SPECIAL FOCUS:

Computer

CONTENTS

Forensics

If there were one brief definition of the work that forensic accountants do, it may be this: looking beyond the numbers and seeing situations as they really are.

Grasping the truth of the matter is vital to lawyers as they weigh and value their cases. More so than ever before, that truth can be obscured by the sheer complexity of new technologies. But despite that—or perhaps because of it—courts demand more and more in the way of transparency and disclosure, in discovery and beyond.

This month, we feature two articles that address the issues that many lawyers deal with daily. Called forensic accounting or computer forensics, this is an area that requires skill and an attorney's full attention.

BY CRAIG REINMUTH

Being Proactive With Electronic Discovery

Computers and the Internet have forever changed how business is conducted. Congress recognized this years ago and made appropriate changes to the Federal Rules of Civil Procedure. Effective Dec. 1, 2006, attorneys are now responsible for the following:

- Understanding their clients' computer systems
- Assuring back-up procedures are in place to preserve electronic data
- Determining what e-data are potentially "relevant" to the litigation, and
- Collaborating with opposing counsel on e-discovery issues

Based on major court rulings to date, failure to comply can result in:

- Their clients' being held responsible, by the court, to pay to have it done correctly
- Exposing their clients to sanctions
- Counsel not pursuing all the information needed to properly represent their clients' positions
- A drastic reduction in the odds of winning the case, and
- Potentially subjecting themselves to professional sanctions or loss of their license to practice

Committee notes indicate Rule 34(a) is amended to confirm that discovery of electronically stored information stands on equal footing with discovery of paper documents. States, including Arizona,[1] are taking steps to incorporate the federal procedural rule changes regarding electronic discovery into their statutes.

Even before changes to Federal Rules of Civil Procedures became effective, the courts' awareness of the importance of electronic discovery was evident. In *Coleman v. Morgan Stanley*,[2] a $1.5 billion judgment was awarded primarily tied to sanctions for failing to preserve and produce e-mails requested to be produced back in 2003.

Computer forensics is the process of using science and technology tools to discover all the responsive data that may exist on relevant computers and other storage media, and then to retrieve the information in a fashion that can be supported by a chain of custody and authenticity grounds. There is some comfort to be had, though, in the knowledge that, among all the other hats lawyers need to wear, the "computer geek" hat is not one of them. As summarized in Table 1, a qualified expert in computer forensics can provide you with assistance in each stage of the litigation process as it relates to electronic discovery.

Stage 1: Strategizing

Rule 26(f) was amended to direct the parties to discuss discovery of electronically stored information during their discovery-planning process. The parties are to discuss any issues relating to *preserving discoverable information and disclosure* of *electronically stored information*, *including the form* or *forms in which it should be produced*. Wise counsel will try to work together, as early as possible.

Counsel for Plaintiff

If you are representing the plaintiff, you are entitled to all electronic information that may be responsive to the litigation. It is estimated that 85 percent to 90 percent of information entered into a computer is never printed out. Therefore, it is imperative that you consider and request the appropriate electronic data that may support their claims or positions.

A properly experienced computer

Craig Reinmuth, CPA, MST, is President and Director of Economic Insights (EI), a litigation support firm based in Scottsdale. He specializes in investigative accounting and computer forensics and has strong expert witness experience in the areas of commercial litigation, family law and fraud/embezzlement cases. He serves as an active member of the BV/LS Services Steering Committee of the Arizona Society of CPAs. He has 30 years of experience in public and corporate accounting including Senior Tax Manager with PriceWaterhouse Coopers and senior financial management positions with Mercedes-Benz of North America.

forensics expert (hereinafter referred to as "expert") can brainstorm together with you and the client as to where all potentially relevant e-data may reside, including the number and location of server/routers, laptops, portable handheld devices, thumb drives, and so forth. The expert can also advise you as to the different forms that e-data can take, including e-mails, instant messaging, temporary files, calendar/to-do lists, Web searches, system logs, Internet history, photos and print files.

The expert can assist in determining if data wiping or encryption utilities might have been used (an area in which sophisticated techniques continue to be developed, even by Microsoft).

Counsel for Defendant

If you are representing the defendant, failure to address preservation issues early in the litigation increases uncertainty and raises the risk of disputes further into the litigation. You need to take action to ensure steps are in place to preserve the data. The expert can sit together with your client and their IT personnel to discuss how to maintain files during litigation.

As stated previously, counsel must understand their clients' computer systems. In order for you to discuss the defendant's information systems relevant to the case, individuals knowledgeable in computer technology can be very helpful, if not mandated. A comprehensive list of recommended actions that counsel should take to preserve electronic data is contained in *Zubulake v. UBS Warburg LLC (V)*.[3]

TABLE 1

Computer Forensics Assistance in Each Stage of Litigation Process

Case Strategy	Discovery	Analysis	Testimony
• Provide assistance throughout litigation process	• Rule 26(f) planning meetings	• Best Way to analyze mass amounts of data	• Reports
• May be only way to obtain needed evidence	• Discovery without vs. with computer forensics	• Key word/date searches	• Integrity of data
• Identify electronic evidence sources	• Types of electronic evidence to request	• E-mails	• Vulnerability assessment
• Balance privacy with evidence production	• Is data accessible?	• Internet access	• Opposing expert cross-examination
• Interrogatory assistance	• Secure collection & preservation	• Evidence tampering	• Presentation of evidence
• Data preservation	• Providing only "relevant" data	• Restoration of deleted files	• Prior experience/ reputation
• Cost - Benefit	• Deposition of opposing expert	• Hidden transactions	
		• Reduce time and costs	

The expert can assist in balancing privacy with evidence production by providing electronic discovery on behalf of their clients, including redacting (filtering out) proprietary data and producing e-data with "metadata" intact (required). IT professionals employed by your client may need to be informed by another technical person as to what the legal requirements of "preservation" entails.

Even before e-data is requested, it is recommended that you independently review the electronic data with your client to determine the extent to which you are being told everything you need to know and/or to avoid at a later date. An expert can do this (e.g., image a hard drive and search the drive for information critical to the case). If this is done, however, it may be wise to not have the expert be a testifying witness.

Discussions concerning privileged and work product protection must also take place in order to protect your client's interests and avoid any assertions that there has been a waiver of privilege.

Stage 2: Discovery

The expert can attend Rule 26(f) meetings, suggest information to request with respect to backup procedures (whether it is done in-house or by outside operators), provide assistance with wording for inter-

rogatories and/or requests for production of electronic evidence, and potential deposition questions for IT personnel.

Once the parties have an agreement in principle as to the parameters of electronic discovery that is to be provided, the form of production then becomes an issue. The responding party must produce the information in a form in which it is ordinarily maintained or in a form that is reasonably usable. Will it be provided in its "native" form, paper, or electronic form? How will the documents be "bates-stamped" for ready reference by both sides and the court. In anticipation of the increased need for compliance with electronic data requests, a new market of providers has surfaced to service this need.

Certain information is likely to be available only via e-data. Table 2 provides an indication of evidence obtainable with and without consideration of electronic data sources.

TABLE 2

Evidence Attainable

WITHOUT	WITH
• Word processing/ spreadsheet documents	• Altered? And when? Perform file signature analysis
• Third-party subpoena	• Whom to subpoena?
• E-mail	• E-mail history; deletions
• Business, at-home computers	• Password recovery
• Printout from Internet site	• Internet history; Web searches
• Awareness of deleted or altered document	• Specific files deleted and when; Potential recovery
• Photos they're proud of	• Photos they're not so proud of
• Purported hard drive "crash" during litigation	• For real? If so, was it intentional? Potential recovery of data
• Who knows what evil lurks?	• What the other party is truly knowledgeable of

Computer Forensics

For example, even if you are successful in securing a key paper document, you cannot be assured that it has not been altered prior to it coming to you, unless you have the ability to review the record electronically. You get a stack of e-mails to review, but can you be assured you have received all e-mails relevant to the case? If information obtained or viewed on the Internet is relevant to the case, how will you know where and how often the suspect has "surfed" on the Internet? How can you be assured files have not been deleted? And if they have been deleted, are they fully or partially recoverable? Backup copies may also be available on the user's system or network.

"Metadata" must also be provided in connection with a response to a request for e-data. Metadata is "data about the data." This includes dates the computer data was created, modified and/or deleted. The expert can research and determine when and if any of these dates have been altered.

Special Master

The expert can also assist in the production of e-data relevant to a case in the role of a special master, wherein the expert acts on behalf of court. The expert can help parties understand the scope and nature of electronic data collection, filter out privileged data and assist in determining the extent to which the data is "reasonably accessible" and how much it might cost to produce it.

"Reasonably accessible" information. Rule 26(b)(2) provides, "A party need not provide discovery of electronically stored information from sources the party identifies as not 'reasonably accessible' due to undue burden or cost." The burden of proof is on the party obligated to disclose, and the court may specify conditions for the discovery. An expert can assist in evaluating claims as to whether data is or is not "reasonably accessible," as was evidenced in the *Morgan Stanley* case.

Exceptions to sanctions for not providing e-discovery. Due to the very nature of e-data, Rule 37(f) has been added: "Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good faith operations of an electronic information system."

This is understandable in light of the routine alteration and overwriting of e-information often without the operator's specific direction, or awareness of routine backup techniques.

The expert can assist in determining whether the steps taken were in the spirit of the exception to sanctions under Rule 37(f).

Stage 3: Analysis

A single hard drive can contain 100 million pages of text, or 50,000 boxes of paper documents. Although statistics like these relative to electronic data can be overwhelming at first, the review of documents, electronically, is the most efficient manner to analyze mass amounts of data. For example, searches can be performed for key words, documents or dates important to the litigation.

→

In addition, there may be no other way to obtain the evidence specifically needed on a case. Examples of this include evidence tampering, data deletion and Internet access.

Will compliance with the new rules for electronic discovery increase the costs of litigation? Most likely it will. However, experience has shown that it can also reduce the time and costs associated with obtaining discovery. Sometimes the mere threat of electronic discovery causes cases to settle. Cases have also been shortened once certain documents begin to surface early in the review of electronic data and the guilty party realizes the power of computer forensics, does not want any further probing, and therefore requests settlement discussions.

Stage 4: Testimony

Venturing into the world of electronic discovery can be extremely technical. Once the case reaches the point where the expert must provide testimony with respect to electronic evidence, the expert will need to do so in an understandable ("non-techy") manner. They must have skills and experience to explain technical concepts and present mass amounts of data in a clear and understandable manner.

To the greatest extent possible, you will want the expert to demonstrate that the electronic evidence has been securely collected and preserved, has not been altered or tampered with, and its integrity has been maintained. This is commonly done through the use of "hash values" to verify the information the expert is testifying to is the same information that was on the computer when the expert obtained it (e.g. image of a hard drive or server). Only a few software programs have been tested and approved by various courts to be "forensically sound" and reliable. When selecting an expert, make sure you question them regarding the software they utilize as well as other accepted procedures in the profession, including documenting the chain of custody of electronic data and their overall ability to testify and demonstrate that the procedures they employed are forensically sound.

The expert needs to also be knowledgeable of ethics guiding their profession and case law governing their expert testimony. Their experience and reputation must also be well founded and be able to withstand cross-examination. This includes significant prior testimony experience. The expert can also assist you in developing questions for an opposing expert (deposition, cross-examination, etc.) in computer forensics.

Other Considerations

In summary, one issue is clear. When you come across cases where information contained on a computer may be relevant to the case (and this will be the rule rather than the exception for nearly all types of litigation), you need to be proactive with the use of computer forensics. The alternative is to risk not obtaining the proper settlement or verdict for your clients.

endnotes

1. Petition to amend Rules 16, 26, 26.1, 33, 34, 37 and 45 was filed Nov. 1, 2006. The deadline for comments was May 21, 2007. The matter is on the Arizona Supreme Court Rules Agenda for Aug. 27, 2007.
2. 2005 WL 679071 and 2005 WL 674885 (Fla. Cir. Ct. Mar. 1, 2005).
3. *Zubulake v. UBS Warburg LLC (Zubulake V)*, 2004 WL 1620866 (S.D.N.Y. July 20, 2004).