

# Digital Discovery & e-Evidence

BEST PRACTICES & EVOLVING LAW

Vol. 3, No. 5 | May 2003

## Survey Indicates Short-Term Growth Likely for Electronic Data Discovery Market, Followed by Consolidation

By George Socha and Thomas Gelbmann

In an industry that knows how to keep its secrets, one team is trying to find the answers to one of litigation's persistent questions—what are the size, scope, and growth of the electronic data discovery market?

In early 2003, we conducted a snapshot survey of the EDD market, interviewing over two dozen vendor, law firm, and corporate legal department personnel and scouring online resources. We had three objectives:

1. assess the size of the EDD market as a whole, its growth over the past 10 years, and its potential for future growth;
2. define and describe the major and minor segments of the EDD market and assess their past, present and future; and
3. estimate the market shares of the top five EDD vendors.

This article presents our conclusions and outlines the methodology we used.

### Market Size

Noticeable expansion of the domestic, commercial EDD market began in 1999. Starting at about \$40 million in revenues in 1999, the market grew to approximately \$70 million in 2000 and

then \$150 million in 2001. Total 2002 domestic, commercial market for EDD services was at least \$270 million.

We project that for the next couple of years the market will double annually. The rate of growth probably will begin to decrease soon after 2005, reflecting increased competition, technological and processing improvements, more judicial intervention and more targeted discovery demands, pressure to contain litigation costs, and better electronic records retention practices.

These numbers are both approximations and conservative. For the most part, they do not include services purchased by governmental units or work done by the major accounting firms.

The numbers include figures for do-it-yourself players—law firms and corporate legal departments that have elected to conduct at least some EDD work internally. While this segment is small today, we anticipate that it will grow considerably in the coming years.

### Major and Minor Segments

From our vantage point, the EDD market consists of three main segments—computer forensics/investigative, electronic discovery/litigation support, and consulting. Vendors are

### Inside

- |           |   |
|-----------|---|
| <b>2</b>  | <b>Conference Report I:</b> Panel Offers Practical Solutions to E-Discovery Problems  |
| <b>4</b>  | <b>Reference Document:</b> Plaintiffs' and Underwriter Defendants' Joint Proposed Electronic Data Preservation Protocol   |
| <b>6</b>  | <b>Conference Report II:</b> Web-based Document Review: Trend for Merger, Antitrust Investigations  |
| <b>8</b>  | <b>Litigator's Guide:</b> Best Practices for E-Discovery Motions  |
| <b>10</b> | <b>Cases:</b> Contents of Computer Screen Not Admissible through Testimony • Mississippi Announces Law on Admissibility of Computer Animation • Attorney Must Produce Client's Billing Computer to Grand Jury |
| <b>12</b> | <b>From the Vendor:</b> Applied Discovery Upgrades Online Review Tool   |
| <b>15</b> | <b>In Brief:</b> Electronic Evidence Thought Leadership Winners   |
| <b>16</b> | <b>Calendar</b>   |

flooding into the first two segments, which to date number at least 100. We expect winnowing and consolidation as the market tests vendors' commitment to this arena. We anticipate that a core group of vendors will stay the course and emerge as the dominant players. Some others will disappear, having failed to keep a focus on and commitment to this market and to de-

continued on page 13

# Conference Report

## Panel Offers Practical Solutions to E-Discovery Problems

Communicating with opposing parties, seeking judicial intervention when electronic discovery disputes cannot be resolved by the parties, educating the judge, and always acting reasonably are important strategies in navigating the constantly changing world of electronic evidence issues, according to panelists at an April 1 conference in Washington, D.C.

John Carroll, law school dean and professor at Samford University, Birmingham, Ala., was the keynote speaker at Kroll Ontrack's "Electronic Discovery: Tips, Tactics & Technology" continuing legal education conference. He presented an overview of issues relating to preservation, protection, and spoliation. The concepts introduced by Carroll, a former magistrate judge for the U.S. District Court for the Middle District of Alabama, were then examined in greater detail by The Honorable Shira Ann Scheindlin, U.S. District Judge (S.D. N.Y.); Mary Kay Brown, partner at Philadelphia's Buchanan Ingersoll; senior associate William J. Furnish Jr. from Frilot, Partridge & Clements in Louisi-

ana; and Jonathan Redgrave of Jones Day in Washington, D.C. All agreed that "communication, communication, communication" is the key strategy for attorneys to solve problems relating to e-discovery.

### Obligation to Preserve

Carroll opened the proceedings by describing the obligation to preserve evidence, which has two elements: scope and timing. The scope of the obligation to preserve extends to parties not in ownership or control of evidence and includes "relevant or material evidence," he explained.

Expanding on this comment, Judge Scheindlin observed that retention and destruction are really one policy. The best practice is to adopt a standard document management practice and follow it. William Furnish added that having a policy and not following it is the "worse case scenario."

The process of deciding what data must be captured and preserved should initially be "driven by business needs," explained Jonathan Redgrave, who

moderated the discussion. In the context of preserving documents for litigation, Judge Scheindlin urged the audience to concentrate on what the case is about and its value, particularly when the production of high-ticket items like back-up tapes is at issue. She suggested that the field of discoverable electronic material could be narrowed by defining an appropriate time-frame, conducting key word searches, and identifying the relevant personnel. Mary Kay Brown accomplishes the last objective by obtaining at the outset of litigation a listing of each piece of computer equipment identified by the name of each person who uses it.

As for timing, Carroll said that a party is under the obligation to preserve evidence both during litigation and in anticipation of it.

The "in anticipation of litigation" standard is one of the most difficult to understand, he said, and it includes objective knowledge—when one reasonably should have known of impending litigation—and actual knowledge. Actual knowledge is imputed to

### 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)  
**Legal Editor**, Robert Emeritz ..... 800/255-8131 ext. 258 (remeritz@pf.com)  
**News Editor**, Scott Sleek ..... 800/255-8131 ext. 291 (ssleek@pf.com)  
**Contributing Editor**, Faith Ruderfer ..... 800/255-8131 ext. 288 (fruderfer@pf.com)  
**Group Publisher**, Zachary Wheat ..... 800/255-8131 ext. 229 (zwheat@pf.com)

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

Published monthly, except for August. ISSN: 1537-5099  
Subscription rate: \$549

© Copyright ©2003 Pike & Fischer, Inc. All rights reserved.

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

**Disclaimer:** Pike & Fischer, Inc., has created this publication to provide you with accurate, concise and authoritative information on developments in electronic evidence and discovery. However, the information in this publication should not be interpreted as legal advice, and should not be used as a substitute for advice from an

attorney. Pike & Fischer is not responsible for any claim, liability, or damage related to the use of information in *Digital Discovery & e-Evidence*. Also, the views expressed by outside authors do not necessarily represent the views of Pike & Fischer.

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

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

a party if it has been served a complaint, received a discovery request, received a letter from an attorney regarding impending litigation, or received a protective order in which a court tells it to halt its document destruction policy.

At that point, communicating with the employees most likely to be affected by the document production is crucial. That task is sometimes complicated by the “disconnect” between “tech speech” and legalese, according to Brown. One way to overcome that hurdle is to craft an electronic data preservation protocol, put it in writing, ensure that it is distributed to the people who need to see it, and monitor compliance. She also suggested sending it out under the signatures of both the CEO and legal counsel, to indicate its importance. (The protocol used in *In re IPO Securities Litigation*, 21 MC 92 (SAS) is reproduced beginning on page 4. Judge Scheindlin, who presided over the case, suggested that while this protocol was used in a complex matter, it is “scalable” and therefore useful in smaller cases as well.)

## Sanctions

Carroll also discussed the legal sanctions a court can impose for a party’s failure to adhere to its obligation to preserve, including monetary sanctions, a default judgment or dismissal, exclusion of evidence, and an adverse inference instruction. (For a recent decision addressing rebuttable adverse presumptions, see the sidebar on page 4.)

The sanctions imposed will be designed to “calibrate the scales,” or “make the punishment fit the crime,” he said, based on the party’s degree of fault, the degree of prejudice caused, and the availability of lesser sanctions. Sanctions can be imposed, said Carroll, on a general showing that there was an obligation to preserve, the party had a culpable state of mind, and the de-

## Where e-discovery is concerned, “good lawyering really matters and not everyone is as cognizant of the issues as they should be.”

– John Carroll, Samford University School of Law

stroyed evidence was relevant to a claim or defense.

He said that the state of mind required by courts is usually a standard beyond simple negligence, such as “conscious disregard,” bad faith, or gross negligence. However, Carroll noted that in *Residential Funding Corp. v. DeGeorge Financial Corp.*, 306 F.3d 99 (2d Cir. 2002), the Second Circuit employed a standard of simple negligence in a failure to produce case with unique facts.

Judge Scheindlin added that judges will frequently take into consideration the steps taken by the company to prevent spoliation from occurring.

## Costs

Furnish reminded the audience that the best guidance for allocating the costs of electronic discovery is contained in *Rowe Entertainment, Inc. v. The William Morris Agency*, 2002 WL 63190 (S.D.N.Y. January 16, 2002) and *Murphy Oil USA, Inc. v. Fluor Daniel, Inc.*, 2002 WL 246439 (E.D. La. December 3, 2002), in which he was counsel. These decisions set out and refine the eight-factor cost-shifting test that has been widely adopted. The key to equitable cost allocation, he explained, is to have credible estimates of the anticipated costs available for judicial consideration from the outset.

## Other Matters

The panel also addressed privilege considerations, inadvertent production, and privacy and confidentiality concerns. The presentation closed with a brief discussion of current proposals to standardize e-discovery processes, such as the Sedona Principles (see

*DDEE*, April 2003). Judge Carroll cautioned that while one solution to the problems presented by electronic discovery may lie in amending Federal Rules of Civil Procedure 16 and 26 to force litigating parties to discuss discovery issues early on in the process, making rules changes can take three years on an expedited track. As an alternative he proposed that courts and parties try to make better use of the existing rules. He captured the sense of the entire panel by concluding with the observation that where e-discovery is concerned, “good lawyering really matters and not everyone is as cognizant of the issues as they should be.”

## Invitation to Authors

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

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

## Plaintiffs' and Underwriter Defendants' Joint Proposed Electronic Data Preservation Protocol

1. As used herein, the term "potentially discoverable electronic information" refers to Underwriter Defendants' and Institutional Named Plaintiffs' electronic "documents" that contain or potentially contain information relating to facts at issue in the litigation, where the term "documents" is used as it is defined in Fed. R. Civ. P. 34(a) [footnote omitted].

2. During the pendency of these actions, the Underwriter Defendants and the Institutional Named Plaintiffs shall securely maintain, to the extent that they currently exist and may contain potentially discoverable electronic information: (i) e-mail back-up tapes, and (ii) network back-up tapes (together, the "Back-Up Tapes") created in the ordinary course of business during the period from August 1997 through August 2002 as set forth in the following sentence. The Underwriter Defendants and the Institutional

Named Plaintiffs shall be obligated to retain only one day's Back-Up Tapes among all Back-Up Tapes created in the ordinary course during a given month, provided that such day's Back-Up Tapes represent a complete back-up of the data contained on the subject servers on that day (as opposed to merely an incremental back-up of the subject servers). If only incremental back-up tapes have been retained for a given month, then all such incremental tapes shall be retained. All Back-Up Tapes other than those specifically required to be preserved pursuant to this paragraph and paragraph 3 below may be recycled, overwritten, or erased, as the case may be, pursuant to each Underwriter Defendant's and Institutional Named Plaintiff's otherwise applicable retention schedule.

3. All electronic information or data archived or backed up during the period from August 1997 through August

2002 as part of a special back-up (a back-up made other than in the ordinary course of business by an Underwriter Defendant or Institutional Named Plaintiff), whether due to system upgrade, transition planning, system migration, disaster recovery planning, Y2K testing, or any other reason, that potentially contains potentially discoverable electronic information shall be securely retained, to the extent that they currently exist, for the remainder of the litigation.

4. All current or legacy software and hardware necessary to access, manipulate, print, etc., potentially discoverable electronic information that either is "live" or has been archived or backed up shall be securely retained, to the extent that they currently exist, for the remainder of the litigation.

5. The Underwriter Defendants and the Institutional Named Plaintiffs shall circulate retention notices designed to

### FTC Sanctions Respondent with Adverse Presumptions

The perils of failing to implement a bona fide document retention program are illustrated in a recently released Federal Trade Commission Order (*In the Matter of Rambus, Inc.*, Docket No. 9302, 2/26/03). Rambus, a technology company that designs, patents and licenses computer memory systems, is in a patent dispute with the Joint Electronics Device Engineering Council (JEDEC) arising out of JEDEC's development of standards for two types of Random Access Memory (RAM). JEDEC moved for a default judgment on the grounds that Rambus had destroyed material evidence pursuant to a "sham corporate document retention policy that was ... an intentional wholesale house-cleaning of corporate documents." Rambus countered that its creation of a corporate document retention program was nothing more than the implementation of a prudent business practice begun on the advice of counsel. Any destruction of documents, it argued, was

not a nefarious attempt to destroy evidence in reasonably anticipated litigation but an attempt to avoid needless litigation expenses if it were ever subject to subpoena in an action as a non-party.

Deeming default judgment too harsh a sanction, the administrative law judge nonetheless holds that the undisputed facts of the record require sanctions in the form of certain adverse presumptions against Rambus at trial, based on its spoliation of evidence. The fatal error committed by Rambus was to implement a document retention program that gave employees little guidance on which documents they should keep and which they could purge. Specifically, writes the ALJ in his order, "no instruction was given to Rambus employees to retain documents relevant to future litigation, nor were employees instructed to create and retain an inventory of all documents purged." He further explains that the document retention policy

# Reference Document

ensure the preservation of potentially discoverable electronic and other information to those employees potentially possessing such information. Thereafter, the Underwriter Defendants and the Institutional Named Plaintiffs shall quarterly re-notify their employees of their continuing obligation to preserve such information.

6. The Underwriter Defendants and the Institutional Named Plaintiffs shall take the following measures to secure and retain, to the extent that it exists, the potentially discoverable electronic information that is on the desktop and laptop hard drives of their respective employees. Either: (i) hard drives containing potentially discoverable electronic data shall be retained with all potentially discoverable electronic data contained therein retained intact; or, (ii) employees shall be instructed to copy all potentially discoverable electronic information to a secure, backed-up network storage device or back-up medium for the remainder of the litigation, making all reasonable efforts to retain all meta-data (file creation dates,

modification dates, etc.) associated with the potentially discoverable electronic information at issue. The periodic retention notifications disseminated pursuant to paragraph 5 above shall advise employees potentially possessing potentially discoverable electronic information of their obligation to store discoverable electronic information on a secure, backed-up network storage device or back-up medium to ensure its preservation and instruct such employees in the manner of doing so in accordance with this paragraph.

7. Plaintiffs within 15 days of receiving the list of business units referred to below shall identify by name, title, or departmental category employees of each Underwriter Defendant for which the respective Underwriter Defendant shall be responsible for maintaining the hard drive, or a mirror image copy (*i.e.*, a bit by bit copy) of such hard drive, during the pendency of this litigation. Defendants shall within 15 days of receiving the list of business units referred to below identify by

name, title, or departmental category of employees of Institutional Named Plaintiffs for which the respective Plaintiff shall be responsible for maintaining the hard drive, or a mirror image copy (*i.e.*, a bit by bit copy) of such hard drive, during the pendency of this litigation. In no event shall the number of computers subject to the provisions of this paragraph be greater than 40 for each Underwriter Defendant and 5 for each Institutional Named Plaintiff. The hard drives or image copies of such hard drives preserved pursuant to this paragraph shall be labeled to identify the employee who primarily used the computer associated with that hard drive. In order to facilitate the identification of the appropriate employees, the parties will provide to each other identification by business unit and positions the employees they reasonably believe could have potentially discoverable electronic information. The parties will meet and confer in good faith and exchange additional information as may be necessary to facilitate the identification, and limit the

was drafted by a non-lawyer, whose most detailed instruction was to “look for things to keep” and “look for reasons to keep it.” Moreover, these weak admonishments were “made by a non-attorney to other non-attorneys in a vacuum, without reference to Rambus’s legal obligations to retain documents relevant to reasonably foreseeable litigation.” The ALJ continues, “Given that this virtually unsupervised destruction of documents took place at a time when Rambus knew or should have known of related litigation, I conclude that Rambus’s actions, regardless of its intent, amount to spoliation of evidence. Rambus destroyed or failed to preserve for another’s use evidence in reasonably foreseeable litigation.”

The ALJ observes that current case law does not require a finding of bad faith in the spoliation in order for the need for a remedy to be present; gross negligence is sufficient. Since Rambus’s failure to maintain an inventory of the documents it destroyed

makes it impossible to discern exactly how those documents related to the instant case, some form of sanction is required, in order to place the risk of an erroneous evaluation of the content of the destroyed evidence on Rambus as the party who destroyed it.

That not all JEDEC-related documents were destroyed saves Rambus from a default. Since a sufficient foundational showing was made that Rambus had notice of potential litigation and that the documents destroyed were potentially relevant to that litigation, the ALJ finds the creation of adverse inferences appropriate. The inferences the ALJ creates address Rambus’ knowledge of how its patents would affect the developing JEDEC RAM standards, the effect of its failure to disclose those patents, its knowledge that litigation over the enforcement of its patents was foreseeable, and specifics regarding the inadequacy of the document retention program Rambus adopted.

---

number, of employees for whom the provisions of this paragraph shall be applicable.

8. To the extent that any Underwriter Defendant or Institutional Named Plaintiff has implemented a system for the purpose of preserving external emails (emails sent to or received by a given Underwriter Defendant's or Institutional Named Plaintiff's employees) in an easily accessible form, other than an email server or the Back-Up Tapes identified in paragraph 2 or 3 above, all emails that were created during the period from August 1997 through August 2002, that contain potentially discoverable electronic information, and that are stored on any such system as of the date hereof, shall be preserved during the pendency of this litigation.

9. Within 45 days, each Underwriter Defendant and each Institutional Named Plaintiff will provide written answers to

the best of its ability to the questions concerning information system and electronic document retention practices set forth in attached Schedule C [omitted]. Should any Underwriter Defendant or Institutional Named Plaintiff believe that it cannot in good faith answer any of the questions as posed, the relevant parties will confer to resolve any disputes and, if necessary, seek Court intervention.

10. By agreeing to preserve potentially discoverable electronic information in accordance with the terms hereof, none of the Underwriter Defendants and none of the Institutional Named Plaintiffs are waiving any objection to the ultimate discoverability of such information at such point when discovery is authorized in these actions.

11. Nothing herein shall be deemed to affect the Underwriter Defendants' and Institutional Named Plaintiffs' obligations to preserve hardcopy docu-

ments pursuant to paragraph V of the Court's August 8, 2001 Order. If counsel to an Underwriter Defendant or an Institutional Named Plaintiff learns that potentially discoverable hardcopy documents pertaining to a given public offering were destroyed by such party subsequent to being named as a party in, and receiving a copy of, a complaint pertaining to that public offering, counsel for such party shall notify opposing counsel in writing of such destruction within two weeks of learning so.

12. Nothing herein shall preclude any party from raising with counsel or the Court the limitation or modification of the foregoing in response to particular facts relevant to that party.

13. Nothing herein relieves any other party of its obligations under the Federal Rules of Civil Procedure, the Private Securities Litigation Reform Act, or any other applicable law.

---

## *Conference Report*

---

### **Web-based Document Review: Trend for Merger, Antitrust Investigations**

Web-based review of electronic evidence is a promising methodology for facilitating discovery in merger and antitrust investigations conducted by the Federal Trade Commission and U.S. Department of Justice, a panel of legal experts said at a session of the Kroll Ontrack April 1 conference. During a presentation entitled "Antitrust Best Practices for Electronic Discovery," Scott Scheele, a trial attorney with DOJ's Antitrust Division, said he would not be surprised if web-based document review becomes the trend of the future.

The technique involves using a vendor to put electronic documents on a web site accessible to both the government and the private parties, but with firewalls in place to prevent each side from identifying the documents the other is reviewing. Other speakers agreed that web-based document review is a promising method for easing the burden of document production.

Meanwhile, John Roberti, a staff attorney with the FTC's Bureau of Competition, noted that there is a lot of "noise,"

or extraneous data, sent to government agencies in response to requests for evidence during investigations of proposed corporate mergers. Therefore, government attorneys need to work with the private bar to be more focused and streamlined to enable the more meaningful information to get through.

#### **Document Retention Policies**

Tom Fina, a partner with Howrey Simon Arnold & White's government antitrust practice group, Washington, D.C., agreed with Roberti, saying that information overload results from expanding the scope of information required to be produced to the government. He said it is "absolutely essential" to have a document retention policy in place as a potential remedy for information overload. He urged attorneys to inform their clients that they not only need a document retention policy, they need to enforce it as well.

If firms hold on to documents for five to six years, they are maintaining an enormous amount of information which

they do not necessarily need, Fina said. He suggested that companies get rid of back-up tapes after a few days since they are merely made in case of a disaster such as a fire or computer meltdown. Plus, it is “unbelievably expensive” to sort through back-up tapes in search of specific data.

Fina recommended that companies be proactive about document retention policies rather than waiting until after a bad situation arises, when firms traditionally “get religion” about document retention.

## Metadata

The panelists were careful to point out that there is a difference between producing electronic and hard copies of

documents. Roberti said that with word processor, spreadsheet, e-mail, and Power Point documents, a wealth of metadata resides on electronic files that is not available from hard copies, such as who worked on a document, edits that were made, formulas used, and recipients of documents.

“I think there is a substantial risk of being found not in compliance [with a document request] if all you produce is paper documents,” Roberti said.

Fina, however, expressed some doubts about the production of electronic documents, arguing, for example, that metadata that shows a rough draft of a memo, may not reflect the true opinions or beliefs of the company or the official who wrote it.

## FTC Guidelines for Electronic Document Production

In December 2002, the Federal Trade Commission released formal guidelines for merger investigations, including how best to produce electronic documents responsive to a second request. Specifically, the Commission offered options for acceptable formats for the production of electronic documents and the scope of searches it will request for them.

### Formats

Citing its cost-effectiveness, the Commission is encouraging electronic production, but only in the following formats, subject to the preferences expressed by the staff in each case:

- in a searchable .pdf format, through a third-party web-based document review vendor providing FTC staff with secure and unlimited online web access and unlimited rights and access to download and print electronic documents;
- in a searchable .pdf format on CD-ROM or on an external network appliance such as a “snap server” or large hard drive (generally, this will only be acceptable if the volume of documents is relatively small);

- in an equivalent, searchable format, not including .tiff, produced either through a secured web site, or by CD-ROM or external network appliance (if the volume is not large); or
- in a .tiff format, if accompanied by a Summation document summary file including a variety of more detailed indexing requirements, where each .tiff file represents a separate record in the Summation file, and the .tiff files are at least 300 dpi image quality.

As the Commission becomes more experienced with electronic production and emerging technologies stabilize, it anticipates modifying these options and possibly specifying a single electronic production format as the required production methodology.

### Search Terms

The Commission advises parties to take the following steps to improve the likelihood that a production resulting from a term search will be accepted:

- providing, at the earliest possible time, organizational charts and information on data and document flows and systems so that the staff can evaluate the search methodology;

- providing a glossary of industry and company terminology;
- providing proposed search methodologies (including the applications that will execute the search) and the results of a sample search or searches so staff can evaluate how the search is working;
- submitting a rolling production, so any deficiencies can be detected and corrected;
- in certain cases, agreeing that certain key employees’ files will be physically reviewed in addition to, or in lieu of, being term-searched;
- in certain cases, agreeing to safeguards such as a stipulation to produce any responsive documents not identified in the term search, but identified by other means, before certifying substantial compliance, or a stipulation that documents not identified in the term search will not be used or cited by the parties before the Commission or in litigation.

The Commission also provided guidance for searching archives and back-up systems and e-mail in connection with these investigations. The full text of the December statement is available on the Commission’s web page, [www.ftc.gov](http://www.ftc.gov).

---

Scheele said that he recognized both points and suggested that metadata may make an electronic document a separate document from the hard copy. However, he said such data is helpful in determining who wrote or viewed a particular piece of evidence.

### Rules of Thumb

Scheele suggested three rules of thumb for attorneys trying to negotiate with the government over document production:

- make contact with the agency early on in the process;
- maintain your credibility; and
- involve technical people and vendors as early as possible.

According to Fina, the most critical way to limit the amount of data to be produced is to work with the government to define the individuals within the company from whom documents are going to be needed.

---

## Litigator's Guide

---

### Best Practices for E-Discovery Motions

---

By Carol E. Heckman and Jerauld E. Brydges

---

Several recent decisions dealing with electronic discovery give the practitioner valuable insight into how best to prepare a motion to compel production of documents.<sup>1</sup> Our analysis of these cases suggest the following “best practices” for success in e-discovery motions:

- Make discovery requests pertaining to electronic data as specific as possible; avoid broad-based discovery requests seeking “any and all” e-mail communications for a lengthy time period or among a large group of individuals. A court will be more likely to shift costs of production to the requesting party in the case of such “extremely broad” requests.<sup>2</sup> Consider serving supplemental document requests aimed specifically at electronic data regarding specific subjects during a narrow time period before moving to compel.<sup>3</sup>
- Be prepared in your motion to make a proffer on the likelihood of the production bearing fruit. ““The more likely it is that the backup tape contains information that is relevant to a claim or defense, the fairer it is that the [responding party] search at its own expense.””<sup>4</sup> This makes depositions regarding use of electronic communications medium—i.e., whether certain persons communicated on particular subjects via e-mail, and the extent to which such communications were deleted—all the more important.<sup>5</sup> Where the likelihood of uncovering relevant information is marginal, cost shifting is more likely. This may require an expert affidavit attesting to the likelihood of re-

covering, as an initial matter, *any* information at all from back-up or deleted files. Obviously, specific examples of misconduct, such as backdated or altered documents, or documents destroyed after requests to retain records, should be brought up if available.

- Exhaust all avenues of obtaining the information from other sources. Doing so will militate in favor of placing the expense of production on the producing party.
- In the case of back-up or emergency tapes, “deleted” data that the producing party has simply neglected to fully discard, or other data not maintained for an ongoing business purpose, courts will be more likely to shift the costs of production to the requesting party. “Just as a party would not be required to sort through its trash to resurrect discarded paper documents, so it should not be obligated to pay the costs of retrieving deleted e-mails.”<sup>6</sup> If, however, the practitioner presents evidence that the producing party routinely searches its back-up tapes or has a means for doing so, the court may be less inclined to shift costs.<sup>7</sup>
- Present the court, if possible, with a benefit to the producing party from the production. If there is either a business or evidentiary value to the producing party that will result from the search and production of the electronic data, cost shifting is less likely.
- Present expert testimony setting forth a protocol that would keep the costs of the producing party at a minimum. Don’t allow the court to be swayed by the producing party’s argument regarding costs; present evidence of your own.<sup>8</sup> A sound understanding of the nature of your opponent’s computer system is important.

- Present your client as the financial underdog, if at all possible. The party who is better able to bear the costs of production will likely be ordered to do so.

## A Protocol for Privilege and Confidentiality

Another major issue to consider in moving to compel are the concerns the producing party will raise regarding privilege and confidentiality issues. Very often the party seeking electronic discovery is asking the court for direct access to the computer system of the respondent, which may lead to the disclosure of irrelevant but commercially sensitive information or material protected by the attorney/client or other privileges. In response to these concerns, the moving party should consider requesting that the court institute some variation of the protocol first set forth by the district court in *Playboy Enterprises v. Terri Welles*.<sup>9</sup>

In *Playboy*, the Court, after granting the plaintiff's motion to compel access to the defendant's hard drive to attempt to uncover deleted e-mails, set forth the following protocol to address defendant's concerns regarding confidential and privileged material on the hard drive.<sup>10</sup>

First, the court would appoint a computer expert to create a "mirror image" of defendant's hard drive, and directed the parties to meet and confer on the designation of the expert. The designated (or court-appointed, if the parties failed to agree) expert would serve as an officer of the court; therefore, her access to possibly privileged material of the defendant's could not be construed as a waiver of defendant's attorney/client privilege.<sup>11</sup> The expert also would be required to sign a protective order.<sup>12</sup>

Second, the computer expert would create the "mirror image" of the producing party's computer that would be given to defendant's counsel, who would print and review any recovered documents, produce to plaintiff any responsive communications, and record any documents withheld on the basis of privilege on a privilege log.<sup>13</sup>

Finally, defense counsel would be charged with maintaining the mirror image for the duration of the litigation. Counsel and the expert also would be required to submit to the court a report on the success of retrieving all or part of the total data on the disk.<sup>14</sup>

Other courts have instituted more refined variations on this protocol that provide, for example, that the expert need not copy the operating systems and higher level programs of the computer, that the expert (rather than counsel for the producing party) would be custodian of the mirror image, and that the expert would destroy the mirror image at the conclusion of the litigation.<sup>15</sup> The court also may direct that it receive a copy of the mirror image in order to resolve later

disputes about documents withheld by the producing party on the basis of privilege.<sup>16</sup>

## Endnotes

<sup>1</sup> See, e.g., *Byers v. Illinois State Police*, 2002 U.S. Dist. LEXIS 9861 (N.D. Ill. May 31, 2002); *Rowe Entertainment, Inc. v. The William Morris Agency, Inc.*, 2002 U.S. 8308 (S.D.N.Y. May 9, 2002); *Murphy Oil USA, Inc. v. Fluor Daniel*, 2002 U.S. Dist. LEXIS 3196 (E.D. La. Feb. 19, 2002).

<sup>2</sup> *Rowe*, 2002 U.S. Dist. LEXIS 8308, at \*14.

<sup>3</sup> *Murphy Oil*, 2002 U.S. Dist. LEXIS 3196, at \*13; cf. *Byers*, 2002 U.S. Dist. LEXIS 9861, at \*38 (shifting costs to requesting parties where they sought archived e-mails "from every day for the last eight years.").

<sup>4</sup> *Rowe*, 2002 U.S. Dist. LEXIS 8308, at \*16 (quoting *McPeck v. Ashcroft*, 202 F.R.D. 31, 34 (D.D.C. 2001)).

<sup>5</sup> *Id.* at \*16-17 ("no witness has testified about any e-mail communications that allegedly reflect discriminatory or anti-competitive practices.").

<sup>6</sup> *Id.* at \*23.

<sup>7</sup> *Murphy Oil*, 2002 U.S. Dist. LEXIS 3196, at \*16.

<sup>8</sup> "In the absence of any evidence from [the requesting party], the undersigned must accept [the producing party's] estimate of the cost. Its magnitude clearly favors shifting the cost to [the requesting party]." *Murphy Oil*, 2002 U.S. Dist. LEXIS 3196, at \*17.

<sup>9</sup> 60 F. Supp. 2d 1050 (S.D. Cal. 1999).

<sup>10</sup> The protocol would take effect only upon submission by the requesting party of an affidavit from a computer expert showing that "recovering some deleted e-mail is just as likely as not recovering any deleted e-mail, and that no damage will result to [the producing party's] computer." *Id.* at 1055.

<sup>11</sup> *Id.* at 1055.

<sup>12</sup> *Id.*

<sup>13</sup> *Id.*

<sup>14</sup> *Id.*

<sup>15</sup> *Simon Property Group L.P. v. mySimon, Inc.*, 194 F.R.D. 639, 641 (S.D. Ind. 2000).

<sup>16</sup> *Antioch v. Scrapbook Borders*, 210 F.R.D. 645, 654 (D. Minn. 2002).

---

*Carol E. Heckman and Jerould E. Brydges are attorneys with Harter, Secrest & Emery in Buffalo, N.Y. This article is an excerpt from their paper "Winning Electronic Discovery Motions," published by The Sedona Conference in connection with its recently concluded program Complex Litigation V: Electronic Discovery & Technology in the Courtroom.*

## Business Records Exception

### Contents of Computer Screen Not Admissible through Testimony

**Baber v. Commonwealth of Virginia**, 2003 WL 1810510 (Va. App., decided April 8 2003)

The testimony of two retail employees that a computer display indicated that no sales of merchandise of the type that was suspected of being shoplifted were made on the day of the alleged theft was inadmissible hearsay, according to a recent Virginia Court of Appeals ruling. Since the trial court's admission of the testimony was harmless error, however, the defendant's conviction of grand larceny is upheld.

The defendant purchased a \$9.99 tool box from a Sears store, then attached the receipt for the toolbox on a \$630 generator he hadn't paid for, in the hopes that the attached receipt would enable him to leave the store with the generator without raising suspicions. Two alert store employees queried the defendant as he attempted to make his departure, however. Not accepting the defendant's story about misplaced receipts, the employees entered the generator's inventory control number into a central computer; at trial, they testified that the computer screen showed that no generators had been sold that day. No hard copy of the information displayed on the computer was ever produced.

The appeals court ruled that the trial court erred when it admitted into evidence the employees' testimony concerning the information displayed on the computer screen. In finding the evidence to be hearsay, the court relied heavily on *Tatum v. Commonwealth*, 17 Va. App. 585, 440 S.E. 2d 133 (1994), which distinguishes between evidence based on "computer generated information" (which is not hearsay), and "the [simple] repetition of prior recorded human input or observation" (which is hearsay). The court concludes, "the evidence in this case proved ... that the information displayed on the computer screen was in part a function of data entered into the system by various sales associates. Thus, we hold that the testimony of both witnesses was merely a recitation of information shown by the computer's display of inventory data, which was based on input by various individuals. This evidence constitutes hearsay unless within a recognized exception."

The court then applied the traditional business records exception to the hearsay rule as set forth in *Kettler & Scott, Inc. v. Earth Tech. Cos., Inc.*, 249 Va. 450, 449 S.E. 2d 782 (1994), to determine the admissibility of the hearsay. *Kettler* made clear that "admission of such evidence is conditioned ... on proof that *the document* comes from the proper custodian and that it is *a record kept* in the ordinary course of

business made contemporaneously with the event by person having the duty to keep a true record." (Emphasis in opinion.) The court reminds us that business *records* are admitted as an exception to the hearsay rule because they are regularly prepared and have a guarantee of trustworthiness and reliability. In this case, however, no written document was at issue. Although the computerized inventory tracking system has the capability of producing a printed document, the Commonwealth produced neither a printout of the computer screen data or an actual record. Instead, the employees merely recited the information they said they observed on the computer screen. In short, the Commonwealth sought to rely on the memory of its witnesses to deliver the contents of the records. The court concludes that this evidence "does not establish that the trustworthiness and reliability of the evidence can be sustained through a recitation of the witnesses' observation of the displayed data." It therefore holds the defense's hearsay objections should have been sustained. Since there was sufficient evidence of the defendant's guilt without the disputed computer information, however, the court affirms the conviction.

## Demonstrative e-Evidence

### Law on Admissibility of Computer Animation Announced

**Cox v. Mississippi**, 2003 WL 1091065 (Miss. Sup., decided 3/13/03)

The Mississippi Supreme Court used the appeal of a convicted murderer as an opportunity to announce the law pertaining to computer animations and demonstrative evidence, making clear that the principles articulated in its decision will be applied prospectively in both criminal and civil cases.

#### The Case Below

Robert Cox was convicted of the murder of his wife's long-time lover, whose body was found beside his car, along with a 12-gauge pump shotgun. The top of the victim's head had been blown off.

At trial, Cox advanced the theory that the victim's death was not the result of murder, but suicide. A computer-generated animation created by Cox's expert witness was used to assist the expert in explaining how the victim's alleged suicide could have occurred. Although Cox argued that the animation was used only as demonstrative evidence, i.e., to help the expert explain his testimony, it was admitted as an exhibit and included in the evidence that was given to the jury to consider during its deliberations.

## The State's Assignment of Error

The state in its cross-appeal claimed the trial court erred both in admitting the animation into evidence and allowing the jury to take it into the jury room. The Mississippi Supreme Court agrees, but finds that both errors were harmless.

At trial, the expert had testified that since no measurements were made at the death scene, the animation was based on his study of the case, including pictures, investigative reports, the weapon, the crime scene, the vehicles, etc. In response to the state's suppression motion, the court ordered Cox to "provide full and complete disclosure of any and all underlying data and scientific principles relating to 'utilized computer analysis, enhancements and animation' of the proposed suicide video. The disclosure by the defendant must include but is not limited to the mathematics, physics, programming, hardware or software and any supporting documentation or studies used to create or support the animation."

The only additional information Cox supplied in response to the order was the name of a person who purportedly assisted the expert in the generation of the animation. The state argued that the response was deficient because it failed to outline the specific, scientific data including measurements which were used to create the animation; it listed various software programs without accompanying explanation of their application; and it failed to describe the hardware utilized. The state also cited as objectionable the absence of any testimony at trial as to the software or hardware actually used to make the animation or the specific mathematical data used to manufacture the video animation prior to it being shown to the jury. The state relied on the testimony of an FBI Visual Information Specialist Examiner who testified that because of current technologies in computer animation, it was possible to create an animation showing literally anything as "real," when it was not based on any facts. The examiner concluded, "[A]ny computer animation which was not based on actual, physical measurements from the crime scene was mere speculation." The Mississippi Supreme Court agrees.

## The Holding

The court adopts the following holdings of several other jurisdictions to support the ruling that to be admissible, an animation must be based on scientific, identifiable, and objective facts:

- The foundation for admission of a computer-generated animation must include specific physical measurements from the scene and testimony as to what software, process and data were used.

- A computer-generated animation is admissible as demonstrative evidence when the proponent shows that the animation is authentic, relevant, a fair and accurate representation of the evidence to which it relates; and its probative value substantially outweighs the danger of unfair prejudice, confusing the issues, or misleading the jury.

- To be admissible, a computer-generated animation must be relevant and fair and accurate, and its probative value must outweigh its prejudicial effect.

The court concludes that while demonstrative evidence is admissible if it is necessary and relevant to a fact at issue, evidence which is admitted for demonstrative purposes only (as opposed to substantive evidence which is evidence offered for the truth of the matter asserted) *should not* be given to the jury for its consideration during deliberations. Accordingly, it agrees with the state's assignments of error. The court finds those errors to be harmless, in light of the jury's returning a guilty verdict.

## Privilege

## Attorney Must Produce Client's Billing Computer to Grand Jury

**In re Original Grand Jury Investigation re Subpoena Duces Tecum Served upon Mark A. Kaiser**, 2003 WL 1721058 (Ohio App. 3 Dist., decided April 2, 2003)

An attorney is required to comply with a subpoena duces tecum by producing for a grand jury the billing computer of his client, a physician, who was the subject of an ongoing criminal and administrative investigation for Worker's Compensation fraud, drug trafficking, and prescription offenses. The attorney, who was never the target of the grand jury investigation himself, obtained the computer from an office manager in the employ of the client's brother, who was also a doctor. The Ohio Court of Appeals was asked to review an order denying the attorney's motion to quash the subpoena and holding him in contempt for not complying with it.

The court first finds that the attorney failed to carry his burden of showing the unreasonableness or oppressiveness of the subpoena. The attorney claimed that while he had no knowledge of the specific content of the computer records at issue, they had no relevance to the grand jury investigation. However, he also acknowledged that the records "may" contain billing information. The court interprets that acknowledgement to mean that the information contained on the computer could conceivably be relevant to the investigation, particularly in light of the broad scope of

# Cases

---

a grand jury's investigatory powers. The subpoena therefore was neither unreasonable nor oppressive.

The court also rejected the attorney's assertion that compliance would be tantamount to violating the disciplinary rule prohibiting a lawyer from knowingly revealing a client confidence or secret. The court acknowledged that the computer records constitute a client secret by virtue of their having come into the attorney's possession through his professional relationship with the doctor and because their disclosure could be potentially embarrassing or detrimental to him. The court explains, however, that the ban against disclosing client secrets is subject to four exceptions. The relevant exception requires disclosure "in the context of mandating that attorneys relinquish evidence and instrumentalities of crime to law enforcement agencies." The court concluded that since the com-

puter records and other physical evidence sought in the case may contain evidence of a possible crime, they must be turned over to the grand jury.

The attorney argued unsuccessfully that his compliance with the subpoena would violate the work product doctrine, which protects from discovery documents and tangible things prepared in anticipation of litigation. The court finds that privilege inapplicable because the attorney "put forth no effort to produce the information contained on the computer."

The attorney's Fifth Amendment assertion was also unsuccessful. The computer not only didn't belong to the attorney, he had denied that it contained evidence that would incriminate him. The court therefore finds that the attorney's request for Fifth Amendment protection is without merit, in light of his not having been called to testify against himself in a criminal matter or to offer up his own personal papers and effects.

## From the Vendor

---

### Applied Discovery Upgrades Online Review Tool

Applied Discovery, Inc., a Seattle-based provider of electronic discovery services, announced April 28 that enhancements to its Online Review application are now available. The changes include faster document-to-document review times, advanced document marking and numbering features, and new options for printing and preparing document sets for production, according to a statement from the company.

The new release makes improvements in the following areas:

- **Speed** — System architecture upgrades provide the ability to advance from document to document in an average of one second, greatly improving reviewer productivity.
- **Document Numbering and Marking** — Advanced document numbering and marking features enable users to create, manage, and apply document marks or numbers (including Bates numbers or marks such as "confidential") to any set of documents in the database at any time during the review process. A simple interface enables users to apply as many as seven different marks on 18 different locations on each page. Users may also choose formatting options for each brand, including font style, size, and color. Once applied, Bates numbers become part of each document's searchable meta data within the database, providing an additional way to pinpoint key documents quickly and accurately.

- **Printing and Pre-Production** — With enhanced printing options, users can easily print large batches of documents. The user will now be able to:

*Print to a local or network printer* — Users can print sets of documents to local or network printers. This feature makes it faster and easier to review documents prior to depositions; print important documents for review at client meetings; preview a sample of Bates numbers or other document brands prior to production; or actually print an entire document collection to produce to a requesting party.

*Save files to disk* — Rather than printing documents on paper, users may utilize the print interface to save batches of documents to any network drive. They may then view documents while disconnected from the network; export documents to an in-house case management system; send the documents to a third party for printing; or prepare documents for electronic delivery to another party.

Mark Chealander, vice president of development at Applied Discovery, said, "Speed and project control are vital to the success of any electronic discovery project. With these new capabilities, our clients can manage electronic document productions more effectively than ever." He added that the new enhancements are provided at no additional charge.

For further information, contact Virginia Llewellyn, telephone 425-467-3021, e-mail [virginia.llewellyn@applieddiscovery.com](mailto:virginia.llewellyn@applieddiscovery.com), or consult the company web page at <http://www.applieddiscovery.com/>.

continued from page 1

velop and pursue viable long-term strategies.

Within the computer forensics segment, we identified five emerging sub-segments: data identification, data collection, data restoration, data conversion, and data culling and filtering. Within the electronic discovery segment, we identified four sub-segments: data hosting, filtering and searching, data analysis, and search software. We did not observe that same focus on consulting. Consulting and efforts to develop standards are parts of the EDD market that are underserved.

## Market Shares of Top Five Vendors

No single vendor dominates the market; only a handful command quick recognition. According to our survey results, the top five market leaders were (in alphabetical order) Applied Discovery, Daticon, Electronic Evidence Discovery (EED), Fios, and Kroll Ontrack. With market shares ranging from just under 10 percent to slightly less than five percent, they accounted for 32 percent of the market.

Among the next 10 vendors there was much compression, with little effective differentiation between the vendors and the services they offer. Beyond that, no vendor appears to have developed much name recognition.

## Methodology

### *Defining the Scope of the Market*

We included only activities connected to materials that were “born electronic,” i.e., materials that started out and stayed in electronic form until they entered the EDD pipeline. We confined our study to EDD activities within the United States. We looked only at EDD vendors who catered primarily to the commercial market; consequently, EDD activities associated with governmental work and vendors who cater to that market are not in this study. Finally, we used 1993 as a chronological starting point.

### *Getting Information from Secondary Sources*

We gathered information from such secondary sources as vendor web sites, published results of earlier surveys, white papers, listings of corporate legal departments, large law firms and major litigation departments, and reports on judicial caseloads.

### *Conducting the Survey*

We considered 74 EDD services and software vendors for inclusion in our survey and interviewed 14. We selected 15 law firms to include in the survey and interviewed personnel from seven. We sought interviews with 11 corporate legal departments and conducted interviews of five. Each of the telephone interviews lasted between 30 minutes and one and a half hours.

## Analysis

We defined three major segments and then sub-segments within them (*see tables 1, 2, and 3*).

We created a set of six factors that formed the foundation of our evaluation of the information we had gathered. The factors, weights and explanations are set forth in table 4.

Within the main factors, we created a second level of factors. To these factors and sub-factors we assigned the questions whose responses we wanted to use for analysis and synthesis. We gave each of those questions a relative weight. The combined weight of questions within each sub-factor added up to 100 percent. The combined weight of questions within a factor added up to 100 percent. And, of course, the combined weight of all the questions within all the factors added up to 100 percent.

## Synthesis

### *Composite Rankings*

After defining factors and weighting questions, we rated the results for 15 vendors. We combined the rating and weighting information to come up with composite numbers, which ranged from 3.7 to 7.2 (*see table 5*).

The composite numbers’ relative differences mattered most, not their absolute values. Of interest is the steadily descending slope from numbers 1 to 6, the compression from numbers 6 to 11, and then the sharp drop after that.

### *Comparing the Top EDD Vendors*

We compared the top five vendors using our six main factors: experience/reputation, capacity, computer forensics/investigative, electronic discovery/litigation support, consulting, and revenue. Of note was the variation—or lack of it—between vendors. The high-low ranges are recorded on table 6.

Extending the comparison down to the top eight vendors exposed some trends. Although the vendors’ capabilities (capacity, computer forensics/investigative, and electronic discovery/litigation support) were almost identical in the aggregate, their presence in the market (experience/reputation) and revenue were not. The top three vendors enjoyed both the greatest presence and the largest revenues. Numbers four and five dropped off, and the remaining three vendors had numbers that were about half those of the leader.

## Market Perceptions

We asked interviewees to identify the top five EDD vendors and explain the reasons for their choices. Some interviewees provided numbered lists, others grouped ven-

dors into tiers, yet others were unwilling to hazard any guesses. In responding, different interviewees focused on different criteria. Nonetheless, several criteria seemed to emerge on a regular basis. Among these, the most important seemed to be size, reputation, quality, and quantity and complexity of work undertaken.

Among the vendors we interviewed, four names dominated the lists; among the law firms, the first three names stood out. All four of those vendors were in our top five.

## Conclusion

As far as we know, this is the first study into the size, scope and growth of the EDD market where the authors of the study have been in a position to disclose the results. We hope that as we move forward, we will expand this study to include a larger group of vendors and respondents. We also hope to pursue related studies in areas such as the factors that drive up and push down demand for EDD services, EDD vendor best practices, EDD consumer best practices, and the development and deployment of EDD standards.

*George Socha is an attorney and consultant whose newly-formed business, Socha Consulting LLC, helps inform digital discovery decisions. He can be reached at 651-690-1739 or [george@sochaconsulting.com](mailto:george@sochaconsulting.com).*

*Tom Gelbmann is an independent management consultant who has helped lawyers realize lasting value from information technology for over 16 years. He can be reached at Gelbmann & Associates at 651-483-0022 or [tom@gelbmann.biz](mailto:tom@gelbmann.biz).*

Table 1	
Computer Forensics/Investigative	
Data identification	Identifying what data should be pursued in discovery.
Data collection	Actual collection of data from various sources & media.
Data restoration	Restoring collected data for evaluation and processing.
Data conversion	Converting restored data to desired media & formats.
Culling / filtering	Culling: Reducing amount of data before processing. Filtering: Examining subsets of data after processing.

Table 2	
Electronic Discovery/Litigation Support	
Data hosting / web	Hosting services of access to discovery data, including on-line hosting.
Filtering / search	Examining subsets of data; search, retrieval & display.
Data analysis	Working the legal team to discern significant patterns & located relevant documents.
Search software	Software provided to client for use in electronic discovery; litigation support.

Table 3	
Consulting	
Consulting	Advice on retention & discovery approaches.

Table 4		
Factor	Weight	Explanation
Experience/	20%	Length and depth of/ reputation experience in the industry; reputation among customers and competitors.
Capacity	10%	Resources dedicated to the EDD market, such as facilities, people, and services.
Computer forensics/ investigative	30%	Breadth and depth of services dedicated to forensic and electronic investigation.
Electronic discovery/ litigation	20%	Breadth and depth of services supported dedicated to conversion to more useable formats and to search, retrieval and analysis capabilities.
Consulting	5%	Advice on retention and discovery approaches.
Revenue	15%	Estimated annual revenues.

Table 5			
Vendor Rank	Composite No.	Vendor Rank	Composite No.
1	7.2	8	5.5
2	6.9	9	5.4
3	6.5	10	5.4
4	6.1	11	5.3
5	5.8	12	4.9
6	5.6	13	4.0
7	5.5	14	3.7

Table 6		
Factor	High	Low
Experience/reputation	1.5	1.0
Capacity	.07	.05
Computer forensics/investigative	2.1	1.9
Electronic discovery/litigation support	1.3	1.1
Consulting	0.4	0.2
Revenue	1.4	0.8

## In Brief

### Electronic Evidence Thought Leadership Winners

The first Electronic Evidence Thought Leadership Awards were presented on April 1 in Washington, D.C. The awards recognize law firms, corporations, government entities and/or individuals in several categories based on their recent and significant contributions to the development of the body of law, practice and procedure in the area of electronic evidence. Kroll Ontrack Inc., a wholly-owned subsidiary of Kroll Inc. (Nasdaq: KROL), made the presentations.

The recipients of the inaugural Electronic Evidence Thought Leadership Awards are:

- *The E-Evidence Thought Leading Law Firm Award:* Jones Day, for the creation of its e-Discovery Committee and for the pioneering work of the committee in the area of legal scholarship on e-evidence topics. The award was accepted by Jonathan M. Redgrave, partner with the firm's Washington, D.C. office and member of the firm's e-Discovery Committee.
- *The E-Evidence Thought Leading Litigator Award:* Julia Guttman, Esq., a partner in the Washington, D.C. office of Baker Botts, LLP, for her integration of e-evidence issues into her litigation case strategies.
- *The E-Evidence Thought Leading Antitrust Practitioner Award:* Michael L. Keeley, Esq., an associate with the New York office of Axinn, Veltrop & Harkrider, LLP, for the firm's innovative use of technology in the context of regulatory compliance matters.
- *The E-Evidence Thought Leading Litigation Support Award:* Tom Powers, with the New York office of

Kaye Scholer, LLP, for his early adoption of e-evidence technology.

- *The E-Evidence Thought Leading Scholar Award:* Kenneth J. Withers, Research Associate with the Federal Judicial Center in Washington, D.C., for his authorship of a myriad of thoughtful articles and delivery of many insightful presentations on e-evidence topics worldwide. Mr. Withers was also recognized for his extensive efforts in educating the federal bench on all e-evidence related topics.

- *The Thought Leading Electronic Discovery Case of the Year Award:* *Murphy Oil USA, Inc. v. Fluor Daniel, Inc.* for its significance towards the evolution of the body of case law relating to e-evidence protocols. The award was presented to the plaintiff's attorney, William J. Furnish Jr., Senior Associate with Frilot, Partridge, Kohnke, & Clements, L.C., who accepted the award on behalf of the entire *Murphy Oil* litigation team.

### Proving Plagiarism

The discharge of a university researcher terminated for having committed plagiarism and academic fraud has been upheld by the Ohio Court of Appeals. The court was persuaded that the university had grounds to dismiss the researcher by evidence comprising a computer identification of 64 instances in which the researcher's manuscript included verbatim "word strings," consisting of at least 10 or more consecutive words identical to word strings in the thesis authored by an academic at a Canadian university some seven years earlier. *Matikas v. University of Dayton*, 2003 WL 1857130 (Ohio App. 2 Dist, decided 4/11/03).

# Calendar

---

## ■ MAY

6-8

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

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

7

**Document Management and Automation for the Federal Enterprise: Improving Performance Through Innovative Business Practices (Session 2).** Arlington, Va. Presented by Market\*Access International, as part of its Market\*Access Government Best Practices Series(tm).

**Contact:** tel: 703-807-2748; Web: <http://www.marketaccess.org>

8-9

**Collecting and Producing Electronic Evidence in Cyber-crime Cases.** Faculty of Law of the University of Namur (Belgium). Funded by the European Commission Community Research Fifth Framework Programme. Organized by Centre de Recherche Informatique et Droit.

**Contact:** Veronica Perez ([Veronica.perez@fundp.ac.be](mailto:Veronica.perez@fundp.ac.be))

8-9

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

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

## ■ JULY

10

**Fraud Litigation Conference.** New York City. Presented by the Foundation for Accounting Education.

**Contact:** tel: 800-537-3635; Web: <http://www.nysscpa.org/faeconferences.htm>

## ■ SEPTEMBER

17

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

**Contact:** tel: 703-807-2748

25-26

**2003 BNA Litigation Forum: Electronic Discovery and Records Management.** Washington, D.C. Presented by Pike & Fischer, Inc. for the Bureau of National Affairs, Inc. Key-note presentation by Magistrate Judge John Facciola, U.S. District Court for the District of Columbia.

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

---

## Digital Discovery & e-Evidence Order Form

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

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

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

Payment Options:     Visa     MasterCard     American Express     Bill me     Payment enclosed  
Card Number \_\_\_\_\_ Expiration Date \_\_\_\_\_  
Authorized Signature \_\_\_\_\_  
(Please note: Your credit card statement will show a charge from Pike & Fischer, Inc., publisher of DDEE.)

Name \_\_\_\_\_ Organization \_\_\_\_\_  
Address \_\_\_\_\_ City \_\_\_\_\_ State \_\_\_\_\_  
ZIP Code \_\_\_\_\_ Telephone \_\_\_\_\_ E-Mail \_\_\_\_\_

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