THE SEDONA CONFERENCE® WORKING GROUP SERIES℠

WGS℠

THE SEDONA CONFERENCE® "JUMPSTART OUTLINE":

Questions to Ask Your Client & Your Adversary to Prepare for Preservation, Rule 26 Obligations, Court Conferences & Requests for Production

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

MARCH 2011 VERSION

The Sedona Conference®

THE SEDONA CONFERENCE®
"JUMPSTART OUTLINE"

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

Author:
The Sedona Conference®

Editor-in-Chief:
Ariana J. Tadler

March 2011 Version

This outline was initially prepared by Ariana Tadler for The Sedona Conference® Institute's℠ program entitled "Getting Ahead of the eDiscovery Curve: Strategies to Reduced 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.
It was updated recently.

Thanks go to all who participated in the dialogue that led to this Commentary.
In addition, we thank all of our Working Group Series℠ Sustaining and Annual Sponsors, whose support is essential to our ability to develop Working Group Series℠ publications. For a listing of our sponsors just click on the "Sponsors" Navigation bar on the homepage of our website.

COMMENTS & SUGGESTIONS should be directed to:
Ken Withers at The Sedona Conference®
5150 North 16th Street, Suite A-215
Phoenix, AZ 85016
602-258-2499
kjw@sedonaconference.org

REPRINT REQUESTS:
Requests for reprints or reprint information should be directed to Richard Braman, Board Chair of The Sedona Conference®, at rgb@sedonaconference.org.

The Sedona Conference® Jumpstart Outline

Introduction

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, requests for production, court conferences, and Fed. R. Civ. P. 26. 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 (iii) structuring and tailoring 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 with extensive experience in this arena know, the process of questioning—and even the questions themselves—are iterative in scope. With each answer 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 in the discovery process, as contemplated by the Rules and The Sedona Conference® *Cooperation Proclamation.*

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? Who is responsible for maintaining/administering the company's electronic systems?

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, request that further efforts be made, if appropriate.

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.

2.4. Are there any third parties that may hold potentially relevant information?

2.4.1. To what extent has information in the possession, custody, or control of third parties been preserved? (Discuss what those efforts have been to date and what, if any, additional efforts are underway.)

2.4.2. If conferring with your client, address efforts to date and further efforts that need to be made with respect to third parties.

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

2.4.4. In representing your client, consider disclosing to your adversary the identities of the third parties for whom information has been/will be preserved.

2.4.5. If you are a requesting party, consider identifying those people who you believe are third parties that may have relevant data 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?

3.2.4. 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?

3.2.5. 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 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 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) backup 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 emails 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 hard drives? 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 firm 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 firm 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 firm to create, receive, store, or send work-related documents or communications?

The Sedona Conference® Working Group Series℠ & WGS℠ Membership Program

"DIALOGUE DESIGNED TO MOVE THE LAW FORWARD IN A REASONED & JUST WAY."

The Sedona Conference® Working Group Series℠ ("WGS℠") represents the evolution of The Sedona Conference® from a forum for advanced dialogue to an open think-tank confronting some of the most challenging issues faced by our legal system today.

The WGS℠ begins with the same high caliber of participants as our regular season conferences. The total, active group, however, is limited to 30-35 instead of 60. Further, in lieu of finished papers being posted on the website in advance of the Conference, thought pieces and other ideas are exchanged ahead of time, and the Working Group meeting becomes the opportunity to create a set of recommendations, guidelines or other position piece designed to be of immediate benefit to the bench and bar, and to move the law forward in a reasoned and just way. Working Group output, when complete, is then put through a peer review process, including where possible critique at one of our regular season conferences, hopefully resulting in authoritative, meaningful and balanced final papers for publication and distribution.

The first Working Group was convened in October 2002, and was dedicated to the development of guidelines for electronic document retention and production. The impact of its first (draft) publication—*The Sedona Principles: Best Practices Recommendations and Principles Addressing Electronic Document Production* (March 2003 version)—was immediate and substantial. *The Principles* was cited in the Judicial Conference of the United State Advisory Committee on Civil Rules Discovery Subcommittee Report on Electronic Discovery less than a month after the publication of the "public comment" draft, and was cited in a seminal e-discovery decision of the Southern District of New York less than a month after that. As noted in the June 2003 issue of Pike & Fischer's *Digital Discovery and E-Evidence, "The Principles*...influence is already becoming evident."

The WGS℠ Membership Program was established to provide a vehicle to allow any interested jurist, attorney, academic or consultant to participate in Working Group activities. Membership provides access to advance drafts of Working Group output with the opportunity for early input, and to a Bulletin Board where reference materials are posted and current news and other matters of interest can be discussed. Members may also indicate their willingness to volunteer for special Project Team assignment, and a Member's Roster is included in Working Group publications.

We currently have active Working Groups in the areas of 1) electronic document retention and production; 2) protective orders, confidentiality, and public access; 3) the role of economics in antitrust; 4) the intersection of the patent and antitrust laws; (5) *Markman* hearings and claim construction; (6) international e-information disclosure and management issues; and (7) e-discovery in Canadian civil litigation. See the "Working Group Series℠" area of our website www.thesedonaconference.org for further details on our Working Group Series℠ and the Membership Program.

Visit www.thesedonaconference.org