

Nashville Bar Journal

March 2006 - VOL 6, NO. 2



“The Times They Are A ‘Changin’” Computer Forensics and the Revised Federal Rules of Civil Procedure

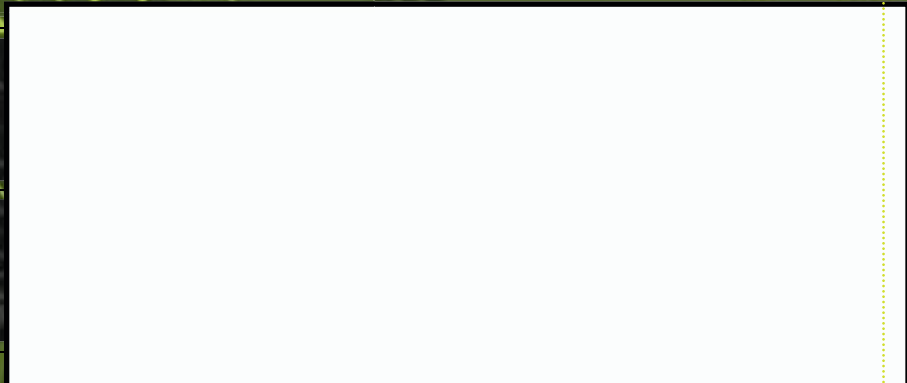
Kaz Kikkawa, Phillip Hampton & Stan Mitchell

**Electronic Filing in the United States District
Court for the Middle District of Tennessee**

Keith Throckmorton
United States District Court, Middle District of Tennessee

**The Napier-Looby Bar Association—
Moving From A Rich Past To A Relevant Future**

Rita Roberts-Turner
Metropolitan Government's Department of Law





“The Times They Are A ‘Changin’”

Computer Forensics and the Revised Federal Rules of Civil Procedure

by: Kaz Kikkawa, Phillip Hampton and Stan Mitchell

Under the current versions of Rules 26 and 34 of both the Federal and Tennessee Rules of Civil Procedure, the term “documents” includes “data compilations” to make it clear that the Rules apply to electronic data compilations.¹ Until recently, however, federal and state courts have applied paper document rules and logic to the discovery of electronic information. In this era of proliferating electronic information, the paper document analogy is no longer viable. The newly proposed amendments to the Federal Rules of Civil Procedure are changing the way electronic information is to be discovered to reflect the changes in the technology of electronic information.

The addition of the phrase “electronically stored information” highlights a sea change in the way discovery is defined and will be handled under the soon-to-be-adopted amendments to the Federal Rules of Civil

Procedure. These amendments, which were drafted to deal specifically with issues relating to the discovery of electronic data, are expected to go into effect on December 1, 2006 pending approval by the U.S. Supreme Court and Congress. Many legal pundits tout these FRCP changes as the proverbial “paradigm shift” in the practice of discovery. Certainly, the proliferation of computer technology and electronically stored information in business and in personal life has already significantly changed the legal landscape. These FRCP amendments now codify and clarify practices for requesting, producing, and resolving disputes regarding electronic data. More importantly, these amendments underscore the fact that electronic discovery is an issue that cannot be ignored by legal practitioners. Its impact must be understood and carefully measured in litigation.²

“The times they are a ‘changin’” — and it is time they did.

Summary of FRCP Amendments

The key phrase “electronically stored information” was added to Rules 26(a), 33, and 34 to clarify and embrace all forms of electronic data that are subject to disclosure and discovery. The amendments also codify and clarify electronic discovery “best practices” such as including arrangements for electronic discovery in the court’s scheduling order and modifying the meet and confer process to include e-discovery planning. Additional changes include establishing: guidelines for electronic data production, rules governing the format and costs of production, and procedures for addressing inadvertent production of work product data. Finally, the amendments create a “safe harbor” for electronic discovery that distinguishes between what may be viewed as spoliation and what may be viewed as loss of data through the routine, good-faith operation of an electronic information system.³

Issues relative to electronic discovery will have to be addressed at the outset of almost every lawsuit. As a result, attorneys should have a basic understanding of the nature of electronic data, the unique requirements for disclosure and production, the potential pitfalls for clients and attorneys, and the new sources of data that may be crucial to a case.

Computer Forensics in Litigation

Computer forensics is the branch of computer science that deals with the retrieval and analysis of data from electronic storage systems in a manner that does not alter or compromise the integrity of the target systems. Computer forensics began in the mid-1980s as a response to demands from the law enforcement community, in particular the FBI, in investigating computer related crimes. In this age of ever-expanding electronic communication, however, almost every case has, or soon will have, a computer

forensics component. Lawyers now must be aware of these issues and know how to deal with them.

Don’t get us wrong, complying with the new federal rules does not require attorneys to be experts in the field of computer forensics. However, an informed awareness of computer forensic technology will prove beneficial in the process of navigating the sometimes treacherous and ever-changing terrain of electronic discovery.

Concomitant with the increase of electronically stored information in civil litigation over the past 10-15 years, private sector computer forensic labs and specialists have emerged to assist parties with the acquisition, preservations, production, and analysis of computerized data.

Planning for Electronic Discovery

The first step to take at the outset of an actual (or potential) legal dispute is to consider all possible sources of electronic evidence. The results can be staggering. Evidence can be lurking in many places...on a computer hard drive, network server, backup tape, CDROM, DVDROM, external hard drive, flash drive, PDA, smart phone, digital camera, mp3 player, voicemail system, printer, fax machine, copier, email system, or internet site. The proposed federal rules make it clear that all sources of electronic information are subject to disclosure requirements. Attorneys must understand the scope of what is considered “electronic data” and be able to inform their clients of their disclosure requirements.

The proposed rules require electronic discovery planning early in the discovery process. Under the new provisions, parties should include discussions related

to electronic discovery in their initial case management conference. Topics to be covered include preservation of electronic data and a discussion of a discovery plan to address issues of privilege, work product protection, and the format of production.

Proposed Rule 34(b) addresses the format of production of electronic information. The amendment will allow the requesting party to designate the desired format in which electronic is to be produced. There are provisions in the rule to resolve disputes if the responding party objects to the format request. The bottom line is that requesting parties may seek to receive electronic data in a format that is most conducive to their efforts to search and locate relevant information. Most often this desired format will be an electronic version of the data, not printed paper. Production in an electronic format is sometimes more efficient and cost-effective as well, making it difficult to object to this format of production. Finally, production of data in electronic format can yield more information about the data than a printed copy of the same data. Certain types of information, such as the date a document was created, the date it was last modified, or the last person to edit the document, can only be ascertained when the information is produced in electronic format.

One of the reasons that electronically stored information is so valuable in the discovery process is because there is a wealth of additional information that can be derived from it as opposed to paper production. A computer forensic examination of a computer hard drive can reveal much more information than simply a listing of all the files that exist on the hard drive. Some additional information that can be revealed by a

Continued on Page 16 ➔

computer forensic examination include:

- What files were deleted from the computer?
- Did someone try to hide information, and if so, can that data be recovered?
- What applications were most recently used on the hard drive?
- Were the documents found on the hard drive created there originally or copied there?
- Has the user employed any type of "wiping" software to delete information in such a way that it cannot be recovered?
- Can email messages be authenticated or proved to be forgeries?
- What internet sites were frequented by the user of the hard drive?
- Are there evidence trails in hidden areas of the hard drive, such as file slack, which the user may not even be aware are being stored?
- What was last printed from the hard drive?
- Is there evidence that date and time stamps on certain documents may be forged?
- Is there evidence of the user accessing files on other drives, such as network mounted file systems or external storage devices?

Preservation and Reasonable Accessibility

The duty to preserve relevant data takes on new meaning when dealing with electronically stored information. Electronic data can be extremely volatile. It may be altered or destroyed simply through the normal use of a computer. In many cases, a forensic image of the electronic media in question is necessary to properly preserve electronic evidence. There is a difference between "backing up" a computer hard drive and forensically imaging the drive. A computer forensic image captures much more information from the hard drive than a traditional "back up" procedure does.

One of the more controversial changes in the Federal Rules is the amendment to Rule 26(b)(2). This proposed amendment establishes a two-tier approach to electronic discovery. It seeks to differentiate between what is "reasonably accessible" electronic information and what is not. Under this provision a responding party must produce electronic information from sources that are "reasonably accessible." However, if the responding party can show that responsive information from certain electronic sources cannot be extracted without incurring substantial burden or cost, the party may not be required to produce it. The issue of reasonable accessibility promises to be a major point of contention between litigants. With modern computer storage systems and increasingly advanced computer forensic tools, accessing and extracting responsive data from even large data pools is becoming more and more feasible, both logistically and economically. The second tier of this amendment will probably be applied more to data stored on out-dated computer media or proprietary computer systems, the retrieval of which might be exceedingly difficult and expensive. Even if a responding party seeks protection from producing electronic under the second tier provision of this rule, the court may still order production for "good cause" shown.

A computer forensic examination very likely meets the reasonable accessibility test of the two-tier discovery standard in 26(b)(2). Indeed, the proposed amendments to Rule 34(b) specifically permit litigants to serve requests not only to "produce" or "inspect" their opponent's electronic information but also to "test or sample" that electronically stored information. A trained computer forensic professional need only image the target hard drive in a forensically sound method in order to conduct such an examination. When issuing or responding to requests for preservation and/or production of electronic data, attorneys

should be aware of the value in utilizing computer forensic methods in this process.

Safe Harbor and Spoliation

Another controversial proposed amendment is the "safe harbor" provision in Rule 37(f). This amendment states that "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 operation of an electronic information system." The rule recognizes the dynamic nature of electronic information and how non-malicious destruction of electronic information often occurs as a normal part of operating an electronic information system. It is important to note that the "safe harbor" provision does not apply when a party violates a preservation order or if the party does not take reasonable steps to preserve data after it knew or should have known that the data would be discoverable in an impending action. As such, destruction of data, even inadvertently through the routine use of computer systems, may be sanctioned if it does not fall within the scope of this safe harbor provision.

Spoliation is a major concern when dealing with electronic evidence. Your adversary need only show that electronic evidence was mishandled in order to invalidate key pieces of evidence that may have been found from an electronic information source. One of the cardinal sins of computer forensic examination is searching and analyzing data on original computer media, in other words, booting up a target computer to see what is on it. The very first step of any computer forensic examination is to make an exact bit stream image of the target hard drive. This process must be undertaken in a sterile computing environment where there is absolutely no possibility of any data being written to the target media. Commercial off-the-shelf backup software applications typically are not sufficient to make a bit stream image of a hard drive in this manner.

After creating an image of the target hard drive, all subsequent search, analysis, and data retrieval should be done from the hard drive image, not the original. This examination of the media in this fashion will not alter the hard drive image in any way. Attorneys should advise their clients that the services of a computer forensic examiner may be required to properly preserve data subject to discovery, and that access by in-house information technology personnel—if done improperly—may result in spoliation claims.

Conclusion

The proposed amendments to the Federal Rules of Civil Procedure (and one must assume that the Tennessee Rules will not be

far behind) illustrate how discovery of electronic information is becoming more commonplace. Now more than ever, attorneys need to know how to properly identify, preserve and produce electronically stored information. Attorneys must be aware of the unique nature of electronic discovery and be prepared to utilize new resources to comply with the proposed federal rules and, more importantly, to represent their clients properly. Computer forensics, while once relegated to the high-tech labs of the FBI and CIA, will soon be an everyday tool in the arsenal of every lawyer who hangs out a shingle. ■

Kaz Kikkawa is an attorney with the law firm of Constangy, Brooks & Smith, LLC. He is a former Chair of the Nashville Bar Association's Labor and Employment Law Committee and currently serves as the Co-Chair of the Nashville Bar's Continuing Legal Education Committee. Phillip Hampton and Stan Mitchell are both with LogicForce Consulting, LLC and will be conducting a CLE seminar with Kaz later this month on the topic of Computer Forensics.

(Footnotes)

¹ Fed R. Civ. P. 26 advisory committee note (revising definition of documents "to accord with changing technology").

² On September 20, 2005, the Judicial Conference of the United States approved a package of amendments to the Federal Rules of Civil Procedure addressing a number of electronic discovery issues. The complete text of the proposed rules, with the official Committee Notes, and a discussion of the comments received during the public comment period is available online as a PDF file. *Summary of the Report of the Judicial Conference Committee on Rules of Practice and Procedure*, <http://www.uscourts.gov/rules/Reports/ST09-2005.pdf> (Sept. 2005). This PDF file is also accessible through the Federal Judicial Center website at http://www.fjc.gov/public/home.nsf/autoframe?openform&url_r=pages/196.

³ *Summary of the Report of the Judicial Conference Committee on Rules of Practice and Procedure*, *supra* note 1, at 85.

CLEALERT

Computer Forensics CLE
March 16, 2006

See CLE PAGE 3 for details



AMERICAN
LEGAL SEARCH
Where Lawyers Look for Lawyers®

As Nashville's premier legal recruiting firm, the most respected and prestigious law firms often come to us *first* to locate top attorneys. We always have positions for attorneys with strong academic credentials and practice experience. If you are such an attorney, please make AMERICAN your *first* call, too! Here are just a few of the current opportunities for the next big step in your career:

Nashville

Corporate Real Estate Associate, 2-4 years experience
ERISA Associate, 2-4 years experience
IP Litigation Associate, 1-5 years experience
Corporate & Securities Associate, 2-4 years experience
Healthcare Associate, 2-4 years experience

Louisville

Health Care Associate, 3-6 Years Experience
Corporate Associate, 1-5 Years Experience
Trust & Estates Associate, 2-4 Years Experience
Immigration Associate, 2-4 Years Experience

Strong academic credentials required for all positions. All inquiries are strictly confidential.

Contact: Jim Intermaggio, Esq. at jim@americanlegalsearch.com or call (615) 515-5051.

www.AmericanLegalSearch.com

Atlanta Birmingham Louisville Miami Nashville New York Los Angeles San Francisco Washington DC