

The Sedona Conference “Jumpstart Outline”

Ariana J. Tadler
Kevin F. Brady
Karin Scholz Jensen



*Ariana J. Tadler, Kevin F. Brady, and Karin Scholz
Jenson**

THE SEDONA CONFERENCE “JUMPSTART OUTLINE”:

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

MARCH 2016 VERSION

Copyright 2016, The Sedona Conference. All
Rights Reserved.

This paper was originally presented at The 10th
Annual Sedona Conference Institute Program on
eDiscovery *Staying Ahead of the eDiscovery Curve:
Retooling Your Practice Under the New Federal Rules*,
held on March 17- 18, 2016, at Rancho Bernardo
Inn in San Diego, CA.



* The authors wish to thank members of The Sedona Conference Working Group 1 Steering Committee for their comments on this Outline. However, this Outline is the work of the three individual authors, and does not necessary represent the views of their respective employers, clients, or of Working Group 1. If you have any comments or suggestions for this Outline, please address them to comments@sedonaconference.org.

Introduction

This Jumpstart Outline sets forth, by way of example only, a series of topics and questions to consider asking yourself, your client, and your adversary (or opposing counsel) with respect to discovery obligations in litigation. Specifically, the answers to these questions should help guide you in (i) making the efforts necessary to comply with rules governing discovery, including the most recent December 1, 2015, amendments to the Federal Rules of Civil Procedure (the “Rules”); (ii) facilitating constructive discussions between outside and in-house counsel, record owners, and others who will be involved in satisfying preservation and production obligations; (iii) understanding the systems and preservation efforts of parties in the case; (iv) crafting a discovery plan; and (v) issuing and responding to requests for production, defending discovery decisions, and resolving or litigating discovery disputes. This is a simplified outline to assist, in particular, those people who have had only limited experience in dealing with electronic discovery. The process of questioning and even the questions themselves are iterative in scope. With each answer you elicit, additional questions may be warranted, and in some instances must be asked to best formulate a discovery process. Hopefully, having an outline like this within easy reach will serve as a “jumpstart” to encourage effective and efficient discovery, as well as cooperation, transparency, and dialogue in the discovery process, as contemplated by the Rules and The Sedona Conference *Cooperation Proclamation*.

Overview of Key Federal Rules

While this outline is not intended to be a primer on the Federal Rules of Civil Procedure,¹ the following provisions provide the backdrop and context for the outline:

- Discovery must be relevant to the claims or defenses and proportionate to the needs of the case. [FRCP 26(b)(1).]
- “Proportionate to the needs of the case” means that counsel and their client(s) should consider, from the outset of the case, what discovery is appropriate considering the importance of the issues at stake in the action, the amount in controversy, the parties’ relative access to relevant information, the parties’ resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit.
- The moving and reordering of the proportionality factors from Rule 26(b)(2)(C)(iii) “does not change the existing responsibilities of the court and the parties to consider proportionality, and the change does not place on the party seeking discovery the burden of addressing all proportionality considerations.” [2015 Advisory Committee Note to FRCP 26(b)(1).] However, the moving and reordering of the factors are intended to encourage parties to consider those factors that do apply and to determine how to formulate an efficient

¹ This document principally focuses on the application of the Federal Rules of Civil Procedure. Of course, lawyers must familiarize themselves with all applicable rules to ensure full compliance, including but not limited to local court and state court rules and practices, some of which may warrant a modified approach to the outline here.

and effective discovery plan that properly allows for the resolution of the parties' claims and defenses.

- References to discovery of “subject matter” and information “reasonably calculated to lead to the discovery of admissible evidence” have been deleted. A party may “deliver” requests for production of documents in advance of the Rule 26(f) conference, but responses are not due until 30 days after the Rule 26(f) conference. [FRCP 26(d)(2).] Requests so “delivered” are considered to have been served at the first Rule 26(f) conference. [FRCP 26(d)(2)(B).]
 - Parties should consider sending a letter or list to adversaries identifying specific topics/questions in advance of the Rule 26(f) conference.
- The parties must discuss any issues about preserving discoverable information. [FRCP 26(f)(2).] To facilitate this discussion, the parties should discuss the steps the parties took to identify and preserve evidence.
- Disputes regarding preservation, the scope of discovery, and any other matter contained in Rule 26(f) may be brought to the attention of the court in advance of the Rule 16 conference.
- The responding party is now required to either produce documents on the date specified in the requests or provide a specific date for when documents will be produced. If you intend to make a rolling production, you must state the dates on which the production will begin and end. [FRCP 34(b)(2)(B); 2015 Committee Notes.]
- If you make an objection, you must state specifically what you are withholding on the basis of that objection. You may satisfy this requirement by describing the search you will conduct. [FRCP 34(b)(2)(B) and (C); 2015 Committee Notes.]
- Rule 34(b)(1) still requires that a request describe with reasonable particularity each item or category of items to be inspected. [FRCP 34(b)(1)(A); 2015 Committee Notes].
- Parties may, and are encouraged to, identify the form or forms in which ESI is to be produced to facilitate an efficient discovery process. [FRCP 34(b)(1)(C).]
- Rule 34(b)(2)(B) now explicitly requires that for each item or category requested, the response must either state that inspection and related activities will be permitted as requested or state with specificity the grounds for objecting to the request, including the reasons. The December 1, 2015, amendment “eliminates any doubt that less specific objections might be suitable under Rule 34.” [FRCP 34(b)(2)(B); 2015 Committee Notes.]

Overview of Key Discovery Questions

In light of these requirements, litigants will normally want to have answers to at least the following basic questions:

- What written or unwritten information-related policies or practices are and/or were historically in place that might impact what relevant ESI is available, where that ESI is, and how that ESI had been/is best preserved and collected?
- What record owners are reasonably likely to have relevant ESI?
- Where is relevant ESI likely to reside?
- How will you meet the ethical obligations of competence regarding discovery?
- In the case of individual litigants and relevant custodians, what habits do they have that may impact the preservation of data (e.g., deleting a text message immediately after they send or read it, or posting, modifying, or deleting information from social media sites)?
- Who are the key custodians for each party, what are their roles, what relevant ESI are they expected to have, and what is the most effective and efficient method to ensure preservation of that relevant ESI?
 - Develop a list of key custodians for your client, as well as a list of those your client believes might be key custodians for the adversary, if possible.
 - Consider providing a list of key custodians to opposing counsel.
- What is/are the principal form(s) of communication utilized by the key custodians?
 - What system(s) or device(s) is/are used for relevant communications?
- What, if any, systems of reporting are utilized within the organization that would contain relevant information?
 - To what extent are reports generated by such systems?
 - To what extent can reports be generated by such systems?
- What reporting is utilized by an individual that would contain relevant information?
 - To what extent are reports routinely generated by such systems?
 - To what extent can reports be generated by such systems?
- What are the primary sources of relevant ESI that will assist in the resolution of the claims and defenses in the case, and who is the best person to advise and assist with preserving and/or collecting it?
 - How is data to be preserved/accessed/collected within an organization?

- What third parties (e.g., vendors or contractors) may have relevant information, and what is the best way to ensure that information is preserved and collected?
 - i. Consider the extent to which the party or the third party maintains possession, custody, and/or control of the data?
- If you represent an individual, how is data to be preserved/accessed/collected from sources the individual uses and controls, and what, if any, specific steps must be taken to preserve relevant information in the litigation?
- Do you need a vendor or expert to assist in preserving/accessing/collecting relevant data?
 - ii. NOTE: Appropriate methods of preservation/collection may differ depending on the types of metadata relevant to the claims and defenses in the case.
- What factual issues are undisputed and not necessary for discovery?
- What are the challenging places where relevant information might reside, such as structured databases, applications, proprietary platforms, or third-party ISPs or other cloud providers?
- Are there sources of relevant ESI that are likely to be lost (e.g., automatic deletion of email) if prompt steps are not taken to preserve them?

1. Information Governance

- 1.1. Written policies: Are there written policies that affect the creation, control, and retention of information in a way that might impact preservation or collection of relevant information? Depending on the issues in the matter, the following types of policies may be important:
- records retention/destruction schedules and policies
 - computer usage policy
 - electronic communications policy
 - mobile/tablet policy and/or bring-your-own-device (“BYOD”) program
 - social media policy
 - information security policy
 - privacy policy
 - backup tape storage/rotation policies
 - accessing data outside an organization
 - offboarding employee policies (e.g., policies that govern the disposition of documents/data of departing employees)
 - Health Insurance Portability and Accountability Act (HIPAA) policy

- 1.1.1. If yes for the relevant policies, when were they implemented? What changes, if any, occurred during the relevant time period? [NOTE: Attorneys should request that clients provide the policies in effect at all relevant times in the matter. Although it may be determined by the parties or the court that the policies need not be produced in the litigation, the information they reflect could help guide discussions with key custodians and the adversary.]
 - 1.1.2. How is compliance with each policy monitored, audited, and enforced? By whom?
 - 1.2. Unwritten procedures: Are there other practices or procedures at the company that affect the way information is maintained and accessed? Examples might include:
 - Automatic deletion of email by age or size of mailbox
 - Archiving of email
 - 1.3. To facilitate the required discussion about preservation, consider whether it is appropriate to ask your adversary at the Rule 26(f) conference about information-related policies that his or her client may have.

2. Custodians Most Likely to Possess Relevant Information

- 2.1. Given the facts of the case and the scope of the information that will be relevant to the claims or defenses, who are the custodians most likely to possess relevant information? Prioritize by importance. Key custodians are those with the more relevant information, while secondary and tertiary custodians may have limited or redundant information or information that relates to narrow topics.
- 2.2. How do/did these custodians create and store documents and/or this information?
 - 2.2.1. Consider how you will obtain the answer to this question: including a questionnaire with the litigation hold? Conducting in-depth interviews with some or all custodians? Discussions with records managers?
- 2.3. When did the duty to preserve relevant ESI arise? To what extent has relevant information in the possession, custody, or control of custodians been preserved?
 - 2.3.1. Determine as early as possible if any relevant information has been or is at risk of being lost, and if so, how to proceed.
 - 2.3.2. When conferring internally or with your client, address preservation efforts to date and further efforts that need to be made.
 - 2.3.3. When conferring with opposing counsel, discuss preservation efforts to date and, if insufficient, request that further efforts be made if appropriate.

2.4. Disclosure of identities of key custodians

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

2.4.1.1. Some names will be on your Rule 26(a)(1) disclosures, but some – such as secondary or tertiary custodians – may not be.

2.4.1.2. By voluntarily and cooperatively disclosing the identity of key custodians to facilitate ESI discussions, you need not concede they are automatically relevant for purposes of Rule 26(a)(1) disclosures.²

2.4.2. Consider identifying those people at the opposing party you believe are key custodians in order to memorialize your request for preservation of their information.

2.5. Third Parties

2.5.1. Are there third parties who have unique relevant ESI (i.e., non-duplicative information different from that maintained by the party)?

2.5.1.1. Could your adversary argue that your client was required to direct the third party to preserve information (for example, if the client outsourced a key area of business to the third party; the third party's documents are within the possession, custody, or control of the client; or an individual has an account with an ISP for email)?

2.5.1.2. If not, is there a reason or legal basis to direct a third party to preserve documents?

2.5.1.3. If not, is there a practical reason why you *want* the third party to preserve the relevant information?

2.5.1.4. Understand the contractual terms between your client and third parties that may impact preservation and potential access to information for discovery purposes (e.g., service level agreements ["SLAs"] related to data export).

2.5.2. To what extent has information in the possession, custody, or control of third parties been preserved?

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

² Initial disclosures, for example, pursuant to FRCP 26(a), often are limited to individuals that a party "may use to support its claims or defenses." Disclosure of other key custodians can facilitate efficient and effective discovery and may facilitate discussions relating to proportionality.

2.5.2.2. When conferring with your adversary, discuss efforts made to date, and if they are insufficient, request that further efforts be made if appropriate.

2.5.2.3. In representing your client, consider disclosing to your adversary the identities of the third parties for whom information has been/will be preserved or third parties for whom your client does not have “possession, custody, or control” of relevant data so that your adversary can take steps to preserve such data if the adversary believes the data is relevant to the case.

2.5.3. If you are a requesting party, consider identifying those people you believe are third parties who may have relevant data in order to memorialize your request for preservation of their information.

2.5.3.1. If you are a responding party and do not have Rule 34 “possession, custody, or control” over the third-party data or people identified, consider alerting your adversary so your adversary can take steps to preserve such third-party data if the adversary believes the data is relevant to the case.

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. Data Sources

Listed below are examples of “common” data sources for companies and individuals. This list should not be viewed as static, as new technologies are adopted continuously and each party has its own mix of data sources. In addition, even though a data source might exist, it is important to be thoughtful about whether information from the source is relevant to the claims or defenses and proportionate to the needs of the case. For example, collection from a smartphone may be critical in a sexual harassment case where it is alleged that the phone was used for the harassment, but it may not be relevant in a contract dispute.

A. Companies

3.1. For each data source, identify:

3.1.1. The individual(s) who could best provide detail regarding the use, preservation, and collection from the source

3.1.2. How the data exists as well as how it is backed up or archived (*see* Backup and Disaster Recovery in Section 4)

3.1.3. Whether the data stored is housed internally or storage and access are provided as a cloud solution

3.1.4. The date ranges of the data in the source

- 3.1.5. The manner used/needed to search, collect, and produce the data in a usable format
- 3.1.6. Any potential problems or limitations on production in discovery (e.g., data cannot be exported and viewed without a software license or proprietary software) and what, if any, alternatives exist to resolve such potential problems or limitations
- 3.2. File Servers (exclusive of supporting the data sources below)
 - 3.2.1. Determine the use and organization of any file servers, including allocation for use by individuals or departments or segmentation by topic or geography.
- 3.3. Messaging
 - 3.3.1. Identify each application used for internal and external messaging communications (e.g., email, instant messaging, mobile application messaging).
 - 3.3.2. For each application/archive, identify the potential export formats of the message content.
 - 3.3.3. For each application/archive, identify whether the data can be associated with a custodian and whether any organizational structure can be maintained upon export.
 - 3.3.4. Determine the extent to which custodians use personal email or PDAs to communicate and/or store information and the extent to which such information can be collected and how it will be collected.
- 3.4. Collaborative applications
 - 3.4.1. Identify each application used as a collaboration platform (e.g., SharePoint, company intranet).
- 3.5. Mobile devices
 - 3.5.1. Determine whether access is permitted to company information through the use of mobile devices (i.e., any portable device generally not defined as a laptop or a desktop computer). If so, what systems and information may be accessed by the mobile device?
 - 3.5.2. Does the company provide mobile devices for use by employees/contractors, or does it engage in a BYOD program?
 - 3.5.2.1. If BYOD, what agreements or practices, if any, have been put in place to allow the company access to the mobile device in the event of litigation, investigation, or other event?
 - 3.5.3. What steps does the company take to limit, control, and/or monitor the downloading and/or storage of company information on the mobile device (e.g., through the use of a mobile device management application)?

3.6. Structured databases

- 3.6.1. What investigation, if any, has occurred to identify relevant information that may exist in group/department or enterprise-level structured database systems?
- 3.6.2. Have subject matter experts been identified who can speak to the business and technical processes related to the databases?
- 3.6.3. What is the general process for extracting relevant information from the databases, and what are the available formats of any exports?

3.7. Workstations (i.e., laptop/desktop computers)

- 3.7.1. In general, what operating system(s) were utilized during the relevant period?
- 3.7.2. To the extent not specifically identified in the Information Governance section, identify and describe company policy directives that pertain to the storage of information on workstations during the relevant time period.
- 3.7.3. Does the company provide workstations for use by employees/contractors, or does it engage in a BYOD program?
 - 3.7.3.1. If BYOD, what agreements or practices, if any, have been put in place to allow the company to access the workstation in the event of litigation, investigation, or other event?
- 3.7.4. Identify any technical controls in place during the relevant time period that limit or prevent information from being locally saved, including a user's ability to override such controls.
- 3.7.5. Does the company have an asset management program that can associate workstations with employees or contractors during the relevant time period?
- 3.7.6. During the relevant time period, what has been the process for decommissioning, upgrading, reformatting, or otherwise destroying/recycling workstation hard drives?

3.8. Portable storage

- 3.8.1. Are portable storage devices (i.e., removable independent devices) such as USB drives and SD cards permitted by policy? What is the policy? If no policy exists, are there any technical controls that preclude the use of such devices (such as lack of USB or SD ports on the computer)?
 - 3.8.1.1. The fact that a policy does not exist does not necessarily mean that the use of such devices is prohibited. Inquire about the practice.
- 3.8.2. Does the company have an asset management program that can associate these devices with employees or contractors during the relevant time period?

3.9. Social media

3.9.1. Does the company maintain any type of social media presence?

3.9.2. If so, identify the platform(s), and for each:

3.9.2.1. Identify the period of use.

3.9.2.2. Identify the applicable information retention plan.

3.9.2.3. Identify whether the content is hosted internally or through an external platform.

3.9.2.4. Identify the department and personnel responsible for maintaining the presence and the content.

3.9.2.5. Assess the extent to which individuals use or are permitted or encouraged to use social media on behalf of or for the benefit of an organization.

3.10. Non-company computers (independent of section 3.7)

3.10.1. 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?

3.10.1.1. If so, what is that policy?

3.10.2. Are there any technical controls to limit employee/contractor use of computers not owned or controlled by the company to create, receive, store, or send work-related documents or communications?

3.10.3. To what extent has information been preserved or collected in the context of other litigation or litigation holds?

B. Individuals

3.11. For each data source, identify:

3.11.1. The individual(s) who could best provide detail regarding the use, preservation, and collection from the source

3.11.2. How relevant data exists as well as how it is backed up or archived (*see* Backup and Disaster Recovery in Section 4)

3.11.3. Whether relevant stored data is housed by the individual or storage and access are provided as a cloud solution

3.11.4. The date ranges of relevant data in a particular source

- 3.11.5. The manner used/needed to search, collect, and produce relevant data in a usable format
- 3.11.6. Any potential problems or limitations on production in discovery and what, if any, alternatives exist to resolve such potential problems or limitations
- 3.12. Depending on the type of matter, the following are potential sources of relevant data (if established, maintained, or used during the relevant time period):
 - 3.12.1. Personal devices used for sending or receiving emails or managing ESI, including personal computers, smartphones, and tablets; a listing of when such devices were purchased and utilized; the current location of same; and if they were disposed of, how and when
 - 3.12.2. Social media and networking accounts (include accounts where data is designated as “private”)
 - 3.12.3. Photo- and video-sharing sites established
 - 3.12.4. Device(s) that tracked and stored location data (like GPS data)
 - 3.12.5. Devices maintained or used for sending or receiving text messages
 - 3.12.6. Blogs or other online discussion forums
 - 3.12.7. Internet- or “cloud”-based services if used to store or back up relevant documents and data during the relevant time period
 - 3.12.8. Other stand-alone media capable of storing relevant ESI (i.e., thumb drives, CD-ROMs, DVDs, stand-alone hard drives, etc.)

NOTE: The above list of potential sources are examples of where relevant data might reside. Not all of these sources will be applicable in every case, therefore a specific inquiry should be made in each case.

4. Backup and Disaster Recovery

Depending on the circumstances, backup and disaster recovery systems may be sources of relevant data to be preserved, collected, and produced. Whether this is so must be determined in the context of an assessment of reasonably accessible versus not reasonably accessible data and the rules that govern each category in a particular case. The questions below apply individually and collectively to each data source identified as containing relevant information. Keep in mind that the terms “backup” and “disaster recovery” may not be synonymous within an organization. Some systems have data backed up exclusively for the purpose of recovering from a full system failure or true disaster. Others have data backed up for short- or long-term archiving, system performance and diagnostics, or other reasons. The business purpose often drives the backup protocol and architecture, which in turn informs potential burdens. Individuals also may back up data, including for their own “disaster recovery purposes,” some using systems that are specifically designed for

backup or copying data to another source (e.g., a thumb drive). Do you have a system that backs up information managed and/or stored by any of the data sources identified as containing potentially responsive information?

- 4.1.1. For each identified data source, what is the protocol for backing up the information?
 - 4.1.1.1. Schedule – daily, weekly, monthly, etc., including retention
 - 4.1.1.2. Type – full, incremental, differential
 - 4.1.1.3. Media – physical/virtual tape, disk, cloud
 - 4.1.1.4. What backups are available for the relevant time period?
- 4.1.2. Under what circumstances have you restored or do you restore information from backups?
- 4.1.3. For each identified data source, are there any gaps or exceptions in your normal backup retention?
- 4.1.4. What steps, if any, have you taken to suspend normal backup retention procedures?
- 4.1.5. Do any of the backup systems or processes store data in the cloud?
- 4.2. Can specific files/content contained on backups be selectively restored? Have you done this before, and if so, for what purpose?
- 4.3. As a matter of firm policy, do you overwrite, reformat, erase, or otherwise destroy the content of backups on a periodic basis?
 - 4.3.1. If so, what is the protocol, and has this changed since the relevant time period (include the nature of any changes)?

5. Ethical Obligations to Be Considered

In August 2012, the American Bar Association amended the comments to Rule 1.1 of the Model Rules of Professional Conduct to emphasize that to be competent, lawyers must “keep abreast of the changes in the law and its practice, including the benefits and risks associated with relevant technology ...”³ (Lawyers include both in-house and outside counsel.) A number of states have amended their rules of professional conduct to follow the changes announced by the ABA in August 2012, and one state even has issued an ethics opinion regarding steps lawyers should take in handling e-discovery.⁴

³ ABA Model Rules of Professional Conduct Rule 1.1 cmt [8] (2013).

⁴ For example, on June 30, 2015, the State of California Standing Committee on Professional Responsibility and Conduct issued Formal Opinion No. 2015-193 (“CA Formal Opinion No. 2015-193”), which addressed a number of issues regarding an attorney’s ethical duties in the handling of discovery of ESI.

5.1 For purposes of the Jumpstart Outline, you should assess whether you have the requisite skill and knowledge, including *understanding the benefits and risks of the technology involved*, to perform the following tasks (either by yourself or in collaboration with an experienced counsel or consultant):

- assess e-discovery needs of the case in terms of your client's claims and the adversary's defenses.
- analyze and understand your client's ESI record retention policies, systems, and storage.
- advise your client on available options for identification, preservation, collection, and production of ESI.
- assist your client in identifying sources (including custodians) of relevant ESI.
- engage in meaningful meet and confer sessions with opposing counsel concerning an e-discovery plan.
- advise your client about the proper method to collect responsive ESI in a manner that preserves the integrity of that ESI for evidentiary purposes.

5.2 In certain situations, it also may be advisable to associate with or consult technical consultants, experts, or counsel who specialize in e-discovery issues or particular technologies.⁵

⁵ See CA Formal Opinion No. 2015-193. See also, fn. 3, *supra*.