American Association of Port Authorities
Executive Management Conference
February 12, 2007 — Miami, FL

The E-Discovery Rules: How To Avoid Being Bitten by a Byte

John M. Barkett
Shook, Hardy & Bacon L.L.P.

The New Federal Rules of Civil Procedure Addressing Discovery of Electronically Stored Information Went Into Effect on December 1, 2006

The Key To The New Federal Rules: C/3/C

COMMUNICATE WITH:

- CLIENT
- COUNSEL
- COURT

Major Changes To Rule 26

Rule 26 Initial Disclosure Obligation

Rule 26(a) now provides for upfront disclosure of ESI:

"Except in categories of proceedings specified in Rule 26(a)(1)(E), or to the extent otherwise stipulated or directed by order, a party must, without awaiting a discovery request, provide to other parties:

* * *

(B) a copy of, or a description by category and location of, all documents, electronically stored information, and tangible things that are in the possession, custody, or control of the party and that the disclosing party may use to support its claims or defenses, unless solely for impeachment;"

Rule 26 Meet and Confer

Counsel must now cover "any issues relating to preserving discoverable information."

The parties' discovery plan must now cover:

"(3) any issues relating to disclosure or discovery of electronically stored information, including the form or forms in which it should be produced;

(4) 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 – whether to ask the court to include their agreement in an order."

District Court's Upfront Role

Rule 16 (b) Scheduling Order may now contain:

"(5) provisions for disclosure or discovery of electronically stored information;

(6) any agreements the parties reach for asserting claims of privilege or protection as trial-preparation material after production;"

Preservation Orders

The Advisory Committee sought to limit the frequency and breadth of preservation orders:

"The requirement that the parties discuss preservation does not imply that courts should routinely enter preservation orders. A preservation order entered over objections should be narrowly tailored. Ex parte preservation should issue only in exceptional circumstances."

Inaccessible Information

Rule 26(b)(2)(B) limits initial production of inaccessible information identified by the party:

> "(B) A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery."

Determining Accessibility

The determination of whether a particular source of electronically stored information (ESI) is accessible or inaccessible does *not* depend upon physical access to the data, availability of technology (hardware or software) to deal with the data, or on the format of the data.

The determination must be based on "undue burden or cost."

This burden/cost test ties the discovery of ESI to the concept of marginal utility. Accordingly, the key question for the discovery of ESI is:

> *"Will the quantity, uniqueness, or relevance of responsive data that can be obtained from any particular source of ESI justify the burden or cost of the acquisition of the data?"*

Just because certain types of ESI sources are difficult to access—backup tapes, legacy data on obsolete systems, and databases are frequently mentioned—has no bearing on whether they are "accessible" for the purposes of discovery.

Examples of Inaccessible Data

The Advisory Committee Notes contain these examples:

- Back-up tapes intended for disaster recovery purposes that are often not indexed, organized, or susceptible to electronic searching;
- Legacy data that remains from obsolete systems and is unintelligible on the successor systems;
- Data that was “deleted” but remains in fragmented form, requiring a modern version of forensics to restore and retrieve; and
- Databases that were designed to create certain information in certain ways and that cannot readily create very different kinds or forms of information.

Scope of the Duty to Identify Inaccessible Documents

Committee Note to 26(b)(2) provides: "Under this rule, a responding party should produce electronically stored information that is relevant, not privileged, and reasonably accessible, subject to the (b)(2)(C) limitations that apply to all discovery. **The responding party** must also **identify, by category or type the sources containing potentially responsive information that it is neither searching nor producing. The identification** should, to the extent possible, **provide enough detail to enable the requesting party to evaluate the burdens and costs of providing the discovery and the likelihood of finding responsive information on the identified sources.**"

Testing Inaccessibility Claim by Motion to Compel or For Protective Order

- **Responding party must show** that the information is not reasonably accessible because of **undue burden or cost.**
- The district court may have to permit focused discovery to determine the costs and burdens in obtaining the information from the sources identified as not reasonably accessible, the likelihood of finding responsive information on such sources, and the value of the information to the litigation.
- **Requesting party** must show **good cause** to reach inaccessible information.
- **Good cause** will be determined by reference to the **proportionality test** set forth in Rule 26(b)(2)(C).

Proportionality Test of Rule 26(b)(2)(C)

The district court may limit the frequency and use of discovery if:

"(i) the discovery sought is unreasonably cumulative or duplicative, or is obtainable from some other source that is more convenient, less burdensome, or less expensive;

(ii) the party seeking discovery has had ample opportunity by discovery in the action to obtain the information sought; or,

(iii) the burden or expense of the proposed discovery outweighs its likely benefit, taking into account the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the litigation, and the importance of the proposed discovery in resolving the issues."

Other Factors In Evaluating Good Cause

The Committee Notes add the following:

(1) The specificity of the discovery request;

(2) The quantity of information available from other and more easily accessed sources;

(3) The failure to produce relevant information that seems likely to have existed but is no longer available on more easily accessed sources;

(4) The likelihood of finding relevant, responsive information that cannot be obtained from other, more easily accessed sources;

(5) Predictions as to the importance and usefulness of the further information;

(6) The importance of the issues at stake in the litigation;

(7) The party's resources.

Court's Options If Good Cause is Shown

- Limits on the **amount, type or sources** of information required to be accessed and produced
- **Payment by the requesting party** of part or all of the reasonable costs of obtaining information from sources that are not reasonably accessible
- **A requesting party's willingness to share or bear the access costs** may be weighed by the court in determining whether there is good cause

Marginal Utility Controls the Definition of Inaccessible Information

In the end, the determination of whether information is accessible does not depend upon either technology or the form of the data but on its marginal utility.

The likelihood the information is unique (it is not available elsewhere) and the materiality of the information to resolving the issues in dispute will be weighed against the cost or burden of retrieving it.

The Duty To Preserve Inaccessible Information

The Advisory Committee Note cautions:

"A party's identification of sources of electronically stored information as not reasonably accessible does not relieve the party of its common-law or statutory duties to preserve evidence."

The Duty To Preserve Inaccessible Information

So, do you store forever?

At a minimum:

- Address at the meet and confer session
- Be guided by the rule of reason
- Take advantage of the Rule 16 conference with the court

Answering Interrogatories by Reference to Electronically Stored Information Under New Rule 33

"Business Records" Redefined

Rule 33(d) allows production of business records in lieu of answering an interrogatory under prescribed circumstances.

New Rule 33(d) defines business records as "including electronically stored information."

Because of concerns over giving someone access to a party's electronic information storage system, the use of this option is not likely to become widespread.

Access Concerns
May Preclude Use of Rule 33(d)

The Advisory Committee recognized the problem:

"A party that wishes to invoke Rule 33(d) by specifying electronically stored information may be required to provide direct access to its electronic information system, but only if that is necessary to afford the requesting party an adequate opportunity to derive or ascertain the answer to the interrogatory. In that situation, the responding party's need to protect sensitive interests of confidentiality or privacy may mean that it must derive or ascertain and provide the answer itself rather than invoke Rule 33(d)."

Requesting Electronically Stored Information Under New Rule 34

Distinguishing Documents and Electronically Stored Information and Providing For Testing or Sampling

Rule 34(a) now provides that a party may serve on any other party a request:

"to inspect, copy, **test, or sample** any designated documents ***or*** **electronically stored information** – including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations **stored in any medium** – from which information can be obtained, translated, if necessary, by the respondent into reasonably usable form…."

Testing and Sampling

This is a well-established concept in the case law.

It is typically used to determine the likelihood of finding relevant information and to evaluate the cost of production versus the likely benefit when dealing with inaccessible electronically stored information.

Specifying The Form of Production

Under new Rule 34(b), the requesting party "may specify the **form or forms** in which electronically stored information is to be produced."

Should a requesting party should always specify the form of production?

Note the form of production may be different for different kinds of electronically stored information (e.g., word processing documents, spreadsheets, databases)

If the Requesting Party Does Not Specify The Form of Production

The responding party must specify the form or forms of production it intends to use.

Under Rule 34(b),

"Unless the parties otherwise agree, or the court otherwise orders:"

"(ii) if a request does not specify the form or forms for producing electronically stored information, a responding party must produce the information **in a form or forms in which it is ordinarily maintained** or in a form or forms that are **reasonably usable**."

If the Requesting Party Specifies the Form of Production

The responding party may object

> "to the requested form or forms for producing electronically stored information stating the reasons for the objection"

and

> "must state the form or forms it intends to use."

Forms of Production

- Native Format
- Tagged Image File Format (or TIFF)
- Portable Document Format (or PDF)
- Paper
- PST (Personal STorage) Format (e-mail)
- HTML or XML with hyperlinked attachments
- Case Management load files (images with selected metadata)
- *Any other negotiated form*

The concept of "ordinarily maintained in the normal course of business" may result in native format production.

Production is Limited to One Form

Under Rule 34(b):

"Unless the parties otherwise agree, or the court otherwise orders:"

"(iii) a party need not produce the same electronically stored information in more than one form."

Subpoena Recipients Under Rule 45

Rule 45 is conformed to Rule 34. The Advisory Committee Note acknowledges that a subpoena asking a third party to permit testing or sampling "may present particular issues of burden or intrusion" for the subpoena recipient. It then admonishes the district courts that the "protective provisions of Rule 45(c) should be enforced with vigilance when such demands are made."

Under Rule 45(c)(2)(B) an order to compel "shall protect any person who is not a party or an officer of a party from significant expense resulting from the inspection, copying, testing, or sampling commanded."

Sanctions For Loss of Electronically Stored Information

The New "Safe" Harbor Under Rule 37(f)

"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."

Questions Under New Rule 37(f)

- What are "exceptional circumstances"? Prejudice to the other side will be raised here
- Note the reference to "under these rules" protecting the inherent power of the court to issue a sanction
- The sanction applies to a "party" — Does that include counsel?
- When is the operation of an electronic information system "routine" and in "good faith" in relation to the duty to preserve?
- Does the "safe" harbor apply to electronic information on employees' computer hard drives or other storage media?
- Does Rule 37(f) apply to a prelitigation loss of electronically stored information that occurred after a duty to preserve existed?

Dealing with Privileged Information and Work Product

The Problem of Privileged Documents Intermingled with Inaccessible Information

- If you look first, the information may no longer be “inaccessible”
- Address at the meet and confer session
- It may be a symmetrical problem leading to a mutually acceptable solution
- If it is asymmetric, consider a “quick peek” or “clawback” agreement

Quick Peek and Clawback Agreements

To avoid the cost of a privilege review but to minimize the risk of waiver of a privilege or work product protection, the Advisory Committee recognized that parties "may agree that the responding party will provide the requested materials for initial examination without waiving any privilege."

After reviewing information designated for production, "the producing party then asserts a privilege under Rule 26(b)(5)(a) describing the nature of documents or information not produced in a manner that allows other parties to assess the applicability of privilege or protection (even though the requesting party's counsel will have already seen the document or information)."

"On other occasions, parties enter agreements—sometimes called 'clawback agreements'—providing that production without intent to waive privilege should not be a waiver so long as the producing party identifies the documents mistakenly produced, and that the documents should be returned under those circumstances."

Inadvertent Disclosure

- New Rule 26(b)(5)(B) applies to paper or electronically stored information
- If privileged information has been produced, the party claiming privilege gives notice of the claim and the basis for it
- After being notified, a party must **promptly return, sequester, or destroy** the specified information and any copies it has and may not use or disclose the information until the claim is resolved
- A receiving party may promptly present the information to the court under seal for a determination of the claim
- If the receiving party disclosed the information before being notified, it must take reasonable steps to retrieve it
- The producing party must preserve the information until the claim is resolved

Revised Rule 26(f)—Meet-and-Confer

- Key Players
- Key Data
- Key Words
- Key Dates

Revised Rule 26(f)—Meet-and-Confer

- Timing: When should e-discovery efforts begin
- Preservation: Who, what, where, when and how
- Key Players: Class membership rules, organization charts
- Key Data
  - Key Words: search terms/technologies
  - Data types and/or key applications/systems
  - Electronic Mail
  - Backup Tapes: Inclusion rules, sampling

Revised Rule 26(f)—Meet-and-Confer

- Processing Data: Native v. Static
- Reviewing Data: Native v. Static
- Timelines
- Form of Production: Native, static, hybrid
- Depositions
- Inadvertent Production: Quick Peek, Clawback
- Dispute handling

Perspective Of The Judge

- More meet-and-confer type activities
- Lawyers must know about e-discovery in general
- Lawyers must have sufficient knowledge about the client's IT environment and of the client's data environment, including legacy data, live data, data types and data access
- Accurate representations regarding the capability, timing, and cost associated with matter-specific e-discovery are a must

Perspective Of The Judge

- Implementation of a *process* that leads to defensible and timely (i.e., not sluggish) e-discovery
- Use of targeted electronic discovery tools such as key player groups, tape and data sampling, selection criteria, de-duplication, metadata inclusion, native review, and native production
- Use of third parties to resolve e-discovery disputes
- Reasonableness informed by the threat of cost-shifting
- Symmetry, scalability, consistency, and diligence

Ten Mistakes to Avoid in *e*Discovery

1. Failing to advise the client of the need to impose proper preservation holds in a pre-litigation setting, especially at the time of retention of outside counsel
2. Using the legend, "Attorney Work Product," when no litigation is anticipated and then claiming a protection from discovery of documents so marked in later litigation, thereby establishing the date on which a records hold should have been implemented
3. Failing to involve information technology personnel early enough in the discovery process
4. Failing to comprehend the universe of the client's electronically stored information in both accessible and inaccessible formats
5. Failing to comprehend the auto-delete or recycling processes of the client's electronic information systems

Ten Mistakes to Avoid in *eDiscovery*

6. Failing to adequately identify "key" players, failing to identify the storage habits of key players, and then failing to secure the storage media of key players
7. Failing to follow up with key players to ensure that preservation orders are being followed
8. Failing to produce electronic information in a timely manner
9. Making unilateral decisions in producing electronic information, particularly with respect to the form of production and metadata
10. Failing to communicate early and clearly with the client, with opposing counsel, and with the court regarding e-discovery issues

States Will Soon Be Following

- Conference of Chief Judges of the state courts has issued a set of guidelines on electronic discovery that closely follows the federal rules. *Guidelines For State Trial Courts Regarding Discovery Of Electronically-Stored Information* (August 2006)
- http://www.ncsconline.org/WC/Publications/CS_ElDiscCCJGuidelines.pdf
- Meet and confer session is not typical in state court
- Cost-shifting rules may be different (e.g. CA, TX)

If you would like a copy of the slides used for this presentation, please email John Barkett at:

jbarkett@shb.com
or call 305-960-6931

and request the "AAPA Slides"—Thank You