

CyberBytes™

Straight Talk about Electronic Evidence Discovery in Civil Cases- February 2007

Rule 16 Pretrial Conference

In summary, new Rule 26(f) requires that 21 days before a Rule 16(b) scheduling conference, the parties are to meet and confer to discuss any issues relating to preserving discoverable information; to develop a proposed discovery plan; to discuss any issues related to disclosure or discovery of electronically stored information (ESI), including the form or forms in which it should be produced; and to discuss any privilege issues, including the potential for a "clawback" agreement to be included in a court order.

Underlying Objectives

- Clarify the scope of the document requests
- To better understand opposing party's technical landscape
- To resolve the question of which form or forms production should be provided
- To reduce waste and reproduction of documents
- To pre-empt the negative impact of inadvertent production of privileged or private ESI

At first blush, this list doesn't seem too daunting. But any attorney who ever spent an afternoon with a client's chief information officer, trying to understand where the data requested by the other side in discovery are stored, knows that even understanding the language of the information technology (IT) world requires a significant investment of time and effort. So what will the courts -- and opposing counsel -- expect at a meet and confer session now that new rules are in effect?

Getting Informed

It breaks down into three general categories:

1. Knowledge of the client's data systems (or, in the case of a data requester, knowledge of what ESI he or she is seeking and where that kind of data might be found).

2. The ability to work cooperatively to develop a reasonable discovery plan based on an understanding of information systems and how data are stored.

3. An understanding of the special problems that production of electronic data poses, such as privilege waiver and form of production.

So what does one need to do to prepare? Perhaps the best thing is: Get educated-fast. The advisory committee notes state that it is "important for counsel to become familiar with [client's IT] systems before the conference." So how does a lawyer who knows little more than how to send and receive e-mail and run a PowerPoint presentation do that? The same way litigators for years have been handling cases about subject matter that they know little or nothing about -- ask questions of the people who are knowledgeable.

Unfortunately, many lawyers don't know what questions to ask; in short, they don't know what they don't know. And the resources for education in the IT world leave a lot to be desired, as they are typically written for people who already speak IT, not those just beginning to learn the language.

Microsoft Corp. did litigators a favor in this area. The company submitted written comments to the rules committee that are a useful entry for lawyers into the IT world. Microsoft has given lawyers a basic blueprint in the form of a graphic showing a simplified data architecture of a corporation. It includes most of the kinds of systems that typical corporations use to manage their data. A practitioner can think of this graphic as a deposition outline if he or she is representing a data producer (because certainly the data requesters will be doing the same thing) and start asking the clients' IT experts questions based on the graphic. The attorney will find many differences and some similarities, but most importantly will be learning about the client's systems. And that is information the attorney will need to prepare for the Rule 26(f) conference.

Data requesters who traditionally handle plaintiffs' work will also find Microsoft's submission helpful. They can use it to home in on the data they are looking for so that they can engage in fruitful discussions with their opponent, focusing on the data-storage areas of the company that might yield the most relevant information. If the opponent is unwilling or unable to discuss his or her client's systems, Microsoft's submission might be a useful way to get the ball rolling on those discussions.

Neither data requesters nor data producers should be shy about asking questions. The lawyers don't know where the data are; even the key players might not know. Lawyers must work with the IT representatives to find the data. Defense counsel cannot protect their clients from spoliation claims unless they know where the data they need to preserve are located. They should start asking these questions early in the engagement, rather than asking 22 days before the scheduling conference and one day before they meet and confer with their opponent.

The next area the parties will grapple with at the meet and confer is developing a discovery plan that is workable and reasonable, and that makes economic and practical sense, given the type of case and the nature of the discovery. Unless counsel knows something about his or her client's data architecture, such discussions at the meet and confer will be virtually impossible. Attorneys representing a data producer will have to know what the system capabilities are before they can negotiate reasonable time frames and limits for production.

For example, if the client has a database that contains the sales and inventory information at issue in a contract dispute, the attorney needs to understand how the database works and its reporting capabilities so that he or she can negotiate with the data requester on a reasonable schedule and form of production of such data. Data requesters will need to know the same information, so that they can determine whether

reports from the database will satisfy their needs or whether they need, for example, to seek an examination of the database itself by an expert hired by them for that purpose. Whatever agreements the parties reach at the meet and confer will be embodied in an updated Form 35 that specifically requires a description of the process for production of electronically stored information.

The final area of discussion is in reality a catch-all for things that make electronic discovery different from paper discovery. One of the key differences springs from the dynamic nature of electronic data. As opposed to paper documents -- which except for acts of God like hurricanes Katrina or Rita require an affirmative act by a human being to be destroyed -- much electronic data disappears through automated processes. The automated roll-off of e-mail from systems is a prime example. Many companies have instituted procedures that automatically delete e-mail based upon either dates or the size of an individual's mailbox. That is, e-mails that reach a set age are automatically deleted from the system, with the user having little or no ability to prevent such roll-off.

Data Preservation

Some organizations achieve a similar result by automating a process by which the oldest e-mail is deleted from a user's box as the box nears a designated size limitation. Companies also regularly write over or "recycle" disaster-recovery backup tapes of their systems to avoid continuously purchasing new tapes at additional cost. Material relevant in a case might be subject to such roll-off or recycling processes.

As reflected in the Rule 26(f) amendments, the federal courts are requiring the parties to give early attention to, and engage in discussions about, data preservation. Such discussions are good for both plaintiffs and defendants. For plaintiffs, they provide the opportunity to identify types of information for preservation, so that the material will be there as discovery progresses. For defendants, reaching agreement with plaintiffs on what must be preserved and what can continue to be disposed of in the ordinary course saves on the expense of preservation and protects against later claims of spoliation. Such agreements can be embodied in the Rule 16 scheduling order and thus sanctioned by the court.

Electronic data are particularly troublesome due to their sheer volume. The legal profession used to think of discovery in terms of boxes but now must think in terms of gigabytes, or even terabytes, of data. By way of comparison, the average box of production contains roughly 3,000 pages; the average gigabyte of e-mail contains 100,000 pages. Ten terabytes of data are roughly equivalent to the entire printed works of the Library of Congress. Many corporations house multiples of the Library of Congress on their active systems. Data are proliferating, and what lawyers need to review and produce in discovery is proliferating right along with it.

Even reviewing a 3,000-page box of paper documents could result in inadvertent production of privileged documents. In imposing the same rules and procedures on 100,000 pages of data, even more mistakes can result. It is for this reason that Rule 26(f) now specifically requires the parties to discuss "any issues relating to claims of privilege or protection as trial preparation material, including -- if the parties agree on a procedure to assert such claims after production" and whether that agreement should be embodied in the form of an order from the court. A word of caution: Even if the parties reach agreement on the clawback of privileged documents, any such agreement is still subject to the substantive law of the jurisdiction. There is a movement afoot to standardize the law of waiver in a proposed Federal Rule of Evidence. Rule 502, currently in draft form, is something that all litigators should monitor closely in the next few months.

Form of Production

The form of production is another issue that was not particularly problematic and didn't require discussion at the meet and confer when all the relevant documents were on paper. New Rule 26(f) requires parties to discuss the form or forms of production. Printing large volumes of electronic documents on paper and then making them available for review makes little economic or practical sense. Instead, lawyers on both sides of the bar often rely upon Web-hosted or internal databases such as Summation or Concordance to house discovery.

Making expectations clear during the meet and confer about the form in which one expects to receive discovery avoids the problems later of getting the production in a form incompatible with

the database one planned to use for the case. Attorneys should have the specifications for the load file required by their database handy at the meet and confer (or before) and should share them with opposing counsel. Chances are the other side will want something very similar. Additionally, agreeing which metadata fields (such as "to", "from", "cc", "bcc", "create date", "modified date", "last accessed date") will come with that database will also alleviate disagreement, as well as expense for both sides, down the road.

Cases will be dominated by e-mail, instant messaging and databases for the foreseeable future. The advisory committee has given lawyers the framework to avoid the problems that in recent cases resulted in dismissal of claims or sanctions for failure to properly preserve and produce electronic information. Lawyers who represent data requesters and those who represent data producers alike can help their clients by preparing to deal with these issue and by following the guidelines and procedures outlined by the amended rules and the accompanying advisory committee notes.

All of this means that practitioners whether they like it or not, have to get more engaged with the technological aspects of conducting or responding to electronic discovery. This ultimately translates to going beyond just the theoretical understanding of computer technology. While that does not necessarily mandate a highly evolved level of expertise in the area of technology, I recommend that you strive to know more than just the basics about computers and data if you hope to be successful in commercial litigation which involves ESI.

-Robert Guinaugh

Editor. Robert Guinaugh

Contributors. Wolfgang Wilke

This document is neither designed nor intended to provide legal or other professional advice but is intended merely to be a starting point for research and information on the subject of electronic evidence discovery. While every attempt has been made to ensure accuracy of this information, no responsibility can be accepted for errors or omissions.

CyberBytes is a monthly newsletter published by CyberControls, LLC and all contents are copyrighted with all rights reserved. Please submit your requests for distribution and additional copies to cyberinfo@cybercontrols.net 847-756-4890-Office 847-620-2500-Fax