greater than ever, raising the monetary stakes for failure to adequately implement the hold. It pays to take the time to review the current status of your client's data architecture and records retention policy, and the sooner the better. Once litigation is on your doorstep, take the time to assess, inform, educate, monitor, and document the situation. Although it feels like it will take a lot of time and money up front, in the end, this approach will more than pay for itself.

*Stacy O'Neil Jackson is Corporate Counsel at IE Discovery, a provider of comprehensive discovery management solutions. She can be reached at [sjackson@iediscovery.com](mailto:sjackson@iediscovery.com).*

# CASES

## Orders for 'Pen Registers,' Tracing Devices to ISPs Must Specify Off-Limits Information

Orders to Internet service providers invoking federal authority for "pen registers" and "trap and trace devices" to gather e-mail and web surfing information must clearly indicate what information should be prohibited from disclosure to the government, such as e-mail subject lines, search queries on Google, and application commands, a magistrate judge in the U.S. District Court for the District of Massachusetts held Oct. 25. *In re Application of the United States of America for an Order Authorizing the Use of a Pen Register and Trap on [xxx] Internet Service Account/ User Name [xxxxxxxx@xxx.com]*, Nos. 2005M0499RBC, 2005M0500RBC, 2005M0501RBC, 2005M0502RBC [D Mass, 2005].

The Department of Justice applied for permission to use pen registers and trap and trace devices on four Internet service accounts. The applications sought the Internet Pro-

ocol (IP) addresses, or the unique numerical addresses identifying each computer on the Internet. The ISP would be required to turn over to the government the incoming and outgoing IP addresses used to determine web sites visited from the particular account.

### Produce No More Than Government's Due

"If, indeed, the government is seeking only IP addresses" and nothing more, then there was no problem, Magistrate Judge Robert B. Collings wrote. The trial attorney specific stated that he did not seek the "subject line" contents of any e-mails emanating from, or being sent to, the Internet address. But the form of order he proposed to serve on the ISP was not sufficient to put the provider on adequate notice that such information is not to be disclosed, the court found.

The governing statute, 18 USC §3122(a)(1) permits an attorney for the government to apply for an order approving the installation and use of a pen register or a trap and trace device, provided that the installation of the device is likely to obtain information whose use was relevant to an ongoing criminal investigation.

The problem with using a pen register or trap and trace device on computers is the prohibition against revealing “content,” the court said. The government is not entitled to receive “dialing, routing, addressing or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted,” in the case of a pen register.

In the case of trap and trace devices, the government cannot receive the incoming electronic or other impulses which identify the originating number or other dialing, routing or other impulses which identify the originating number, or any information reasonably likely to identify the source of a wire or electronic communication. “Content” includes any information concerning the substance, purport or meaning of the communication. 18 USC §2510(8).

### **Telephone Numbers Never Disclose Message Content**

The court described “the telephone world” where it was easy to distinguish numbers dialed out and numbers dialed in from the contents of the communications. Even so, there may be problems, the court said. “Suppose, for example, a person first dials a telephone number and then, after being connected, is asked to dial a second number such as a personal account number or social security number or any other identifying number in order to receive further information.”

The court asked if anyone would doubt that the government would be prohibited from obtaining that information on a pen register because it contained the “content” of a communication, even though the action of dialing the second numbers created dialing, routing, addressing or signaling information?

### **‘Contents’ Included E-Mail Headers, Addressees**

In the Internet world, the problem is greater, the court said. With e-mail, the portion of the “header” which revealed the e-mail addresses of the persons to whom the e-mail was sent, from whom the e-mail was sent, and anyone cc’d on the e-mail would certainly be obtainable using a pen register and/or a trap and trace device, the court noted.

There were a number of ISPs receiving these orders, and some of the ISPs might be inexperienced in dealing with these matters, the court said. The court was concerned that the providers “may not be as in tune to the

distinction between ‘dialing, routing, addressing or signaling information’ and ‘content’ as to provide the government only that to which it is entitled, and nothing more.” For example, a user could go to a web site and type in a bank account or credit card number. This would be considered “dialing, routing, addressing and signaling information,” but it is also “contents” of a communication not subject to disclosure to the government under a pen register or trap and trace device order.

The issue of search terms also troubled the court. A pen register would capture that the user visited the Google web site. But if the user entered a search phrase, that search phrase would appear in the URL after the first forward slash, the court said. That would reveal content. Or, in the words of the statute, “information concerning the substance, purport or meaning of that communication.” 18 USC 2510(8).

### **‘Mere Statement’ Insufficient, Listing Required**

Thus, “a mere statement in an order” authorizing the installation of a pen register and/or a trap and trace device that the Internet service provider was to disclose only “dialing, routing, addressing and signaling information” and not to reveal “contents” and in addition not to disclose dialing, routing, addressing and signaling information that contained contents was insufficient notice to the ISP as to what may and may not be disclosed, the court ruled.

“Accordingly, in my judgment, an order to an internet service provider should contain a listing, to the extent possible, of what may NOT be disclosed pursuant to the order.” A violation of the order, including the disclosure of a prohibited information, may be found to be in contempt of court and subject the violator to punishment, the court said. This would ensure that the ISPs configure their software in such a manner so as to disclose only that which has been authorized.

If the order were violated, the ISP could turn to the protection of 18 U.S.C. §3124(e), which provides that a “good faith reliance on a court order under this chapter . . . is a complete defense against any civil or criminal action brought under this chapter or any other law.” The degree of specificity in the order, stating what the ISP may and may not disclose will minimize the unauthorized disclosures, the court said.

The court described the term “contents of communications,” banned from disclosure, as “subject lines, application commands, search queries, requested file names, and file paths.” The recipients of the orders were invited to apply to the court for clarification or guidance, the court said.

John P. McAdams, of the U.S. Department of Justice, Tax Division, Washington, D.C., represented the United States.

### *Ethics and Professional Responsibility*

## Virginia Panel Finds No *Per Se* Prohibition Against Paperless Client Files

Virginia lawyers may maintain a client's file in wholly electronic format, with no paper copies of documents, as long as the client's interests are not prejudiced by this approach, the Virginia state bar's ethics panel has advised (Virginia State Bar Standing Comm. on Legal Ethics, Op. 1818, 9/30/05).

Finding no *per se* ethical prohibition against maintaining paperless client files, the panel concluded that lawyers generally may destroy paper copies of documents if the client consents and may retain only scanned electronic copies, except for items that have independent legal significance such as testamentary documents and marriage certificates.

Subject to the need to preserve such documents, lawyers may even require clients to consent to electronic files as a condition for representation in the first place, the panel advised.

### Paper Chase

The hypothetical situation presented to the committee involved a lawyer who practices administrative law and represents clients before a federal agency. During the course of each representation, the lawyer generates numerous paper documents and exchanges a number of electronic documents with the agency.

The attorney's clients generally prefer for documents to be provided to them in electronic format to help reduce storage costs. In some cases, clients insist on receiving electronic documents only, and the attorney expects that more clients will take that approach.

Accordingly, the lawyer proposes the following procedure:

- scan each paper document into an industry-standard format for which free "reader" software is readily available;
- transmit the electronic document to the client via e-mail; and
- subsequently destroy the paper document.

The inquirer asked whether an attorney must maintain a paper copy of a client's file, whether paper documents in a current client's file may be destroyed once the client consents, and whether an attorney may request such consent as a condition of the representation.

### No *Per Se* Prohibition

The committee advised that lawyers are not obligated to keep paper records in a client's file. The Virginia Rules of Professional Conduct do not dictate the form in which a client's file must be kept, it said

In determining whether a lawyer is meeting his ethical obligations to a particular client, the panel said, "it matters not generally what form the documents in the file take, but instead whether all the documents necessary for the representation are present in the file." There is no *per se* prohibition against electronic files in all instances, it advised.

But the panel cautioned that it may be critical to keep papers such as testamentary documents, marriage certificates, or handwriting exemplars. Also, clients without access to a computer would need for their lawyer to keep a paper file, it pointed out.

The panel cautioned that the preference for electronic storage cannot water down a lawyer's obligations of competence, diligence, and communication. Storage expediency does not trump those duties when deciding what to keep in a client's file and in what form, it made clear.

### Destroying Paper Copies

The panel also advised that in general, a lawyer may destroy a current client's paper documents with the client's consent. "[A]n attorney may ask for the client's consent to destroy the paper documents, retaining only the scanned version, so long as that procedure does not prejudice that client's interests," the opinion states.

The committee recommended that before destroying paper documents, a lawyer review the file to identify documents that have legal significance in their paper form or that may be of continued use or benefit to the client only in paper form.

Before destroying a paper document that was provided to the lawyer by the client, the lawyer should consult with the client and obtain consent, the panel added.

### Advance Consent

Finally, the committee found no blanket prohibition against conditioning representation on a prospective client's consent to an electronic-only file.

But if the destruction of a hard copy of a particular item would prejudice the client, then the lawyer should not insist that the client agree to it, the panel said, citing the directive in Rule 1.3 not to "intentionally prejudice or damage a client."

The full text of Legal Ethics Opinion 1818 is available at <http://ddee.pf.com>.

# TALKING TECH

## Legal Defensibility of E-Signatures Tested in Simulated Trial

By Brian Casey and Pat Hatfield

The law firm of Lord, Bissell & Brook LLP and on-demand electronic-signature firm DocuSign Inc. recently staged a two-hour mock trial to demonstrate the unique issues that challenge electronically signed documents. The event included a summary of applicable e-signature law, a trial demonstration and an expert panel discussion.

The outcome of the trial, heard before Judge Michael A. Yarnell, recently retired from the Maricopa County, Arizona Superior Court, revealed that while the issues may be different, proving an electronically signed document presents no greater risk than proving a paper document signature — if a well-defined e-signing process is in place. Moreover, a company can actually improve its ability to defend or enforce its rights by using an effective e-process.

### Applicable e-Signature Law

The federal Electronic Signatures in Global and National Commerce Act (ESIGN), along with state-adopted versions of the model Uniform Electronic Transactions Act (UETA), establish a foundation for implementing e-signature and e-record processes. ESIGN doesn't preempt state versions of e-signature laws entirely; however, such state laws must be based on a pristine version of the model UETA.

As a result, state laws that are not "pristine" versions of UETA might be preempted in whole or part by ESIGN. With its broad preemption provisions and interplay with UETA, ESIGN provides a basis for developing a national e-signature strategy.

ESIGN doesn't require anyone to use or accept an electronic signature or record, but specifically provides that neither a signature nor e-record can be denied legal effect solely because it is in electronic form. Under ESIGN, an e-signature can be as simple or complex as one of the following:

- Clicking "I Agree;"
- Saying "I agree" into a recording device;
- A digital signature using PKI technology;
- An electronic image captured on a peripheral device;
- Any other way an electronic sound, symbol or process

can be attached to or logically associated with an electronic record that is adopted by a person with the intent to sign.

Although ESIGN specifically exempts certain areas from coverage, exemptions are narrow and ESIGN covers most types of commercial transactions. Under ESIGN, for instance, an archived e-record will satisfy statutory requirements that a contract or other document be retained "in writing," if the

electronic record is maintained in a form that all parties can retrieve later for reference.

ESIGN also recognizes that records of a transaction (whether completed electronically or not) may be archived exclusively electronically, but failure to archive records that can be accurately reproduced could render unenforceable the agreement the electronic record represents and bring about regulatory sanctions for failing to maintain the proper records.

### Proving the Electronic Signature

The mock trial involved an electronically signed auto insurance application and whether or not the plaintiff's now deceased husband had purchased uninsured motorist coverage. The plaintiff, a very sympathetic widow, produced a paper copy of an insurance application that was different from the company's electronic record.

As a result the trial involved a challenge between the widow's paper copy and the company's electronic records. The mock trial included the widow's moving story and the company's testimony detailing its electronic signature process, which was based on the DocuSign web-based e-signature service.

A new process for eMutual, the name of the defendant in the simulated trial, allowed customers to complete insurance applications entirely online without the need to fax, mail, or courier paper documents. Through a Web browser and Internet connection, eMutual customers were able to walk through coverage options, either independently or with the help of an agent, and then make selections to sign contracts online in DocuSign. This service provided a way for signers to create a unique electronic signature based on a number of identifiers including e-mail authentication, secret word authentication, and questions pulled from the customer's credit file.

To sign a document, signers dragged their signature to tagged locations in the document, with every action recorded in an audit trail. The signed document was then locked down and stored in a secure repository.

Electronically signed documents are essentially computer records that courts have long allowed as evidence. Under the Federal Rules of Evidence, and most similar state laws, objections to the admissibility of computer records are typically based on challenges to authenticity of computer records and challenges to computer records under the hearsay rule. Precedent surrounding these types of chal-

lenges has been exhaustively developed. As a result, the mock trial did not focus on admissibility arguments and methods. Most of the testimony was instead directed at how to develop the credibility of the competing documents where the original record was created electronically.

Using encryption and related technologies, an electronically signed document is effectively locked so that subsequent alterations are virtually impossible (tamper-proof) or readily detectable (tamper-sensitive). Key mock-trial testimony centered on the storage of the electronically signed, encrypted, and hashed insurance application within a secure central data repository.

Tom Gonsler of DocuSign, who played the role of expert witness for the defendant, testified a document cannot be modified once it is in the system. "What goes in is locked and can't be changed," he said. "Documents are not 'sent' to anyone, but stored on a DocuSign computer called a server the whole time during the signing process, and merely accessed and viewed for signing. The way the system checks the fingerprint or hash each time, and then can only be displayed if the numbers add up, virtually ensures that the data has not been manipulated or altered after it gets placed in that system."

Moving to cross examination of the defense witness, the plaintiff's attorney explored the possibility of what it would take to make changes to an electronically signed document without detection. In contrast to paper documents which can easily be modified using simple tools such as paper cutters, correction fluid, and copy machines, Gonsler pointed out that cracking an electronic vault is a far more complex process.

"It is technically possible, but the effort required to do it would be impressive," Gonsler said. "DocuSign uses an electronic key to lock the documents. The National Institute of Standards and Technology has estimated that it would take approximately 149 trillion years to break this security key. However, the real challenge would be to also access the DocuSign database in Los Angeles, and break into that system without being detected, find the right file, decrypt the document, which could take years using very powerful computers, then ensure the audit system did not notice the intrusion."

Also critical to system trustworthiness was its ability to collect and record real-time transaction-related data in the mock trial. Systems such as the one described in the mock trial are designed to capture audit-trail data specific to the critical elements of a particular transaction. The audit-trail data included the date and time the late husband signed his electronic auto insurance application and the contents of that document at the precise moment it was electronically signed.

Ultimately, an effective e-signature process incorporates technology and redundant processes that could improve a company's ability to defend and enforce electronically

signed documents. For example, the ability to make a document essentially tamper-proof and tamper-sensitive with common encryption and hashing technologies, and the ability to collect audit-trail data are not available when dealing with paper documents signed in wet ink.

Equally important, however, is how the proponent of the signature uses trial testimony to explain the system and the technology that makes that system secure and the e-signed documents tamper-proof and tamper-sensitive. With effective trial witnesses and testimony that a jury will understand and believe, the benefits of the electronic signature process and its technology have much to offer.

## The Verdict

In the end, Judge Yarnell first found undisputed evidence that the insurance company, eMutual, had made uninsured coverage available to the insured and did so by a written electronic offer, complying with relevant statutory requirements.

From there he determined that "credible, substantial, and persuasive evidence" had been admitted from the electronic systems showing that the plaintiff rejected the offer of uninsured motorist coverage and electronically communicated that rejection to eMutual, and that no credible evidence of corruption, forgery, or alteration of those electronic records had been presented. He also concluded, "The electronic systems of eMutual and third party DocuSign used by the parties in this insurance transaction are secure, redundant, and encrypted."

Although neither party in this case was able to explain the inconsistency between the electronic records and the paper copy of the Uninsured Motorist Selection form, the preponderance of evidence and the credibility of the witnesses led Judge Yarnell to rule in favor of the defendants.

Key pieces of evidence included testimony that the electronic system and processes used by eMutual conformed to E-SIGN legislation and accurately captured the plaintiff's intent. And that eMutual stored the signed contract in a secure repository where it effectively could not be altered in any way.

Given the rapid growth of online commerce activities involving larger and more complex contracts and agreements that normally would require a wet ink signature, it's only a matter of time until a case such as this comes to trial. Careful examination of the technology involved from a legal perspective and effective planning will help ensure a similar outcome.

*Brian Casey and Pat Hatfield practice in the Atlanta office of Lord, Bissell & Brook LLP. They focus a significant portion of their respective practices on e-signature and e-commerce. Reach them at [bcasey@lordbissell.com](mailto:bcasey@lordbissell.com) and [phatfield@lordbissell.com](mailto:phatfield@lordbissell.com).*

# CALENDAR

## DECEMBER

### 8-9

**Twenty-sixth Annual Employment Law Conference.** Washington, D.C. Presented by The National Employment Law Institute. Includes session on discovery in the electronic workplace.

Contact: Telephone: 303-861-5600; web: <http://www.neli.org>; email [neli@neli.org](mailto:neli@neli.org).

### 9-10

**26th Annual Institute on Computer & Internet Law: Information Security, Corporate Governance & In-House Counsel Perspective.** New York City and Live Webcast. Sponsored by the Practising Law Institute.

Contact: Practising Law Institute, 810 Seventh Ave., New York, NY, 10019. Tel: (800) 260-4PLI; Web: <http://www.pli.edu>; fax: 800-321-0093; e-mail: [info@pli.edu](mailto:info@pli.edu).

### 14

**b-Discovery Meeting.** LeBar at The Sofitel, 806 15th Street N.W., Washington, D. C., 6:00 p.m.

Contact: Dan Regard, [dregard@lecg.com](mailto:dregard@lecg.com)

### 15

**b-Discovery Meeting.** Warren's Inn, 307 Travis Street, Houston, Texas.

Contact: Dean Kuhlmann at Cataphora, 830-798-1444, [dean.kuhlmann@cataphora.com](mailto:dean.kuhlmann@cataphora.com)

## JANUARY 2006

### 30-FEBRUARY 1

Legaltech® 25th Anniversary. **New York City. Presented by American Lawyer Media.**

Contact: [http://www.almevents.com/r5/cob\\_page.asp?category\\_id=38991&initial\\_file=cob\\_page-ltech\\_agenda.asp](http://www.almevents.com/r5/cob_page.asp?category_id=38991&initial_file=cob_page-ltech_agenda.asp)

## FEBRUARY

### 9-11

**Evidence Issues and Jury Instructions in Employment Cases.** Washington, D.C. Presented by ALI-ABA at Georgetown University Law Center.

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

### 28-March 1

**E-Discovery: Real World Solutions and Practical Strategies in a Complex and Challenging Environment.** Miami, Fl. Presented by International Quality and Productivity Center. Full day pre-conference workshop on February 27 and full day post conference workshop on March 2.

Contact: <http://www.iqpc.com/na-2398-01>

## MARCH

### 27-28

**E-Discovery Preparedness For the Pharmaceutical Industry: Building Teams, Controlling Costs, and Developing Compliant Retention Strategies.** New York City. Presented by American Conference Institute. Half-day post conference workshop on March 29 – “Implementing Document Management Test-Kits When Choosing a Consulting Firm.”

Contact: <http://www.americanconference.com>

### 27-29

**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: web: <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: web: <http://www.marcusevans.com>

# 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

The screenshot displays the website's layout with a top navigation bar, a central content area with a subscription offer, and a sidebar with search and navigation options. A secondary window shows a detailed article page with a title, date, and introductory text.

**For More Information:**  
**Call:** 800-255-8131, ext 248  
301-562-1530, ext. 248  
**Email:** [customercare@pf.com](mailto:customercare@pf.com)  
**Visit:** <http://ddee.pf.com>

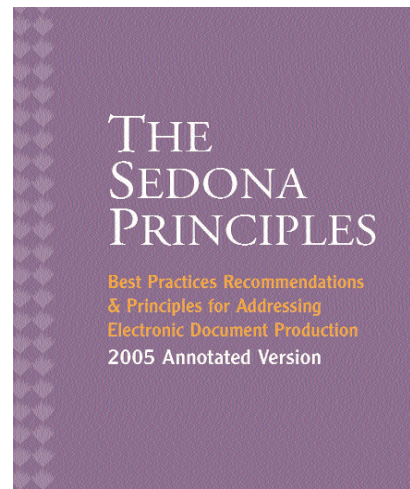


# The Sedona Principles



## 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](mailto: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.



Pike & Fischer is a division of IOMA, Inc - a subsidiary of BNA, Inc. All rights reserved.

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