Published by Pike & Fischer, Inc., a subsidiary of The Bureau of National Affairs, Inc.

Digital Discovery & e-Evidence

BEST PRACTICES & EVOLVING LAW

Reprinted from Vol. 2, No. 7 | **July 2002**

Challenges and Opportunities of Digital Discovery

Wendy R. Leibowitz

The digital day has dawned: Virtually all business activities are now computerized, and e-mail traffic has surpassed telephone and postal service communications. Indeed, according to a study by the University of California at Berkeley, cited by Kenneth J. Withers, a Research Associate at the Federal Judicial Center in Washington, D.C., 93 percent of all information generated in 1999 was originally generated in digital form, and might never be transferred to paper. Withers spoke at a forum on May 21 at the Georgetown University Law Center entitled, "E-Discovery: Getting Wired for 21st Century Litigation." Addressing technical issues and e-discovery battles was former FBI special agent John McElhatton, who is now the director of digital services at the James Mintz Group. Daniel Prywes, litigation partner at Pepper Hamilton, served as moderator.

Special Issues with Electronic Information

An electronic document can be copied and stored in literally hundreds of places, emphasized Withers, from e-mail attachments to automatic back-ups through home laptops. Frequently, the data is not indexed or organized. Electronic files may contain irrelevant and sometimes embarrassing information, and dealing with the computerized mountains of electronic documents is the new frontier of discovery. It often requires experts to handle the information, analyze it, and, if matters proceed to trial, testify about it.

The costs of retrieving the information are yet another characteristic distinguishing electronic from traditional paper discovery. Even so, the review of the documents may be more cursory, warned Withers: if there are seven million e-mails to be reviewed, for how many seconds will each one be scrutinized? Lawyers could live in constant fear that privileged information will be inadvertently turned over to opposing counsel.

The special issues posed by the storage and retrieval of electronic information, said Withers, are still being analyzed by the courts. "We are living in a world where many litigators don't know how to use e-evidence, or how to use it as a battering ram," he said.

Withers, who will be issuing his findings on electronic discovery case study research in October 2002, painted a picture of the landscape of electronic discovery quite distinct from paper-based discovery processes. Electronic discovery involves much more involvement by experts, with all the issues they pose—is there such a thing as a neutral expert, and who should pay for these experts?—and for more direct supervision by judges. Ironically, said Withers, the daunting nature of digital discovery issues may produce a more peaceful pre-trial process as the parties are forced to negotiate their way through these issues.

Six Moments in Electronic Discovery Battles

John McElhatton is a computer-forensics expert with the James Mintz Group, an investigative firm headquartered in Washington, D.C. He served as an FBI special agent for 27 years, and was a founding member of the FBI's Computer Analysis Response Team.

McElhatton, who frequently assists litigators with electronic discovery projects, characterized the following as the "six crucial moments" in electronic discovery battles:

1. Before the next battle begins: Record-keeping and business document maintenance is haphazard at best. "E-mail is a mess," said McElhatton. Once litigation has started, it is too late to set up orderly processes involving the creation, storage, maintenance, and destruction of electronic records. Companies and their law firms must be aware of the need for a good document retention policy, and must implement and enforce the policy. One way to formulate such a policy, said McElhatton, is to think of litigation: "What will I have to produce if I'm sued, where is it, and how can I find it?"

It is not enough to simply destroy e-mail after 30 days or so, cautioned McElhatton, and to call that a "retention" policy. Important e-mails and other electronic documents must be preserved. One of the most frequent errors he sees in his work is the inadvertent overwriting of data during the ordinary course of business. He called it "trampling evidence." It is prudent to preserve and isolate important business data, he said. He pointed to the Arthur Andersen "document shredding" policies regarding Enron files as a good

example of an office whose destruction of such files cast doubt on their integrity and that of their oil company client.

2. At the outset of litigation: The most important consideration at this point is protection of the potential evidence from any processing which will call its integrity into question, said McElhatton. Data on computers is very volatile, and it is easy for even trained technicians to trample the data.

If you are requesting data, it is important that your demands be as specific as possible to "quarantine" the data you need. If you are producing data, it is incumbent upon you to protect the data as securely as possible, consistent with maintaining the business. Key technical personnel, such as the system administrator, should be interviewed to understand the network topology, back-up, storage, and deletion procedures.

McElhatton referred to a company with strict e-mail deletion policies on the books. But an interview with technical employees who were supposed to carry out the policies revealed that they deleted nothing, but simply kept everything.

3. When finalizing the responsive product: The focus should be on ensuring that privileged and proprietary data is not produced. Ideally, the final production should be burned onto a CD to allow those with institutional knowledge, as well as counsel, to review the documents easily. Counsel, together with a technical expert, should ensure that no information is inadvertently produced, such as "embedded" data that contains previous drafts of the document. Similarly, filter out duplicative, non-responsive, irrelevant, and, of course, privileged material.

4. When addressing objections by opposing parties: If opposing counsel objects to electronic evidence, do not offer to provide a paper printout or images that have been scanned into digital form, said McElhatton. Printouts will not suffice since digital data contains much more information than can be printed. Digitally-based data can also be much more easily transported, copied, and searched. Develop a general strategy for production to try to minimize the "undue burden" and "too broad scope" objections, he said.

> "All conclusions about the gathered evidence must be backed not only by the basis for your expert's opinion, but also on confidence that the tools and methods are tested, reliable, and proven. To put it another way, both the product and the process have to be authenticated."
>
> **—John McElhatton**

Such a strategy would include:

- a full understanding of the opposing parties' computer system and personnel, to argue the feasibility of obtaining and producing information;
- an offer to provide an on-site inspection and/or data acquisition without disrupting business;
- an offer to provide automated methods for retrieving and reviewing data, such as key-word searches within a narrow time frame;
- eliminating duplicate data and/or
- concentrating on specific users.

5. After production of data: It is important to have a specific objective in mind when examining the data, emphasized McElhatton. Make sure whoever is examining the data will be able to recognize a "smoking gun," as well as data that could provide leads or corroborate other parts of the investigation.

When dealing with electronic evidence, it's not just the content of the evidence, but the history of the document. User activity could be significant in and of itself, if it departs from someone's normal or expected activity, (i.e., logging on at an odd hour, or moving or deleting files). Internet activity—sites visited, time of day, and duration—might be useful.

Make sure all data is examined, said McElhatton, including "meta-data"—the names, paths, and key dates associated with the document. "Most file types have unique signatures that can be discerned through analysis," he said. They include creation and modification dates and author data. E-mail has routing information, links to attachments, threads, and responses.

6. At trial: "The overriding issue at this stage is authentication of the offered evidence being introduced," McElhatton. "All conclusions about the gathered evidence must be backed not only by the basis for your expert's opinion, but also on confidence that the tools and methods are tested, reliable, and proven. To put it another way, both the product and the process have to be authenticated." Both the process and the product are subject to scrutiny and cross-examination, he emphasized.

Prepare the expert witness to be questioned. It is appropriate for parties to ask questions about credentials, for example, and to probe every step an expert took. And don't be surprised at any ignorance by people in the judicial system, he concluded. Things go more smoothly when everyone is educated, and all technical terms explained, as the expert testifies.