IMPORTANT NOTICE:
This Publication Has Been Superseded

See the Most Current Publication at

https://thesedonaconference.org/publication/Jumpstart_Outline

THE SEDONA CONFERENCE® WORKING GROUP SERIES

THE SEDONA CONFERENCE® "JUMPSTART OUTLINE": QUESTIONS TO ASK YOUR CLIENT AND YOUR ADVERSARY TO PREPARE FOR PRESERVATION, RULE 26 OBLIGATIONS, COURT CONFERENCES AND REQUESTS FOR PRODUCTION (PUBLIC COMMENT DRAFT)

A Project of The Sedona Conference®
Working Group on Electronic Document
Retention & Production (WG1)

MAY 2008 (Subject to Periodic Updating)

The Sedona Conference® "Jumpstart Outline"

This outline was initially prepared by Ariana Tadler for The Sedona Conference® Institute's program entitled "Getting Ahead of the eDiscovery Curve: Strategies to Reduce Costs & Meet Judicial Expectations" held March 13-14, 2008 at The Westin Horton Plaza San Diego, San Diego, CA as an example of a tool to assist counsel in dealing with electronic discovery issues. The Sedona Conference® is seeking feedback on this outline as it is reviewed and used by practioners in real world discovery situations.

COMMENTS AND SUGGESTIONS SHOULD BE DIRECTED TO:
Ken Withers at:
The Sedona Conference®
5150 North 16th Street, Suite C 152
Phoenix, AZ 85016
(602) 258-2499 (Fax)
kwithers@sedona.net (e-mail)

Visit www.thesedonaconference.org

This outline sets forth, by way of example only, a series of topics and questions to ask your client and your adversary as you prepare for meeting obligations related to preservation, Rule 26, court conferences and requests for production. The answers to these questions will guide you in (i) instructing your client about its preservation and production obligations and (ii) understanding your adversary's systems and preservation efforts to date and then structuring your discovery requests addressed to your adversary. This is a simplified outline to assist, in particular, those people who have had only limited experience in dealing with electronic discovery. As those who have had extensive experience in this arena know, the process of questioning and even the questions themselves are iterative in scope. With each answer that you elicit, inevitably additional questions must be asked. Hopefully, having an outline like this within easy reach will serve as a "jumpstart" to encourage transparency and dialogue for a successful Rule 26(f) meet and confer.

1. Document Retention Policy

1.1. Do you have a document retention (or records management) policy? Is it a written policy?

1.1.1. If yes, when was the policy implemented?

1.1.2. If yes, is the policy enforced? By whom? How?

1.1.3. If yes, did the policy change during [insert relevant time period]?

1.1.4. If yes, are you willing to produce the policy/policies?

2. Key Custodians of Potentially Relevant Information

2.1. Given the facts of the case, who are the key custodians of potentially relevant information?

2.2. To what extent has information in the possession, custody or control of the key custodians been preserved? {Discuss what those efforts have been to date and what, if any additional efforts are underway.}

2.2.1. If conferring with your client, address efforts to date and further efforts that need to be made.

2.2.2. If conferring with your adversary, discuss efforts to date and, if insufficient and appropriate, request that further efforts, as discussed, be made.

2.3. Disclosure of identities of key custodians:

2.3.1. In representing your client, consider disclosing to your adversary the identities of the key custodians for whom information has been/will be preserved.

2.3.2. If you are a requesting party, consider identifying those people who you believe are key custodians to memorialize your request for preservation of their information.

NOTE: This is an iterative process. You should plan to confer with your adversary on a recurring basis so that you can continue to update your adversary on any additional key custodians.

3. Network Servers

The questions below concern current and former database and file servers on any potentially relevant network that now store or previously stored discoverable electronic data (hereinafter referred to as "network servers"). These questions should be asked of both your client and your adversary.

3.1. Do you use, for any purpose, a network-based system? If yes, please describe.

3.2. Do you have a system that serves to back up the information managed and/or stored on the network(s)?

3.2.1. If yes, do you have at least one computer (i.e., non-incremental) backup of each of your network servers for each month for the period [insert relevant time period]?

3.2.2. If not, for which months do you/do you not have at least one complete backup?

3.2.3. For those months, if any, for which you do not have a complete backup, do you have incremental backups or other backups from which a full backup can be created of all data as of a given date in each such month?

3.2.4. If so, please describe the nature of such incremental or other backups and identify the months for which you have them.

3.3. Can specific files contained on network backups be selectively restored?

3.3.1. How? By what means?

3.3.2. Have you ever done this before?

3.3.3. In what context? Is the context such that the data restored might be deemed relevant in the context of the current litigation?

3.4. As a matter of firm policy, do you overwrite, reformat, erase, or otherwise destroy the content of the backups of your network servers on a periodic basis?

3.4.1. If so, under what circumstances?

3.4.2. If so, what is the rotation period?

3.4.3. If the rotation period has changed since [insert date], please describe the changes.

3.5. Do you maintain a company-wide intranet or other database accessible to any or some employees that provides/stores potentially relevant information? [Consider being more specific, e.g., "regarding [a particular subject]."]

3.6. Do you maintain network servers at any or all of the Company's divisions/business units/locations/offices/subsidiaries that exist separately from or in addition to Company-wide server(s)?

3.6.1. If yes, to what extent do any of those servers store any potentially relevant information in the context of this litigation?

3.6.2. Ask follow up questions consistent with the network server-based questions above.

4. Email Servers

The questions below concern the current or former servers on your network ("email servers") that now or previously stored discoverable electronic internal or external peer-to-peer messages, including email, third party email sources, and instant messages (collectively, "email").

4.1. Identify the systems (client and server-side applications) used for email and the time period for the use of each such system, including any systems used at any [overseas] facilities.

4.2. Do you maintain email servers at any or all of the Company's divisions/business units/locations/offices/subsidiaries that exist separately or in addition to the Company-wide server(s)?

4.2.1. Are the systems the same/different from those identified in Question 4.1 above? Discuss any differences.

4.3. Are end-user emails that appear in any of the following folders stored on (i) the end-user's hard-drive, (ii) an email server, or (iii) a server of a third party application service provider:

4.3.1. "In Box"?

4.3.2. "Sent Items"?

4.3.3. "Delete" or "trash" folder?

4.3.4. End user stored mail folders?

4.4. If any of your email systems have changed since [insert relevant period], identify any legacy systems, the current system(s), and the date of the last backup made with each relevant legacy system.

4.5. Do you have at least one complete (i.e., non-incremental) back up of each of your email servers for each month [for the period _____ to _____]?

4.5.1. If not, for which months do you not have at least one complete backup?

4.5.2. For those months, if any, for which you do not have a complete backup, do you have incremental or other backups from which a full backup can be created of all data as of a given date in each such month?

4.5.3. If so, please describe the nature of such incremental or other backups and identify the months for which you have them.

4.6. Does each complete email backup contain all messages sent or received since creation of the immediately prior complete email backup?

4.6.1. Do your email backups contain the messages that are in each employee's "In Box" as of the time such backup is made?

4.6.2. Do your email backups contain the messages that are in each employee's "Sent Items" folder as of the time such backup is made?

4.6.3. Do your email backups contain the messages that are in each employee's "delete" or "trash" folder as of the time such backup is made?

4.6.4. Do your email backups contain the messages that are in each employee's stored mail folders as of the time such backup is made?

4.6.5. Do your email backups contain the messages that have been stored to each employee's hard drive?

4.7. Can specific email boxes contained on email backups be restored selectively?

4.7.1. Does the Company have or maintain an index or mapping resource that would serve as a reference to identify which employees' email is stored on particular backups?

4.8. As a matter of firm policy, do you overwrite, reformat, erase, or otherwise destroy the content of the backups of your email servers on a periodic basis?

4.8.1. If so, what is the rotation period?

4.8.2. If the rotation period has changed since [insert date], describe the changes.

4.9. Did you, at any time, have a system that maintained electronic copies of all emails sent or received by certain of your employees? Do you have such a system now?

4.9.1. If so, describe the system(s) and the date(s) of first use.

4.9.2. If so, does such system(s) contain copies of all mails captured from the date of first use until the present?

4.9.3. If so, does such system(s) capture a copy of all emails sent and/or received by employees in [identify relevant departments/groups that might be relevant]?

5. Hard Drives

The questions below concern the current and former local or non-network drives contained in current or former employees' laptop and desktop computers or workstations.

5.1. As a matter of firm policy, are employees' desktop and laptop hard drives backed up in any way?

5.1.1. If so, under what circumstances?

5.1.2. If so, how long are such backups retained?

5.1.3. Please describe the backup system.

5.2. As a matter of firm policy, are employees permitted to save files, emails or other data (excluding system and application generated temporary files) to their desktop or laptop hard drives?

5.3. Since [insert relevant date], has it been technically possible for firm employees to save files, emails, or other data (excluding system and application generated temporary .files) to their desktop or laptop hard drives?

5.4. Do you implement technical impediments to minimize the opportunity for employees to save files, emails or other data (excluding system and application generated temporary files) to their desktop or laptop hard drives?

5.4.1. Is it possible for employees to override such impediments?

5.5. To what extent has a search been done to determine the extent to which any of the key custodians in this litigation did, in fact, save files, emails or other data to their desktop or laptop harddrives? Flash drives?

5.6. As a matter of firm policy, are employees' desktop and laptop hard drives erased, 'wiped," "scrubbed" or reformatted before such hard drives are, for whatever reason, abandoned, transferred or decommissioned?

5.6.1. If so, are, as a matter of fm policy, files, emails or other data stored on such hard drives copied to the respective employee's replacement drive, if any.

5.6.2. If so, as a matter of firm policy, are such files, emails or other data copied on a "bit-by-bit" basis?

6. Non-Company Computers

6.1. Does company policy permit, prohibit or otherwise address employee use of computers not owned or controlled by the company to create, receive, store or send work-related documents or communications?

6.1.1. If so, what is that policy?

6.2. Is there any technical impediment to employees using computers not owned or controlled by the company to create, receive, store or send work-related documents or communications?