THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF OKLAHOMA

Guidelines for Discovery of Electronically Stored Information (ESI)[1]

These guidelines are intended to facilitate compliance with the provisions of Fed. R. Civ. P. 16, 26, 33, 34, 37, and 45, as amended December 1, 2006 and December 1, 2007, relating to the discovery of ESI. In the case of any asserted conflict between these guidelines and the above-referenced rules, the latter shall control.

1. Early Attention to Electronic Discovery Issues. Prior to the Fed. R. Civ. P. 26(f) conference, counsel should become knowledgeable about their clients' information management systems and their operation, including how information is stored and retrieved. In addition, counsel should make a reasonable attempt to determine where ESI is likely to be located, including backup, archival and legacy data (outdated formats or media), and to consider preservation obligations.[2]

2. Duty to disclose. Initial disclosures pursuant to Fed. R. Civ. P. 26(a)(1) must include any ESI that the disclosing party may use to support its claims or defenses (unless used solely for impeachment). Counsel should identify those individuals with knowledge of their clients' electronic information systems who can facilitate the location and identification of discoverable ESI prior to the Fed. R. Civ. P. 26(f) conference.

3. Duty to notify. A party seeking discovery of ESI should notify the opposing party of that fact and, if known at the time of the Fed. R. Civ. P. 26(f) conference, should identify as clearly as possible the categories of information that may be sought. Parties and counsel are reminded that, under Fed. R. Civ. P. 34, if the requesting party has not designated a form of production in its request, or if the responding party objects to the designated form, then the responding party must state in its written response the form it intends to use for producing ESI. It must be in the form in which it is ordinarily maintained or in a reasonably usable form or forms. For a discussion of "form of production," see Fed. R. Civ. P. 34(b) cmt. to 2006 amendments.

4. Duty to meet and confer regarding ESI. During the Fed. R. Civ. P. 26(f) conference, the parties should confer regarding the following matters:[3]

---

[1] These guidelines are adapted from those promulgated by the United States District Court for the District of Kansas, which are acknowledged and appreciated.

[2] For definitions of terms used in these guidelines, see The Sedona Conference® Glossary: E-Discovery & Digital Information Management (Second Edition) at http://www.thesedonaconference.org.

[3] For a more detailed description of matters that may need to be discussed, see Craig Ball, *Ask and Answer the Right Questions in EDD*, LAW TECHNOLOGY NEWS, Jan. 4, 2008, accessed on Feb. 1, 2008 at http://www.law.com/jsp/ihc/PubArticleIHC.jsp?id=1199441131702# and reprinted in these Guidelines with permission at Appendix 1.

(a) ESI in general. Counsel should attempt to agree on steps the parties will take to segregate and preserve ESI in order to avoid accusations of spoliation.

(b) E-mail information. Counsel should attempt to agree on the scope of e-mail discovery and e-mail search protocol.

(c) Deleted information. Counsel should attempt to agree on whether responsive deleted information still exists, the extent to which restoration of deleted information is needed, and who will bear the costs of restoration.

(d) "Embedded data" and "metadata." "Embedded data" typically refers to draft language, editorial comments, and other deleted matter retained by computer programs. "Metadata" typically refers to information describing the history, tracking, or management of an electronic file. The parties should discuss at the Fed. R. Civ. P. 26(f) conference whether "embedded data" and "metadata" exist, whether it will be requested or should be produced, and how to handle determinations regarding attorney-client privilege or protection of trial preparation materials.

(e) Back-up and archival data. Counsel should attempt to agree on whether responsive back-up and archival data exists, the extent to which back-up and archival data is needed, and who will bear the cost of obtaining such data.

(f) Format and media. Counsel should attempt to agree on the format and media to be used in the production of ESI. Counsel should also discuss the benefits and need for native format versus imaged format.

(g) Reasonably accessible information and costs. The volume of, and ability to search, ESI means that most parties' discovery needs will be satisfied from reasonably accessible sources. Counsel should attempt to determine if any responsive ESI is not reasonably accessible, i.e., information that is only accessible by incurring undue burdens or costs. If the responding party is not searching or does not plan to search certain sources containing potentially responsive information, it should identify the category or type of such information. If the requesting party intends to seek discovery of ESI from sources identified as not reasonably accessible, the parties should discuss: (1) the burdens and costs of accessing and retrieving the information, (2) the needs that may establish good cause for requiring production of all or part of the information, even if the information sought is not reasonably accessible, and (3) conditions on obtaining and producing this information such as scope, time, and allocation of cost.

(h) Privileged or trial preparation materials. Counsel should attempt to reach an agreement regarding what will happen in the event privileged or trial preparation materials are inadvertently disclosed. Pursuant to Fed. R. Civ. P. 26(5)(B), if the disclosing party inadvertently produces privileged or trial preparation materials, it must notify the requesting party of such disclosure. After the requesting party is notified, it must return, sequester, or destroy all information and copies and may not use or disclose this information until the claim of privilege or protection as trial preparation materials is resolved. This rule has been

described as the "clawback" rule.

(i) The parties may agree to provide a "quick peek," whereby the responding party provides certain requested materials for initial examination without waiving any privilege or protection.

(ii) The parties may also establish a "clawback agreement," whereby materials that are disclosed without intent to waive privilege or protection are not waived and are returned to the responding party, so long as the responding party identifies the materials mistakenly produced.

(iii) Other voluntary agreements should be considered as appropriate. The parties should be aware that there is an issue of whether such agreements bind third parties who are not parties to the agreements.[4] The parties may consider asking the court to incorporate the agreement into a court order.

(iv) Counsel should be aware this rule merely establishes a procedure to minimize the effects of inadvertent disclosure. It does not resolve the question of whether inadvertent disclosure causes waiver of the privilege. That question is resolved by the law of the jurisdiction involved.

5. **Duty to meet and confer when requesting ESI from nonparties (Fed. R. Civ. P. 45).** Parties issuing requests for ESI from nonparties should attempt to informally meet and confer with the non-party (or counsel, if represented). During this meeting, counsel should discuss the same issues with regard to requests for ESI that they would with opposing counsel as set forth in paragraph 4 above.

---

[4] For a detailed discussion on this issue, see Hon. John M. Facciola, *Sailing on Confused Seas: Privilege Waiver and the New Federal Rules of Civil Procedure*, 2006 Fed. Cts. L. Rev. 6 (Sept. 2006) at http://www.fclr.org/2006fedctslrev6.htm.

APPENDIX 1

Ask and Answer the Right Questions in EDD

Craig Ball
Law Technology News
January 4, 2008

Sometimes it's more important to ask the right questions than to know the right answers, especially when it comes to nailing down sources of electronically stored information, preservation efforts and plans for production in the FRCP Rule 26(f) conference, the so-called "meet and confer."

The federal bench is deadly serious about meet and confers, and heavy boots have begun to meet recalcitrant behinds when Rule 26(f) encounters are perfunctory, drive-by events. Enlightened judges see that meet and confers must evolve into candid, constructive mind melds if we are to take some of the sting and "gotcha" out of e-discovery. Meet and confer requires intense preparation built on a broad and deep gathering of detailed information about systems, applications, users, issues and actions. An hour or two of hard work should lie behind every minute of a Rule 26(f) conference. Forget "winging it" on charm or bluster and forget "We'll get back to you on that."

Here are 50 questions of the sort I think should be hashed out in a Rule 26(f) conference. If you think asking them is challenging, think about what's required to deliver answers you can certify in court. It's going to take considerable arm-twisting by the courts to get lawyers and clients to do this much homework and master a new vocabulary, but, there is no other way.

These 50 aren't all the right questions for you to pose to your opponent, but there's a good chance many of them are . . . and a likelihood you'll be in the hot seat facing them, too.

1. What are the issues in the case?
2. Who are the key players in the case?
3. Who are the persons most knowledgeable about ESI systems?
4. What events and intervals are relevant?
5. When did preservation duties and privileges attach?
6. What data are at greatest risk of alteration or destruction?
7. Are systems slated for replacement or disposal?
8. What steps have been or will be taken to preserve ESI?
9. What third parties hold information that must be preserved, and who will notify them?
10. What data require forensically sound preservation?
11. Are there unique chain-of-custody needs to be met?
12. What metadata are relevant, and how will it be preserved, extracted and produced?

13. What are the data retention policies and practices?
14. What are the backup practices, and what tape archives exist?
15. Are there legacy systems to be addressed?
16. How will the parties handle voice mail, instant messaging and other challenging ESI?
17. Is there a preservation duty going forward, and how will it be met?
18. Is a preservation or protective order needed?
19. What e-mail applications are used currently and in the relevant past?
20. Are personal e-mail accounts and computer systems involved?
21. What principal applications are used in the business, now and in the past?
22. What electronic formats are common, and in what anticipated volumes?
23. Is there a document or messaging archival system?
24. What relevant databases exist?
25. Will paper documents be scanned, and if so, at what resolution and with what OCR and metadata?
26. What search techniques will be used to identify responsive or privileged ESI?
27. If keyword searching is contemplated, can the parties agree on keywords?
28. Can supplementary keyword searches be pursued?
29. How will the contents of databases be discovered? Queries? Export? Copies? Access?
30. How will de-duplication be handled, and will data be re-populated for production?
31. What forms of production are offered or sought?
32. Will single- or multipage .tiffs, PDFs or other image formats be produced?
33. Will load files accompany document images, and how will they be populated?
34. How will the parties approach file naming, unique identification and Bates numbering?
35. Will there be a need for native file production? Quasi-native production?
36. On what media will ESI be delivered? Optical disks? External drives? FTP?
37. How will we handle inadvertent production of privileged ESI?
38. How will we protect trade secrets and other confidential information in the ESI?
39. Do regulatory prohibitions on disclosure, foreign privacy laws or export restrictions apply?
40. How do we resolve questions about printouts before their use in deposition or at trial?
41. How will we handle authentication of native ESI used in deposition or trial?
42. What ESI will be claimed as not reasonably accessible, and on what bases?
43. Who will serve as liaisons or coordinators for each side on ESI issues?
44. Will technical assistants be permitted to communicate directly?
45. Is there a need for an e-discovery special master?
46. Can any costs be shared or shifted by agreement?
47. Can cost savings be realized using shared vendors, repositories or neutral experts?

48. How much time is required to identify, collect, process, review, redact and produce ESI?
49. How can production be structured to accommodate depositions and deadlines?
50. When is the next Rule 26(f) conference (because we need to do this more than once)?