

How Will the 2006 FRCP Changes Affect You?

by Gregory Fordham

The 2006 changes to the Federal Rules of Civil Procedure were effective Dec. 1, 2006. For those well versed with digital evidence, the changes will probably have little effect. On the other hand, those who are not yet skilled in cyber litigation are at risk from their enemies as well as the fulfillment of their own wishes.

As Judge Francis concluded in *Rowe Entertainment v The William Morris Agency, Inc.* (205 F.R.D. 421), “Too often, discovery is not just about uncovering the truth, but also about how much of the truth the parties can afford to disinter.” Thus, at a time when over 95 percent of relevant evidence is in electronic form and never reduced to paper, it is more important than ever that litigators understand how to use this new technology most efficiently.

It is somewhat similar to the story of the lumber jack who stops by the hardware store to have his ax sharpened and sees a sign for chainsaws guaranteeing three truck loads a day. Since the lumber jack had never produced more than one truck a day with his ax he buys a chainsaw.

After using the chainsaw for three days and never being able to get more than one truck of wood in a day, he returned to the store for a refund. When the salesman asked to inspect the chainsaw and started it, the lumber jack asked, “What’s that noise?”

The difference between paper and digital is very much like the difference between the ax and the chainsaw. The chainsaw is not only more economical but more potent. It is also a new technology and requires a different approach.

In some respects, e-discovery is no different than paper discovery. What is different is that the relevant evidence is contained in a variety of mediums (hard drives, servers, tapes, memory sticks, PDAs, cell phones, etc.) and systems (e-mail, financial, engineering, personnel, manufacturing, etc.) rather than a single medium (paper).

All too often litigators think only in terms of e-mails. A quantum claim has three parts, however—liability, causation and quantum. While liability may be found in an e-mail, it is unlikely that quantum or even causation will be found in an e-mail.

Moreover if the bad guy has taken efforts to hide his evil deed, it is unlikely that liability will even be found in an e-mail—at least not an active one. Thus the litigator must understand how the various sources can contribute to the case as well as how media forensics can assist in either finding the hidden smoking gun or uncovering what has been done to disguise the evil deed.

The first step for litigators is to understand the people, places and events important to the case. At the same time, they must

start building a conceptual model of the opponent’s computer systems and digital holdings in order to accurately determine how best to match the digital resources available to meet the requirements of the case.

Second, litigators must realize that digitized paper is not the same as digital evidence. The latter is much more economical and robust. Furthermore, it is foolish to spend part of the litigation budget to have the original digital evidence converted to an inferior format like TIFF or PDF.

Third, litigators must become proficient in using tools (viewers and analyzers) and how the techniques (digital fingerprints and file signatures) can be used to work more efficiently and minimize costs.

Fourth, as explained in the comments to Rule 26(b)(2), e-discovery can take an iterative, multi-stage approach where the low hanging fruit is harvested before proceeding to the more costly and difficult-to-access sources. Said another way, just because you have 5,000 backup tapes, that does not mean that you need to look at all of them.

Fifth, accessibility will be the next battleground. When digital evidence is deemed inaccessible, respondents may be able to get production relief or at least shift the cost of production to the requester.

In order to avoid having production requests denied, requesters must be proactive and use the various processes such as interrogatories, inspections, conferences, etc. to learn about the respondent’s computer systems and data holdings.

It is unlikely that the respondents will propose the most efficient production plan. So, it is essential that the requester be able to advise the respondent on how best to produce the data needed.

Finally, digital data makes preservation more important than ever. Continuing to use a computer can destroy relevant evidence. Without proper preservation a case can be lost before it starts and both client and counsel can be sanctioned.

§§§

Gregory Fordham is a founder of K&F Consulting, Inc., in Atlanta. He is a Certified Public Accountant, Certified Internal Auditor, Certified Computer Examiner, Security Plus certified and a Microsoft Certified Professional. He regularly advises clients on how to structure their e-discovery plans in order to minimize cost and maximize return. He also has served as an expert witness in many state and federal cases involving e-discovery and computer forensics. His e-mail is greg@knfcon.com