SUMMARY OF CHANGES RELATING TO ELECTRONICALLY STORED INFORMATION IN THE FEDERAL RULES OF CIVIL PROCEDURE EFFECTIVE DECEMBER 1, 2007

By Kary Pratt

Initially, what the Courts generally refer to as the "Electronic Discovery Amendments" to the Federal Rules of Civil Procedure went into effect on December 1, 2006. These Amendments involved Rules 16, 26, 33, 34, and 37 of the Federal Rules of Civil Procedure. These rules were re-written as part of the "Style Project." The current version of the rules went into effect on December 1, 2007. This handout contains the Rules that went into effect on December 1, 2007.

- ***Summary of Changes to FRCP 16.***

FRCP 16(b)(3)(B) was modified to provide that the Scheduling Order may "provide for disclosure or discovery of electronically stored information" and "include any agreements the parties reach for asserting claims of privilege or of protection as trial-preparation material after information is produced." This rule essentially allows for the Court to include so-called "claw-back" and "quick peek" agreements in the Court's scheduling order.

- ***Summary of Changes to FRCP 26.***

The changes to Rule 26(a) clarify a party's duty to include disclosure of "electronically stored information" in its initial disclosures. Although most parties in Oregon "opt out" of initial disclosures as permitted by District of Oregon Local Rule 26.2, the changes to Rule 26(a) may discourage some parties from opting out of these disclosures as they are a way to require parties with significant electronically stored information to provide such information up front, at the beginning of the litigation.

FRCP 26(b)(2)(B) clarifies the obligation of a responding party to provide discovery of electronically stored information that is not reasonably accessible. A party does not need to produce information that is not "reasonably accessible" because of undue burden or cost. However, the responding party must identify the sources of potentially responsive information that it has not searched because those sources are not "reasonably accessible" because of undue burden or cost. If the requesting party moves to compel, the responding party has the burden to show that the data is not "reasonably accessible" because of undue burden or cost. If this showing is made, the Court looks to the requesting party to demonstrate that it has good cause. If the requesting party demonstrates such cause, the Court may order production, but has the discretion to impose certain limitations or conditions on production.

FRCP 26(b)(5) clarifies the procedure that applies when a responding party asserts a claim of privilege or work product protection after production. It is a new procedural rule, and it is not intended to affect the substantive rules for determining whether waiver of privilege or work product protection has occurred. Under the new rule, the producing party must notify the receiving party of its claim of inadvertent production. Once notification has occurred, the receiving party must return, destroy or sequester the information and cannot disclose it to third parties until the claim of privilege is resolved. If the information has been disclosed before receiving the claim of privilege or work product protection, the receiving party must take appropriate recall steps. The rule allows the receiving party to submit the information to the Court to decide the privilege issue, and can make any waiver arguments to the Court. Any delay in notification to the receiving party can be considered by the Court when it examines the waiver question.

- ***Summary of Changes to FRCP 33.***

The changes to FRCP 33(d) clarify that a party may answer an interrogatory regarding the review of business records by providing access to the information if the interrogating party can find the answer as easily as the responding party can.

- ***Summary of Changes to FRCP 34.***

The changes to FRCP 34(a) create a distinction between "electronically stored information" as a category distinct from documents and things. The new FRCP 34(b)(1)(C) also authorizes the requesting party to specify the form of production of "electronically stored information" and gives the responding party a way to object to the requested format. Absent a court order, an agreement between the parties or a request for a specific form of production, a party can produce the electronically stored information in the form in which it is ordinarily maintained or in a "reasonably useable form."

- ***Summary of Changes to FRCP 37.***

FRCP 37(e) recognizes that some electronically stored information is lost as a result of routine, good faith operation of an electronic information system and provides that a court may not impose sanction for failure to produce electronically stored information "absent exceptional circumstances."

- ***Summary of Changes to FRPC 45***

Rule 45 was changed so that the rules relating to information sought by subpoena conforms to the other changes to the rules regarding electronically stored information.

E-DISCOVERY IN FEDERAL COURT:

TOP TEN CHANGES YOU SHOULD MAKE TO YOUR PRACTICE

By Kary Pratt

1. ELECTRONICALLY STORED DATA MUST BE IDENTIFIED RIGHT AWAY.

- "Electronically stored data" is now a separate category for discovery. You must identify where the data is and what kind of data exists early in the case because you have a duty to preserve that data.

- This may require a discussion with your client's IT staff. If the systems are very complex, or you are completely unfamiliar with understanding the technology, you should consider hiring an e-discovery/forensics firm to assist you.

    - Check out Form 2.3 in *The Electronic Evidence and Discovery Handbook*, Sharon D. Nelson, Bruce A. Olson, John W. Simek, available from the American Bar Association for $129 – 1-800-285-2221 or online at www.ababooks.org. This form provides guidelines for hiring an electronic discovery or computer forensics expert.

- Information you will need to obtain from your client:

    - detailed descriptions of computer systems used by the company, including hardware systems, primary operating systems, and major software systems, including any customized software.

    - detailed description of how those computers are networked or connected to others outside of the company

        - If your client operates from multiple locations, you will need to consider all potential data locations, including geographic locations as well as storage locations such as file shares, archival tapes, and hosted email.

    - detailed description of computer systems used by relevant employees outside of the corporate system (home computers, PDAs)

    - detailed description of backup processes and schedules, document retention and destruction schedules, organized by type of data, with locations for each of the systems.

    - the company's document retention and destruction policy, email and internet usage policies and litigation hold policies if any.

- whether and how the company monitors employees' computer usage.

- whether any third parties have access to the company's data, identify them and get contact information.

- Distinguish between accessible data and inaccessible data- The new rules distinguish between data that is readily accessible and data that is not. FRCP 26(b)(2)(B) clarifies that a party need not produce information that is not reasonably accessible because of undue burden or cost.

  - Examples of data which is not reasonably accessible include: deleted information, information on backup systems for disaster recovery purposes, and legacy data remaining from systems no longer in use.

2. YOU MUST ADVISE YOUR CLIENT OF ITS OBLIGATIONS TO PRESERVE ELECTRONIC EVIDENCE AS SOON AS YOU ARE ENGAGED.

- Once you have an idea of where the data is and who might have it, you need to prepare letter to your client advising them of their obligation to preserve evidence, including electronic evidence.

  - Should you fail to advise your client of its obligation in sufficient detail, and your client is ultimately sanctioned, you can wind up with a claim against you.

- You should assist your client in crafting a litigation hold to prevent the destruction of responsive evidence.

  - You can use the Sedona Guidelines at http:www.thesedona conference.org/publications_html, which provides recommended best practices for electronic document retention and production, to help develop electronic information policies.

    - Make sure that the litigation hold is issued not only to the employees whose conduct was at issue, but any employee who may have been likely to have had any contact with the issues in the lawsuit.

    - Make sure the litigation hold is issued to the IT department if any, and ensure that they understand the obligations to preserve electronic evidence.

    - Consider whether it is necessary to send a letter regarding preservation duties to any third party vendors or contractors of your client who might have evidence relating to the claim.

- Sanctions can be awarded when counsel fails to cause the defendant to adopt a litigation hold to prevent destruction of responsive information. See, eg *Metropolitan Opera Assoc. v. Local 100*, 212 FRD 178 (SDNY 2003)

- IMPORTANT NOTE: You must make it clear to your client that the duty to preserve evidence trumps the client's standard information retention/destruction policies.

3. YOU MUST BE PREPARED TO DISCUSS ELECTRONIC DISCOVERY AT THE MEET AND CONFER UNDER FRCP 26(f)

- Under our local rules, this conference is required to takes place 30 days after the last defendant is served.

- Under revised FRCP 26(f) this conference is to include consideration of issues related to disclosure or discovery of electronically stored information, including the form of production, the identification of any distinctive or recurring problems occurring from the fact that the information is stored electronically, issues related to preservation of electronically dynamic information, and inadvertent production of privileged information in discovery.

    - Parties are encouraged under the commentary to develop agreed upon protocols to facilitate discovery that are faster and less expensive and can be included in the court case management order.

- You'll need to know the systems and applications your client has or have someone sit in on the conference who does.

- Your client may want you to arrange for some relief from some of the measures it has employed to preserve evidence. This is your opportunity to request an agreement to allow for that relief.

- Be prepared if your opponent asks that it be permitted to rotate server back up tapes, replace systems or delete older emails. Don't concede that your opponent can destroy any information in any form unless the party demonstrates that the information lost is not likely to be relevant to any issue in the case or lead to the discovery of admissible evidence.

- If you anticipate that the volume of electronic discovery in your case will be very large, at this point you should consider and discuss quick peek and claw back agreements so that no privileges are waived.

    - However, as noted in the article entitled "*Dangers In The Use Of Quick Peek And Claw Back Agreements Under The New E-Discovery Rules*"

with these materials, there are some dangers in using these agreements you should be aware of before entering into one.

4. YOU MUST CHANGE THE WAY YOU REQUEST DOCUMENTS

- FRCP 34(a) explicitly recognizes electronically stored information as a category distinct from "documents" and "tangible things" (see FRCP 34(a)(1)(B)).

- FRCP 34(b) specifically authorizes the requesting party to specify the form of production and gives the responding party a means to object to the requested format.

    - FRCP 34(b)(2)(E)(iii) states that a party need not produce the same electronically stored information in more than one form. So, be sure from the outset that you can handle the form of the information that you request.

    - You need to evaluate what form you want your opponent's documents in- hard copies, images of data, exported data, native data, hosted data (this is data that resides on a controlled access website.)

        - Review the November 2006 Article in In Brief entitled "*Requesting and Producing Electronic Discovery"* by Craig Ball for advice on choosing an ESI form.

- Figure out the production formats that will best work for you from a cost perspective and what you have the capacity to process.

    - Do you want the information in native format? For example, do you want documents created in word in electronic form in Word? Native format usually includes all of the metadata associated with the document.

        - Metadata is information about a particular data set or document that tells how, when or by whom it was collected created, accessed and modified and how it is formatted. This data is generally not reproduced in full form when a document is printed.

        - You need to consider whether you have the program necessary to view the data in native form before you request it that way. You may be able to easily have the data converted to a format which will make it accessible to you if it is in a proprietary format, or even request that the opposing party convert it to a common program, such as Excel, if their system has the capacity to do that. But you have got to do your homework to figure this out and make your request accordingly. Talking to an e-discovery vendor may help on this issue.

    - If you are unsure you have the applications necessary to read the data in native format, you should request it in a static format, such as TIFF or PDF. However, if you request it that way, you will get a static image of the document without metadata.

- If you need metadata, you must specifically request that electronic data be produced in the form it is maintained. If you don't say that, the rules allow the opposing party to produce it any reasonably useable form and this may mean you will get only copies of screen shots, stripped of metadata.

- If all you want is hard copies, you need to be specific in your request for production because the opposing party can produce in the form the data is reasonably kept unless you make a specific request for production in hard copy form.

    - Be careful when you ask for hard copies rather than native files in electronic form in cases where the volume of discovery is large. The opposing party may complain that the cost of blowing back the electronic data to hard copy form is too expensive and may invoke the cost sharing mechanism of the new rules to force you to pay for that process.

- When the volume of documents requires electronic searchability, just getting the image files may not be enough unless they include a searchable data layer or load file. Native data might be more useful if there is no way to search image files. Native data would include the .doc, .wpd and .rft formats.

- Carefully formulate your requests for production for electronic formats.

    - Forms 5.15-5.23 in *The Electronic Evidence and Discovery Handbook*, Sharon D. Nelson, Bruce A. Olson, John W. Simek, available from the American Bar Association for $129 – 1-800-285-2221 or online at www.ababooks.org. will give you ideas on what kinds of requests you can make and how to frame them for different types of production formats.

- A good strategy is to make targeted requests for data in electronic form in your first request and then expand on that in subsequent requests depending on how useful the information and format was and then follow up with additional requests as appropriate.

- When requesting email, you must be sure to request not only all related metadata, but also all attachment files.

- Don't forget to request instant messaging and voicemail files that are electronically stored if those might be relevant to your case. Many systems

preserve voicemail in a data form on the computer, even after the voicemail has been deleted from the phone system.

- What happens if you don't specify a form of production for ESI? Under revised FRCP 34, absent a court order, party agreement, or a request for a specific form of production, a party may produce the electronically stored information in the form in which it is ordinarily maintained **or in a reasonably useable form.**

    - Absent a court order, the information need only be produced in one form, so if you forget to specify a format, you are likely to be stuck with the form produced by the opposing party..

- Be sure to specifically request the opposing party's document retention policies.

- Be careful what you ask for! Once you get it, you are going to have to sort through it. So, ask for it in a form you can manage.

    - The old standby "produce any and all …relating to" may well be problematic if you find your self the recipient of terabytes of information that you need to pay large sums of money to process and analyze only to find out that the data was useless to your case.

    - Your mantra should be: COMPEL BROAD E-RETENTION BUT SEEK NARROW E-PRODUCTION.

5. YOU MUST PAY CAREFUL ATTENTION TO THE WORDING OF THE REQUESTS FOR PRODUCTION YOU RECEIVE AND OBJECT TO FORM IN A TIMELY FASHION

- ***If no form for producing ESI is specified*** in the request for production, FRCP 34(b) nonetheless requires you to state the form you intend to use. FRCP 34(b)(2)(E)(ii) provides that if a request does not specify the form, you must produce the information in the "form or forms in which it is ordinarily maintained or in a reasonably useable form or forms."

- ***If the form for producing ESI is specified but you object to production in that form***, you must specifically object to the form and must state the form or forms of production you intend to use under FRCP 34(b)(2)(C) and FRCP 34(b)(2)(D).

    - The new rules do not say when this objection needs to be made, but a good practice is to do it at the time you respond to the request for production, before the date set for actual exchange of production.

6. YOU MUST IDENTIFY AND OBJECT TO REQUESTS SEEKING ESI FROM SOURCES WHICH ARE NOT REASONABLY ACCESSIBLE

- ***If the request includes ESI from sources which are not reasonably accessible because of undue burden or cost***, such discovery may be subject to the limitation of FRCP 26(b)(2)(B). However, to invoke that protection, you should object to the production specifically on that ground.

    - The new rules do not say when this objection needs to be made, but a good practice is to do it at the time you respond to the request for production.

    - After you object, the ball is then in your opponent's court and they must make a motion to compel or file for a protective order. If they do that, you must show that the information is not reasonably accessible due to undue burden or cost under FRCP 26(b)(2)(B). If you make that showing, the burden shifts back to the party requesting the production to show good cause.

        - Who pays if such non-readily accessible information is ordered produced? The rules don't address this, but the Advisory Notes do. Under the Advisory Committee Note, the court has authority to set conditions for permitting the discovery, including "payment by the requesting party of part or all of the reasonable costs of obtaining information from sources that are not reasonably accessible." The note also states that "the requesting party's willingness to share in the costs may be weighed in determining whether there is good cause."

            - The Advisory Committee Notes also talk about the possibility of sampling to test the assertion of inaccessibility

7. YOU MUST CAREFULLY PROTECT FROM THE INADVERTANT DISCLOSURE OF PRIVILEGED INFORMATION

- Like you did with paper discovery, you must have a system to sort out privileged materials from ESI. New FRE 502 provides some protection for inadvertent disclosure, however it is limited. A copy of this rule is included in these materials.

-

8. YOU MUST NOW CONSIDER ESI WHEN PREPARING AND RESPONDING TO SUBPOENAS

- Revised FRCP 45 conforms the subpoena provisions to the changes in the other rules related to electronic discovery.

- Be careful what you ask for, especially when issuing a subpoena to a large institutional party.

- Be careful to specify the form of production you need from the subpoenaed party.

    - You can always negotiate this issue with the subpoenaed party. Most parties will tell you the way the information is stored so that the request can be tailored to cause the least disruption to their business.

9. YOU MUST CHANGE YOUR DEPOSITION PRACTICE

- Depending on the size of the case and type of data you expect, you may need to take 30(b)(6) depositions of the opposing parties IT personnel to make sure that you ask for what is available and ask for it in a form that provides the maximum amount of information and in a form which is useable to you.

    - You need to discover information from your opponent about offline storage and external data sources. Once you know where the potential evidence is, you may have to ask the court to establish a search protocol if you do not trust the opposing party or that party is obstructive.

        - Check out Form 5.24 in *The Electronic Evidence and Discovery Handbook*, Sharon D. Nelson, Bruce A. Olson, John W. Simek, available from the American Bar Association for $129 – 1-800-285-2221 or online at www.ababooks.org.

    - You may need to rewrite requests for production after the 30(b)(6) deposition, so be sure to do it early enough in the case so that you have time to follow up.

- Ask fact witnesses where they looked for evidence to comply with your requests for production, how they conducted a search, their individual practices with regard to document/email retention, whether they searched their email archives, etc. Be specific.

    - If you think that the search was not adequate, make a request on the record that the additional sources be searched and any additional materials produced.

    - Be sure to specifically ask witnesses about the opposing party's compliance with their firm document retention policies.

- If you do not inquire deeply enough of your opposing party, you will likely either fail to get complete discovery or lose an opportunity to put the adverse party in a position of having to defend its discovery failures.

- Be sure to prepare your own fact witnesses to respond to questions as to how they looked for the requested electronic documents, eg., what searches they performed, whether they searched archived email, performed a google desktop search, etc.

- If there is data that has been lost or destroyed, you must be prepared to have your witness respond to questions concerning whether the loss or destruction of the data was a necessary feature of the normal routine operation of the systems in order to establish the good faith defense of FRCP 37(f).

    - If there is a simple way to suspend the operation of normal processes, your witness must be prepared to explain why that step was not taken. If the suspension of the operation of normal processes to avoid overwriting information would have created problems for the system, the witness should be prepared to explain why or identify the person who can explain why. You may need to engage an expert to explain the processes for especially complex, customized systems.

10. YOU MUST THINK ABOUT HOW YOU ARE GOING TO AUTHENTICATE ELECTRONICALLY STORED DATA FROM THE START

- Whether you are collecting it from your client or from an opposing party, you must keep in mind that it is more difficult to authenticate electronic data and that some courts have set high standards. Depending on the size of the case and type of data you expect, you may need to take 30(b)(6) depositions of the opposing parties IT personnel to make sure that you ask for what is available and ask for it in a form that provides the maximum amount of information and in a form which is useable to you.

-

    - Check out *In Re Vinhnee*, 336 B.R. 437 (9th Cir. B.A.P. 2005) for some guidelines set by the Ninth Circuit Bankruptcy Appeals Panel. See also *Lorraine v. Markel American Insurance Co.*, 241 F.R.D. 534, 538 (D. MD. 2007).