wgs

The Sedona Conference

Primer on Managing Electronic Discovery in Small Cases

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

December 2022
Public Comment Version
Submit comments by February 12, 2023, to
comments@sedonaconference.org

The Sedona Conference Primer on Managing Electronic Discovery in Small Cases

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

PUBLIC COMMENT VERSION

Author: The Sedona Conference

Drafting Team Leaders

Greg M. Kohn
Trena M. Patton

Drafting Team Members

Hon. Jerome B. Abrams
Kevin M. Clark
Hon. Alice R. Senechal
Gary Soliman
Sean Broderick
Michael J. Scimone
David B. Seserman

Steering Committee Liaisons

Kimberly J. Duplechain
Greg M. Kohn
Martin T. Tully
Tara S. Emory
Amy Sellars

Staff Editor: David Lumia

Preface

Welcome to the December 2022 Public Comment Version of *The Sedona Conference Primer on Managing Electronic Discovery in Small Cases ("Primer")*, a project of The Sedona Conference Working Group 1 on Electronic Document Retention and Production (WG1). This is one of a series of Working Group commentaries published by The Sedona Conference, a 501(c)(3) research and educational institute dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation, intellectual property rights, and data security and privacy law. The mission of The Sedona Conference is to move the law forward in a reasoned and just way.

The intent of this *Primer* is to offer best practices and practical guidance tailored to cases involving smaller quantities or less complex varieties of electronically stored information (ESI) or in which the smaller stakes involved significantly limit the time and money that can and should be spent on electronic discovery. In the interest of the underlying concept of proportionality—tailoring eDiscovery efforts to fit the particular circumstances of the case and resources at hand—some of the guidance provided may diverge from what The Sedona Conference recommends for large, complex cases. But just as in larger cases, cooperation between parties remains central in efficiently managing discovery in small cases and meeting the mandate of Federal Rule of Civil Procedure 1: The just, speedy, and inexpensive determination of every action and proceeding.

This project began with the formation of a brainstorming group in 2018. The passage of time leading to this publication is a reflection of the huge volume and variety of small cases and the difficulty in arriving at common-sense approaches that can be applied uniformly. There is no "one size fits all." The *Primer* was the topic of dialogue at the 2018 Working Group 1 Annual Meeting, the 2019 Midyear and Annual meetings, and, after considerable reworking, the 2022 Annual Meeting. Previous drafts of the *Primer* were published for member comment in both 2019 and 2022, and this public comment version reflects the valuable input provided by Working Group members.

On behalf of The Sedona Conference, I thank drafting team leaders Greg Kohn and Trena Patton for their leadership and commitment to the project. I also recognize and thank drafting team members the Honorable Jerome Abrams, Sean Broderick, Kevin Clark, Michael Scimone, the Honorable Alice Senechal, David Seserman, and Gary Soliman for their dedication and contributions, and Steering Committee liaisons Kimberly J. Duplechain, Tara Emory, Greg Kohn, Amy Sellars and Martin Tully for their guidance and input. I also thank Stephanie Mitchell and Sonali Ray for their contributions.

Please note that this version of the *Primer on Managing Electronic Discovery in Small Cases* is open for public comment through February 12, 2023, and suggestions for improvement are very welcome. After the deadline for public comment has passed, the drafting team will review the public comments and determine what edits are appropriate for the final version. Please submit comments by email to comments@sedonaconference.org.

In addition, we encourage your active engagement in the dialogue. Membership in The Sedona Conference Working Group Series is open to all. The Series includes WG1 and several other Working Groups in the areas of international electronic information management, discovery, and disclosure; patent remedies and damages; patent litigation best practices; trade secrets; data security and privacy liability; and other "tipping point" issues in the law. The Sedona Conference hopes and anticipates that the output of its Working Groups will evolve into authoritative statements of law, both as it is and as it should be. Information on membership and a description of current Working Group activities is available at https://thesedonaconference.org/wgs.

Craig Weinlein
Executive Director
The Sedona Conference
December 2022

Table of Contents

I. INTRODUCTION

For years, members of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1) have urged the development of a publication on electronic discovery best practices tailored to "small cases"—that is, matters involving little electronically stored information (ESI) and/or where the stakes significantly limit the time and money that realistically can or should be spent on electronic discovery. In response, WG1 has spent what seems to be as many years developing this *Primer on Managing Electronic Discovery in Small Cases (Primer)*. Compared to the effort required to publish papers addressing the challenges of discovery in large, complex litigation, the topic of small cases might seem a minor thing to tackle. It has proved to be anything but.

To begin, most cases are small cases, and most of those are pending in state courts.[1] The sheer volume and variety of small cases make it difficult to offer a singular approach. Unlike larger cases where the financial or public policy stakes are higher, the cost and burden of employing the latest and greatest ESI preservation and production practices may not be necessarily proportional to the needs of a small case or consistent with "the just, speedy, and inexpensive determination of every action and proceeding."[2] Indeed, proportionality is—at bottom—all about tailoring and scaling eDiscovery efforts to fit the particular circumstances, capabilities, and resources at hand. Sometimes, one can only do what one can with the resources available, even if they might not be necessarily considered reasonable or defensible in larger matters or different contexts. For this reason, students of other Sedona Conference publications may perceive some of the shortcuts and "MacGyver" solutions discussed in this *Primer* as somewhat at odds with the sage guidance offered in previous papers.[3] Rest assured, The Sedona Conference and the drafting team for this *Primer* continue to heartily endorse those prior papers and best practices and have tried to acknowledge where the suggestions herein may diverge from previous guidance out of practical necessity and based on proportionality considerations. The drafting team merely acknowledges that, in some circumstances, "best practices" themselves might not be proportional to the needs of the case or the means of the parties.

Along with proportionality and the mandate of Federal Rule of Civil Procedure 1, the most important principle in discovery in cases of any size is cooperation, and this *Primer* reinforces and elevates the central role of cooperation in effectively and efficiently managing discovery in small cases.[4]

---

1 This *Primer* largely references the Federal Rules of Civil Procedure (Rules 1, 26, 34, etc.), but recognizing that many small cases are litigated in state court, the Primer focuses on general principles that apply across various rules of court and on concepts common in most jurisdictions. Practitioners should consider whether the rules vary in their venues in ways that are significant to the topics discussed.

2 FED. R. CIV. P. 1.

3 Merriam-Webster.com defines "MacGyver" as a verb meaning "to make, form, or repair (something) with what is conveniently on hand."

4 The Sedona Conference, *The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production*, 19 SEDONA CONF. J. 1, 125 (2018) [hereinafter *The Sedona Principles, Third Edition*] ("In addition to what is required by those Rules, it is generally in the best interests of the responding party to engage in

Indeed, "[i]f both requesting and responding parties voluntarily elect to cooperatively evaluate and agree upon the appropriate procedures, methodologies, and technologies to be employed in the case, both may potentially achieve significant monetary savings and non-monetary efficiencies."[5] In short, the parties' informed agreements on the conduct of discovery can become the de facto best practices as tailored to the matter. Of course, flexibility in electronic preservation and production requires superior communication among the parties. While each party remains in full control of its own destiny,[6] where best practices are departed from out of necessity, efficiency may more likely be achieved through clear communication by the parties about expectations and intentions for discovery processes, involving disclosure,[7] and if possible, the endorsement of the other party.

As always, however, cooperation may not work in every case, particularly in matters that involve shorter timeframes for negotiating and completing the discovery process. Where the parties cannot reach agreement, thoughtful proportionality arguments will be critical in the event a party must seek judicial support for its proposed electronic discovery approach.[8]

Without doubt, the volume of ESI in the possession of both organizations and individuals increases each year. Cases that would have had little electronic evidence years ago may now require more significant electronic discovery. This *Primer* offers suggestions for managing electronic discovery costs and efforts in proportion to the needs of a small case. In short, the *Primer* embraces a need for bespoke flexibility in small cases that may not be appropriate in other, especially larger, matters. Lest practitioners feel that The Sedona Conference has made "the perfect the enemy of the good," this *Primer* acknowledges the primacy of proportionality, cooperation, and communication as the guiding principles in efficient and cost-effective discovery, particularly when it comes to small cases. The *Primer* also identifies some low- or no-cost tools and technologies that can help meet small case needs when on a tight budget.

---

meaningful cooperation with opposing parties to attempt to reduce the costs and risk associated with the preservation and production of ESI.").

5 *Id.*

6 *Id.* at 118. ("[T]he case law and the procedural court rules provide that discovery should take place without court intervention, with each party fulfilling its discovery obligations without direction from the court or opposing counsel.").

7 *See* FED. R. CIV. P. 26(a), (f).

8 *The Sedona Principles, Third Edition*, *supra* note 4, at 118.

II. WHAT CONSTITUTES A "SMALL CASE"?

This *Primer* is intended to provide guidance to attorneys, parties, and judges in matters that are not large or complex in order to meet the directive of Rule 1 (and its state counterparts) that the Federal Rules of Civil Procedure be "construed, administered, and employed by the court and the parties to secure the just, speedy and inexpensive determination of every action and proceeding." Although the majority of cases implicate ESI, the complexity and expense of electronic discovery can undermine the goals of Rule 1 and the proportionality considerations of Rule 26(b)(1).[9] This may be particularly true in a "small case," regardless of how that term is defined.

Courts have tried to define a "small case" either by the amount in controversy or the type of case. Both of these methods can be helpful to define a small case, but each has shortcomings. Some jurisdictions have implemented rules that limit discovery based upon the relief sought.[10] For example, Utah's Rules of Civil Procedure employ a tiered structure for discovery, based on the amount in controversy identified in the complaint: Tier 1 ($50,000 or less), Tier 2 ($50,001 to $299,999 or nonmonetary relief), and Tier 3 ($300,000 and above).[11] The tiers are easy to apply, but the approach may undervalue the complexity or the importance of the issues involved in the case. A relatively simple collection matter seeking $300,000 or more would be classified as Tier 3, although there may be little or no electronic discovery necessary; a claim for nonmonetary relief could be considered Tier 2 even though it may implicate public policy and, therefore, require significant electronic discovery. A study of Utah's rule change suggests that practitioners may now be increasing the amount in controversy claimed in the complaint to secure classification at a higher tier with a broader scope of discovery.[12]

The Arizona Rules of Civil Procedure use the case classification method. Arizona also uses a three-tier system, although tiers are not based solely on the relief requested.[13] Instead, the tier to which a case is assigned is "determined by either: (1) stipulation or motion, for good cause shown; (2)

---

9 Under Rule 26(b)(1), the parties are entitled to discovery of matters "relevant to a party's claim or defense and proportional to the needs of the case." The Rule directs that six factors be considered in determining proportionality: "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." FED. R. CIV. P. 26(b)(1). *See also* The Sedona Conference, *Commentary on Proportionality in Electronic Discovery*, 18 SEDONA CONF. J. 141 (2017).

10 *See* UTAH R. CIV. P. 26(c)(5), Tex. R. Civ. P. 190.

11 UTAH R. CIV. P. 26(c)(5).

12 NATIONAL CENTER FOR STATE COURTS CIVIL JUSTICE INITIATIVE, UTAH: IMPACT OF THE REVISIONS TO RULE 26 ON DISCOVERY PRACTICE IN THE UTAH DISTRICT COURTS 3 (April 2015), *available at* utah-rule-26-evaluation-final-report2015.pdf (ncsc.org).

13 ARIZ. R. CIV. P. 26.2.

placement by the court based on the characteristics of the case; or (3) the sum of the relief sought in the complaint, and any counterclaims or crossclaims."[14]

Under the Arizona method, Tier 1 cases are "simple cases that can be tried in one or two days," such as automobile tort, intentional tort, premises liability, and insurance coverage claims.[15] These are cases with "minimal documentary evidence and few witnesses."[16] These cases will benefit from the strategies in this *Primer*. Under the Arizona rule, a $300,000 collection case would be classified as Tier 1 because it involves minimal evidence, a few witnesses, and can be tried in one or two days.

Tier 2 cases have "intermediate complexity" and likely involve more than minimal documentary evidence and more than a few witnesses (and may include expert witnesses).[17] Tier 2 cases are likely to involve multiple theories of liability and may involve counterclaims or cross-claims.

Tier 3 cases are logistically or legally complex, such as class actions, antitrust, multiparty commercial or construction cases, securities cases, environmental torts, construction defect cases, medical malpractice cases, product liability cases, and mass torts.[18] These cases may have voluminous documentary evidence, or numerous pretrial motions raising difficult or novel legal issues. Tier 3 cases also require management of a large number of witnesses or separately represented parties or coordination with related actions pending in other courts.[19]

Rather than relying on arbitrary or bright-line rules offered above to define a "small case," the parties should discuss the discovery needs of the case prior to but no later than the Rule 26(f) conference or state court equivalent. The parties should consider all aspects of the case and not focus solely on the amount of monetary relief in controversy or the type of case.[20]

This *Primer* offers the following nonexhaustive list of factors for initial discussion among counsel before the scheduling conference and that should be considered throughout the litigation:

- the proportionality factors, including nonmonetary factors.
- the parties' and counsel's familiarity with the facts and issues involved.

---

14 *Id.*, 26.2(c).

15 *Id.*, 26.2(b)(1).

16 *Id.*

17 *Id.*, 26.2(b)(2).

18 *Id.*, 26.2(b)(3).

19 *Id.*

20 *See* FED. R. CIV. P. 26(b).

- whether the parties and counsel have a reasonable understanding of the scope of necessary discovery.

- whether the parties and counsel have a reasonable understanding of potentially discoverable ESI that might be available.

- whether the documentary evidence is minimal versus "document-intensive."

- whether the subject matter of the case involves a short and discreet time period, since cases involving longer time periods typically involve more potentially discoverable ESI.

- the number of anticipated custodians of ESI and the number of anticipated devices that may contain potentially discoverable ESI.

Consideration of the factors above will help the parties and courts determine the applicability-of the strategies in this *Primer*.

III. PROPORTIONALITY CONSIDERATIONS FOR A SMALL CASE

Various aspects of discovery give rise to different burdens, and proportionality considerations may justify creative workarounds for some aspects of discovery within the same case. To understand the burden mitigated by any particular "small case" strategy, it is incumbent upon counsel to understand the difference between such a strategy and ostensible requirements under the discovery rules; be able to quantify that burden, if necessary; and be able to determine that the burden avoided by their client justifies the resulting difference in what is ultimately produced to the requesting party in light of the proportionality factors.[21]

For example, Rule 34(b)(2)(E) requires that ESI be produced in a form requested or, if none is provided, "in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms." This requirement may present a helpful starting point for cooperation in small cases because a form of production that is objectively usable (and likely necessary) in standard cases may not actually be what a requesting party wants to receive in a small case. While a standard ESI production often involves files in a format intended to load into a review platform, a requesting party in a small case may prefer standalone PDFs[22] or native format even if such a production would not contain the information (e.g., metadata) contained in a standard production.

Counsel in small cases must carefully decide whether adaptations to mitigate costs are justified in light of the needs of the case, including the likely benefit that would be achieved if a more standard approach were taken. Even in small cases, it is possible that the tools and methods employed—particularly for collecting, processing, and producing ESI—may result in problems later in the case or deprive the requesting party of necessary information. In particular, processes that may alter or destroy metadata may affect whether the evidence can be authenticated later and how it can be used.[23]

The court shares the obligation with the parties of ensuring proportional discovery. Where it is available, it is helpful to have the assigned judge guide the parties to the appropriate scope of discovery by implementing case management policies and procedures.[24] The court and counsel should continue to evaluate and adjust the scope of discovery whenever it is reasonable to do so.

---

21 *See* Sung Gon Kang v. Credit Bureau Connection, Inc., No. 18-CV-01359, 2020 WL 1689708, at *5 (E.D. Cal. Apr. 7, 2020) ("These conclusory, unsupported statements are insufficient to meet Defendant's burden").

22 PDF: Portable Document Format, *The Sedona Conference Glossary: eDiscovery & Digital Information Management, Fifth Edition*, 21 SEDONA CONF. J. 263, 353 (2020) [hereinafter *The Sedona Conference Glossary, Fifth Edition*].

23 *See The Sedona Principles, Third Edition*, *supra* note 4, at 169.

24 *See* FED. R. CIV. P. 26(b)(2)(C); *see also* Webinar: Civil Justice Initiative, *It's All About Teamwork: Creating Effective Civil Case Management Teams*, https://www.ncsc.org/Microsites/Civil-Justice-Initiative/Home/Webinars.aspx.

IV. SMALL-CASE TAILORED ELECTRONIC DISCOVERY TIPS

The Sedona Principles, Third Edition[25] contains broad guidance on electronic discovery applicable to civil cases in general. Some aspects of *The Sedona Principles, Third Edition* are particularly salient in small cases. Accordingly, this section focuses on the pragmatic application of those Principles to small cases, including examples of how they might be applied to suit the circumstances of the matter and the resources of the parties.

The focus in small cases is conducting discovery in the most efficient and cost-effective manner. Clients in small cases often are unable or unwilling to budget for expensive processes, a problem that is not unique to electronic discovery. As Sedona Principle 1 makes clear, ESI is generally subject to the same preservation and discovery requirements as other relevant information.[26] What makes ESI different, and at times very burdensome, is its quantity and complexity.

In small cases, discovery is more effective if the parties can simplify the identification and production of relevant ESI and employ strategies to address the volume of ESI as well as the cost of preservation, review, and production. The tips in this *Primer* are geared toward these goals.

A. Early Client Engagement and Process Education

Many parties engaged in small cases may not have experience with litigation or electronic discovery and are often unfamiliar with the process and requirements. This is particularly true when the client is a small organization or an individual. Small organizations may not have a general counsel or information technology (IT) staff; individuals often have no formal organizational "system" for keeping and preserving documents or ESI. Instead, they may simply have devices and systems that they use and interact with as part of their daily routine. In these instances, it is imperative that practitioners educate clients as soon as litigation is reasonably anticipated and throughout the case so that they understand their discovery obligations and can work with counsel to identify and explore options for reasonable and proportional discovery solutions for their small case.

1. Make ESI part of the earliest discussions about the case

At the outset of the case, counsel should inform the client of the obligation to locate and preserve relevant ESI. Counsel should also be sure that the client understands the scope of relevant ESI and the method of preserving ESI in each of the storage locations identified. Many individuals and small organizations may not even be aware of the types and sources of ESI that they possess or have access to, so early communication and discussion on these topics are essential.

---

25 *The Sedona Principles, Third Edition*, *supra* note 4.

26 *Id.*, at 56.

2. Conduct custodian interviews

When dealing with an organization, it is important to identify the employees and representatives who have information relevant to the asserted claims and potential defenses. Where possible, speaking with them in real time helps to ensure that sources of discoverable material are properly identified and understood by the client and counsel. When speaking with a custodian about relevant data sources, counsel should ask searching questions to identify where data is located—an essential first step in determining options to access and collect. An excellent and thorough reference point is *The Sedona Conference "Jumpstart Outline."*[27] It may be valuable to spend some time tailoring or simplifying the questions suggested in the *Jumpstart Outline* to fit the scope of the issues in the case or the client's data sources.

For cases involving several custodians or if circumstances do not permit contemporaneous custodian interviews, counsel may use a standardized written questionnaire for some or all custodians—similar to client interrogatories. At minimum, a conversation with someone familiar with the relevant data sources at the outset of the case can provide counsel with valuable information about relevant ESI and save time and expense at later points in the case.

3. Preservation/Legal Hold

Counsel should educate clients on the need for and methods of reasonably preserving relevant ESI. This should be discussed early to avoid disputes, potential spoliation, and avoidable litigation costs down the road. If the client is an organization, the client should consider the need to send a formal legal hold notice to employees and non-parties who maintain or possess the client's data and records.[28] Here again, "principles of proportionality should be applied when the costs and burdens of preserving large amounts of ESI may be disproportionate to the needs of the case, and even the sole copy of an ESI item need not be preserved if doing so would be disproportionate to the needs of the case."[29] As such, a party's duty to preserve relevant evidence does not require the freezing of "all documents" and ESI, even if relevant.[30]

---

27 Ariana J. Tadler, Kevin F. Brady & Karin Scholz Jenson, *The Sedona Conference "Jumpstart Outline"* (2016), https://thesedonaconference.org/publication/Jumpstart_Outline.

28 *See* Alter v. Rocky Point Sch. Dist., No. 13-1100, 2014 WL 4966119, at *8 (E.D.N.Y. Sept. 30, 2014). *See also The Sedona Principles, Third Edition*, *supra* note 4, at 107 ("Parties should also consider whether some preservation notice should be sent to third parties, such as contractors or vendors, including those that provide information technology services.").

29 *Id.* at 94–96.

30 *See*, *e.g.*, *id.*, at 111, Comment 5.g. ("A party's preservation obligation does not require 'freezing' of all ESI, including all email. Parties need not preserve 'every shred of paper, every e-mail or electronic document, and every backup tape,' nor do they have to go to extraordinary measures to preserve 'all' potentially relevant ESI.") (citing Zubulake v. UBS Warburg, LLC, 220 F.R.D. 212, 217 (S.D.N.Y. 2003)).

Regardless of the form or simplicity of the legal-hold notice, follow-up by counsel is essential to ensure compliance with preservation instructions. Especially in small cases, counsel should never assume that the client has taken steps to preserve relevant ESI. Small organizations and businesses are unlikely to have a formal records retention policy or information governance program, and individuals' organizational systems will vary widely. Instead, counsel should help the client understand how their systems and devices retain and delete data to determine if retention settings need to be adjusted. Examples include changing mailbox size, suspending auto-delete, or enlarging retention periods.

The involvement and direction of counsel is particularly important when the client is an individual. Individuals may rely heavily on devices like smartphones, cloud storage, and laptops that can be lost, broken, or use auto-delete settings. Counsel should consider obtaining backups of clients' devices—including supervising and documenting the process—to avoid any potential spoliation issues that might occur after the preservation obligation is triggered.[31] Many smartphone users automatically back up device data to a cloud service. Clients who do not use cloud backups for their devices should consider doing so during the pendency of litigation (and for data over the relevant time period), as doing so mitigates the risk of data loss and may lessen the need for more expensive methods of preserving data from mobile devices. At the same time, some clients may need to turn off backups to avoid overwriting an existing backup that may contain unique and relevant information, until the existing backup can be copied.

The aforementioned preservation methods are less thorough than complete forensic imaging, which would also capture logged information like location data that may not be captured by a simple backup. Counsel should engage in a proportionality analysis to determine whether forensic imaging is important to the specific needs of the case. If that analysis shows that forensic imaging (or equivalent preservation method) is not warranted, counsel should consider proactively raising that preservation issue with opposing counsel at the 26(f) conference to avoid later disagreements. It is also important to keep in mind that the cost of eDiscovery services is constantly changing, so counsel should not assume that forensic imaging or other preservation steps are cost prohibitive.

For litigants with older technology and devices, preservation of data on broken/obsolete equipment may be especially important. The client may not have a backup system and may be more likely to use a device to the breaking point rather than upgrade systems that are nearing the end of their usable life.

4. Consider the pros and cons of collection for preservation, as compared with preservation-in-place

In small cases, proportionality must play an important role in determining the reasonable scope of preservation and avoiding the potential costs associated with some forms of collection. In some cases, early collection of ESI may be the appropriate preservation strategy. Collection efforts might

---

[31] *See, e.g.*, Barton & Assocs., Inc. v. Liska, No. 9:19-CV-81023, 2020 WL 8299750, at *2 (S.D. Fla. May 11, 2020).

include exporting a key custodian's email account as an Outlook PST[32] file or making a copy of the data on a client's cell phone. Collection for preservation is an important strategy if counsel cannot be sure that the client will undertake appropriate preservation measures, or where the only source of information is a device with some risk of loss or destruction.

When the client is an individual, the collect-to-preserve strategy mitigates the risk that the client is not capable of taking "reasonable" preservation steps as defined in the federal rules and interpreted by the courts. An additional benefit of collecting relevant ESI at the outset of a case is that it may eliminate the need to revisit these data sources with the client for collection later (assuming that new discoverable information will not be created). Early collection may also help counsel prepare for the meet-and-confer process by providing concrete information about the client's data types and volume.

Alternatively, preservation-in-place—i.e., the practice of taking steps to ensure data is preserved where it is stored—may be a more appropriate preservation method, particularly when the likelihood of the ESI being destroyed or lost is low. Factors to consider in weighing the best preservation method include whether the method would impose storage costs (beyond those already allocated by the custodian), whether it would require forensic resources, or whether it would be less convenient than alternatives (for example, where a user's device must be taken into custody). Keep in mind that if discoverable information may be created during the life of the case, collection (or backup) at a single point in time may require counsel to perform additional collection steps later in the case.

Cloud-based storage is also important to consider. Most bank accounts, phone accounts, payment histories, and similar services generally offer their users access options that can help identify relevant data, such as filtering and sorting tools. At the same time, these accounts may have deletion schedules, so if these accounts will be important to the case, counsel should ensure that those records are otherwise preserved, which may call for early collection or proactive communication with third-party service providers to ensure the information is not deleted or destroyed.

Some applications owned or used by clients may already contain tools and functionality designed for eDiscovery purposes. For example, enterprise platforms like Microsoft 365 increasingly include eDiscovery tools that may be used to search for content in other platforms or applications. Users can also search mailboxes and sites by using built-in tools to identify, hold, and export content found in such mailboxes and sites.[33] These built-in eDiscovery solutions do have limitations, however, and their capabilities can vary based on licenses, client configurations, and other technical limitations. Counsel should be aware of the capabilities and limitations when using such solutions for preservation, search, and production of ESI in litigation matters of any size.

---

[32] PST: A Microsoft Outlook email storage file containing archived email messages in a compressed format, *The Sedona Conference Glossary, Fifth Edition*, *supra* note 22, at 357.

[33] *See* Microsoft Purview eDiscovery Solutions, MICROSOFT, https://docs.microsoft.com/en-us/microsoft-365/compliance/ediscovery?view=o365-worldwide.

Text messages from mobile devices are often targets for electronic discovery in litigation and investigations. Failure to preserve and produce relevant mobile device data can result in serious consequences.[34] As discussed in Section V below and the *Primer*'s Appendix, several tools might be helpful to inexpensively collect ESI from mobile devices and generate copies of text message communications.

Beyond email and text messages, new challenges are posed by burgeoning social media and messaging environments, expanded use of ESI stored on collaborative platforms, and other cloud applications and storage. Such environments may require advanced tools and training to manage complex search, collection, and processing efforts.[35] In all cases, counsel will need to identify relevant ESI within these sources as well as cost-effective ways of retrieving or representing it in a reasonably defensible manner. As noted above, it may be cost-effective to investigate the search and export capabilities that already exist within the platform.

5. Consider the Pros and Cons of Properly Supervised Self-Collection vs. Other Options

Numerous articles and reported decisions have outlined the risks to both clients and attorneys from the self-identification or self-collection of discoverable ESI by custodians, especially if they are interested parties.[36] The case law is clear that self-collection of ESI by a client raises a real risk that data could be destroyed (including metadata in the collection process), altered, or otherwise corrupted. Indeed, there are many dangers inherent in self-collection, including good-faith omission by inadvertence, insufficient diligence, or lack of technical or legal training.[37] To be sure, a custodian or its IT professional may not possess the knowledge of how to collect data in a manner that avoids

---

34 *See, e.g.,* Paisley Park Enters. v. Boxill, No. 0:17-cv-01212, 2019 WL 1036058 (D. Minn. Mar. 5, 2019) (Court found the defendants acted with "the intent to deprive" in failing to preserve text messages when they failed to make reasonable efforts to preserve their data and admonished them for their "troubling" and "completely unreasonable" behavior.); Christou v. Beatport, LLC, 849 F. Supp. 2d 1055 (D. Colo. 2012) (Court sanctioned defendant for not taking steps to preserve text messages, which led to a spoliation sanction.).

35 "Costs and risks may increase if the technology makes it more difficult to preserve or collect relevant ESI for litigation. For example, mobile devices that are not synchronized with the organization's servers may require physical collection of the mobile device to meet preservation or discovery obligations if there is unique, relevant ESI on the device that the IT or legal group cannot collect from the organization's servers." *The Sedona Principles, Third Edition*, *supra* note 4, at 63.

36 *See, e.g.,* Equal Emp't Opportunity Comm'n v. M1 5100 Corp., No. 19-cv-81320, 2020 WL 3581372 (S.D. Fla. July 2, 2020) (Explaining reasons why attorneys should not allow clients to self-collect potentially relevant ESI.); Nat'l Day Laborer Org. Network v. U.S. Immigration and Customs Enf't Agency, 877 F. Supp. 2d 87 (S.D.N.Y. 2012) ("Searching for an answer on Google (or Westlaw or Lexis) is very different from searching for *all* responsive documents in the FOIA or e-discovery context . . . " and "most custodians cannot be 'trusted'" to effectuate a legally sufficient collection.).

37 *See, e.g.* Green v. Blitz U.S.A., Inc., 2011 WL 806011, 2:07-CV-372 (TJW), at *6, n.5 (E.D. Tex. Mar. 1, 2011) ("That Blitz put someone in charge of its discovery who knows nothing about computers does not help Blitz's effort to show that it was reasonable in its discovery obligations.").

spoliation of file contents and its metadata. Further, as discussed in Section III.F.2, below, self-collection of ESI may not be self-authenticating because custodians or in-house IT staff might not possess the tools necessary to produce the authenticating hash values necessary to meet the "authenticated . . . process of digital identification" for self-authentication under Federal Rule of Evidence 902(14).[38]

Importantly, though, the disdain for self-collection most commonly expressed by courts and commentators stems from counsel's complete delegation and failure to properly supervise the client's search and retrieval of discoverable ESI.[39] In this regard, "[t]he relevant rules and case law establish that an attorney has a duty and obligation to have knowledge of, supervise, or counsel the client's discovery search, collection, and production."[40] There are circumstances under which custodian self-collection—diligently supervised by counsel or a service provider acting at counsel's direction—may satisfy counsel's certification obligations under Rule 26(g)(1). Because collecting data must be done carefully, and all aspects must be completely and accurately documented, counsel should consider investing in training on how to supervise and/or implement defensible collection procedures.

While self-identification and collection of potentially responsive documents by custodians is not usually recommended, as noted above, there are scenarios in which it may be proportional and defensible, so long as a reasonable process is followed and documented. This process includes providing a timely and detailed litigation hold notice and providing instruction to custodians on how to identify potentially relevant documents and perform the self-collection, including how and where to store or transfer the collected information. The process should be documented, and counsel should make themselves available to answer questions that custodians may have throughout the process.[41][42]

Counsel in a small case may determine that self-collection poses undue risk *and* that preservation through a full forensic collection performed by an outside eDiscovery vendor is disproportionately

---

38 FED. R. EVID. 902(14).

39 "Self-collections by custodians may give rise to questions regarding the accuracy and completeness of collections if directions and oversight by legal counsel or forensics experts are poor or non-existent." *The Sedona Principles, Third Edition*, *supra* note 4, at 168.

40 *Equal Emp't Opportunity Comm'n*, 2020 WL 3581372, at *2 ("It is clear to the Court that an attorney cannot abandon his professional and ethical duties imposed by the applicable rules and case law and permit an interested party or person to "self-collect" discovery without any attorney advice, supervision, or knowledge of the process utilized.").

41 *See* Mirmina v. Genpact LLC, 2017 WL 3189027, Civil No. 3:16CV00614(AWT) (D. Conn. July 27, 2017) (Where defendant's in-house counsel supervised and documented the preservation and search process, the court denied plaintiff's motion to compel additional responsive electronic communications despite the fact that an individual directly involved in the underlying claims of the suit "self-identified" potentially responsive emails.).

42 To ensure that self-collection actually saves costs, counsel should look for ways to make the process streamlined and repeatable, such as having simple, easy-to-follow instructions or tutorials on how to export from common sources like Gmail or Outlook. These instructions may need to be updated periodically to reflect technical changes and/or upgrades.

costly, burdensome, and disruptive to operations given the needs of the case.[43] Accordingly, counsel may justifiably adopt an approach that, while not consistent with "best practices," may still produce a forensically sound copy of the data,[44] by using tools, trained individuals, and proper documentation of the steps taken.

B. Preliminary Considerations and the Rule 26(f) conference

1. Dialogue at the Beginning of the Case

Early case management conferences, such as the Rule 26(f) conference under the Federal Rules, are an often-missed opportunity to address ESI issues that are specific to small cases. Reference guides, such as *The Sedona Conference "Jumpstart Outline*,"[45] may be beneficial to tee up key questions to frame the scope of electronic discovery. Engaging in dialogue regarding eDiscovery and anticipating issues will help avoid costly disputes, especially when counsel wants to select low-cost eDiscovery solutions that may have shortcomings but may be proportional for the small case. Be prepared to educate opposing counsel, if necessary, to facilitate a productive discussion. Mutual education and cooperation can save time and money in small cases by addressing eDiscovery early. In jurisdictions that do not require early disclosure, or if such disclosures are honored more in the breach than the observance, requesting parties may consider using early discovery devices such as a small number of focused interrogatories to achieve the same goal. Identifying a custodian or the name of a database this way may save weeks or months of meet-and-confer time.

2. Don't be Coy

Requesting parties should avoid the temptation to play it close to the vest by not disclosing the kinds of ESI they will seek. When litigating in venues that permit early delivery of discovery requests (see, e.g., Rule 26(d)(2)), consider delivering Rule 34 requests before the case management conference to frame the discussion of the nature and sources of responsive documents.

Neither party is required to limit its disclosures to the information called for by Rule 26 or local guidelines. For example, counsel may consider disclosing the discovery platform it will use (if any) to review and categorize documents.[46] This can lead to multiple opportunities to save costs, if the party receiving that information is familiar with the platform. Although there is wide variation, many review platforms have analytics and other features included for no additional charge, or at modest

---

43 "Forensic data collection requires intrusive access to desktop, server, laptop, or other hard drives or media storage devices . . . . However, making a forensic copy of computers is only the first step of an expensive, complex, and difficult process of data analysis that can divert litigation into side issues and satellite disputes involving the interpretation of potentially ambiguous forensic evidence." *The Sedona Principles, Third Edition*, *supra* note 4, at 140–41.

44 *See The Sedona Conference Glossary: Fifth Edition*, *supra* note 22, at 312 (defining "Forensic Copy").

45 Tadler et al., *supra* note 26.

46 *See In re* Valsartan, Losartan & Irbesartan Prods. Liab. Litig., No. 19-2875, 2020 WL 7054284 (D.N.J. Dec. 2, 2020) (requiring parties to meet and confer regarding ESI discovery).

cost, but those platforms will require that the data loaded into them is formatted a certain way. If a requesting party wants to use a platform and the other party is unfamiliar with it, the parties should confer to resolve any issues with form of production and the extent to which searchable text and/or metadata will be produced.[47]

3. Strive to Reach Agreement

Sedona Principle 3 stresses the importance of reaching an agreement on discovery issues early and cooperatively.[48] This is especially important in small cases where clients have limited resources. Cooperation can lead to significant cost savings for all parties. Early, informal discussions between counsel about dates at issue, potential search terms and custodians, and data collection methods can move the case forward quickly and avoid motion practice. Some time- and cost-saving agreement points may include:

- the date range of discoverable ESI;
- custodians and noncustodial sources of ESI;
- search terms or other methods of searching data, such as email domains;
- methods for searching databases containing relevant information, such as the filters or fields that can be readily searched;
- an exchange of "hit counts" that help identify overinclusive search terms to avoid burden arguments; and
- a sampling exercise in which small batches of ESI that hit on key terms or other criteria are reviewed to see if the documents are relevant.

Suggesting and then reaching agreement on alternative and simpler ways to capture and produce relevant information can sometimes go a long way. For example, an individual faced with responding to a government subpoena or civil investigative demand may not have the resources to engage a vendor to conduct a forensic collection of text messages from the user's cell phone. By promptly raising the issue with the requesting agency, it may be possible to reach agreement that the individual be permitted to instead produce screen shots of the responsive text messages—so long as the underlying native data is separately preserved in place and intact (i.e., via a backup).

---

47 *See infra* Appendix for list of discovery platforms available on the market.

48 *The Sedona Principles, Third Edition*, *supra* note 4; *see also* The Sedona Conference, *Cooperation Proclamation*, 10 SEDONA CONF. J. 331 (2009 Supp.).

4. Focus on Accessibility

Sedona Principle 8 is particularly applicable here.[49] Especially in a small case, first focus on the ESI that is easiest to collect, produce, and review, which in many instances may be more than enough to achieve a resolution of the dispute. Start with what the parties agree on, such as the most relevant custodians, the most accessible data sources, or agreed-upon searches. Use this data to evaluate whether the agreed search parameters are effective. Leave open the possibility that search terms and other limitations may be modified and narrowed as parties become more familiar with the data.

Counsel may do well to prioritize the most important information, since processing, review, and production costs are directly proportional to the volume of ESI. This approach may support a proportionality analysis against needing to collect data from more difficult or expensive sources that are less accessible for technical or other reasons.[50]

5. Address "Bring Your Own Device" issues

Some organizations allow employees to use personal devices for business purposes, often under a "Bring Your Own Device" (BYOD) policy or agreement. The use of personal devices and accounts at work may mean that business information responsive to litigation is commingled with an employee's personal information. The reverse may also be true—an employee may have stored personal information on a device owned by the organization. These situations trigger privacy concerns and rights under local or state law.[51] A company may not be able to compel an employee to turn over a personal device for inspection or collection, even when a BYOD policy or agreement is in place.[52]

Such issues often arise as a question of whether the responding party has possession, custody, or control of the personal device. While a full discussion of these issues is jurisdiction specific and beyond the scope of this *Primer*,[53] it will be helpful to identify whether there are BYOD sources at issue

---

49 "The primary sources of electronically stored information to be preserved and produced should be those readily accessible in the ordinary course. Only when electronically stored information is not available through such primary sources should parties move down a continuum of less accessible sources until the information requested to be preserved or produced is no longer proportional." *The Sedona Principles, Third Edition*, *supra* note 4, at 134.

50 The Sedona Conference, *Commentary on Preservation, Management and Identification of Sources of Information that are Not Reasonably Accessible*, 10 SEDONA CONF. J. 281 (2009), *available at* https://thesedonaconference.org/publication/Commentary_on_Preservation_Management_and_Identification_of_Sources_of_Information_that_are_Not_Reasonably_Accessible.

51 *See* The Sedona Conference, *Commentary on BYOD: Principles and Guidance for Developing Policies and Meeting Discovery Obligations*, 19 SEDONA CONF. J. 495 (2018).

52 *See, e.g.*, Hayse v. City of Melvindale, No. 17-13294, 2018 WL 3655138, (E.D. Mich. Aug 2, 2018).

53 *See* The Sedona Conference, *Commentary on Rule 34 and Rule 45 "Possession, Custody, or Control,"* 17 SEDONA CONF. J. 467, 527 (2016) for a more detailed discussion of the topic. The *Commentary* addresses the variation in approaches taken by different jurisdictions.

and what position the responding party will take regarding their control over information stored on those devices.

Before insisting on the collection of data from these devices, consider the following questions:

- Is the data on the device unique, or is it a copy of data that can more easily be collected from laptops or computers?
- Is the data on the device critical to the claims and defenses in the case, or is data from other sources sufficient?
- Does the responding party have a BYOD policy or agreement, and what are the terms of that policy?
- Does the responding party have the legal right to obtain relevant information stored on its employees' devices?
- Does the responding party have the practical ability to obtain relevant information stored on its employees' devices?[54]

Regardless of who controls a BYOD device, preservation of these devices early on, as set forth above, is important. Even if the responding party is not in control of the devices, it may still need to notify the device owner for preservation purposes. The Appendix to this *Primer* suggests a representative sample of the least costly and technically simple applications and technologies to collect and preserve ESI from mobile devices.

6. ESI Protocols

In some large or complex matters, the parties may find it desirable to establish an ESI protocol early in the case to document agreement as to the form of production, the scope of preservation, and the procedures to search for responsive documents. ESI negotiations and protocols help set expectations for each party about the other's needs and plans, particularly on the issue of production format. For example, production in searchable PDF or native formats may be preferred in small cases. However, if the production includes hundreds or thousands of emails, production in PDF format may not be appropriate due to the loss of searchability and metadata. For some file types, such as spreadsheets and presentations, native files may be preferred because they are difficult to review once converted to images or static form.

---

[54] Note that the previous two questions will be appropriate in different jurisdictions based on how that jurisdiction interprets "control." *See Id.* at 482–91. Whether or not the responding party is required to notify the requesting party that the information sought is in the hands of a third party is also jurisdiction specific. *Id.* at 483.

However, the process of negotiating, drafting, and complying with an ESI protocol may be too impractical, time consuming, or costly in a small case. Regardless, counsel should document their agreement to the form of production even if a formal or more extensive ESI protocol is not warranted. Such an agreement can prevent later confusion and arguments over document production.[55] If agreement is not possible or preferred, the responding party may wish to clearly disclose its intended form of production if it is not what was requested.

If the production includes data types with which either party's counsel may be less familiar, such as text messages or communications from channels such as Teams, Slack, or WhatsApp, consider including a protocol for the production of these data types *only* if counsel fully understands the complexities and costs of collecting, searching, and producing such ESI. In the absence of a protocol, counsel should consult the default requirements of Rule 34(b)(2)(E) or the local rule for the form of production and address other topics through the meet-and-confer process as they arise.

C. Discovery Requests & Responses

1. Avoid boilerplate requests and responses

Sedona Principle 4 has long recognized the importance of specificity in both document requests and responses.[56] Subsequent Sedona publications have similarly urged litigants to avoid vague responses and boilerplate objections to document requests, providing guidance on how to effectively do so.[57] Yet, despite the changes made to Rule 34 in December 2015 regarding specificity, parties frequently fail to follow the requirements of the Rule.[58]

Boilerplate requests or responses tend to be counterproductive because they lead to ambiguity and additional time spent meeting and conferring before the parties settle down to the actual information being sought or produced. This can be especially problematic in a small case, particularly when discovery periods are short. A request for all documents on a very broad topic (especially one couched in language like, ". . . that refer or relate to . . .") is even less likely to net additional documents in a small case if the universe of documents is relatively small.

Responses will be most effective in limiting cost when they disclose the scope and limits of the search or production that a responding party undertakes. For example, a party may agree to search a

---

55 *See* Corker v. Costco Wholesale, No. C19-0290RSL, 2020 WL 1987060 (W.D. Wash. Apr. 27, 2020); Lundine v. Gates Corp., No. 18-1235-EFM, 2020 WL 1503514 (D. Kan. Mar. 30, 2020).

56 The Sedona Conference, *Primer on Crafting eDiscovery Requests with "Reasonable Particularity,"* 23 SEDONA CONF. J. 331 (2022).

57 *See* The Sedona Conference, *Federal Rule of Civil Procedure 34(b)(2) Primer: Practice Pointers for Responding to Discovery Requests*, 19 SEDONA CONF. J. 447 (2018).

58 *See, e.g.*, Mancia v. Mayflower Textile Servs. Co., 253 F.R.D. 354, 358 (D. Md. 2008); Fischer v. Forrest, 14 Civ. 1304 (PAE) (AJP), 14 Civ. 1307 (PAE) (AJP), 2017 WL 773694, (S.D.N.Y. Feb. 28, 2017); CBF Industria de Gusa S/A v. AMCI Holdings, Inc., 13-CV-2581, 2019 WL 3334503 (S.D.N.Y. July 25, 2019).

shared drive or the workstation of a single custodian but object on burden/proportionality grounds to searching mobile devices or social media. Disclosure informs the meet-and-confer process and can facilitate compromise on the scope of discovery.

2. Don't Wait to Produce

Though the rules allow responding parties to file responses before producing documents,[59] in a small case it may be more efficient to produce documents with the discovery responses. This allows the requesting party to evaluate the documents produced and assess whether the production is sufficient. Objections are often drafted before the responding party's counsel reviews the document production, but conferring about those objections before reviewing the documents may lead to pointless disputes.

3. Be practical about making and logging claims of privilege

"Logging large volumes of withheld ESI is often costly, burdensome, time-consuming, and disproportionate to the needs of the case."[60] The Federal Rules of Civil Procedure (and the state rules that follow them) do not explicitly require privilege logs.[61] If the parties can openly discuss what the privilege issues are and how they may be resolved, then the parties may agree that they may not need to exchange privilege logs.[62] This may be especially true in a small case, where it is less likely that there will be large volumes of ESI and where counsel is less likely to have been involved in pre-litigation communications. If a privilege log is needed, the parties should discuss how logging effort can be done to keep costs low. The need to log large numbers of privileged documents can also be sidestepped by wording requests carefully to avoid them. Sometimes this is as simple as inserting the word "nonprivileged" in the request. This will mean there is less opportunity to challenge a claim of privilege, but if privileged documents are unlikely to be important to the litigation, this may be an acceptable tradeoff.

Federal Rule of Evidence 502(d) provides heightened protection against waiver in instances where privileged information is knowingly or unknowingly disclosed. A 502(d) order or equivalent is useful

---

59 FED. R. CIV. P. 34(b).

60 *The Sedona Principles, Third Edition*, *supra* note 4, at 159 (internal citations omitted). "In addition, logging ESI such as email strings and attachments is difficult and lacks any uniform standard. Reviewing, redacting, and logging metadata or embedded information similarly can be a significant and undue burden." *Id.*

61 FED. R. CIV. P. 26(b)(5)(A) (requiring that the party making a claim of privilege disclose sufficient information for the other parties to assess the claim).

62 *Contra* Desoto Health & Rehab, L.L.C. v. Philadelphia Indem. Ins. Co., No. 2:09-CV-599-FTM-99S, 2010 WL 4853891, at *2 (M.D. Fla. Nov. 22, 2010) ("Agreements [not to produce privilege logs] are not controlling on this Court as the requirement to file privilege logs is not only for the parties, but also for the Court to use in evaluating the sufficiency of a privilege claim. Therefore, the Plaintiff is still required, by this Court, to complete privilege logs . . . ."); *see also* Williams v. Taser Int'l, Inc., 274 F.R.D. 694, 696 (N.D. Ga. 2008) (requiring log for all claims of privilege); S.C. Coastal Conservation League v. Ross, 431 F. Supp. 3d 719, 725 (D.S.C. 2020) (requiring an index to determine whether documents were improperly excluded from production).

for all parties in cases of all sizes, and The Sedona Conference recommends the entry of 502(d) orders as a best practice.[63]

D. Use Technology to Achieve Cost Savings

1. Use (all available) technology to your advantage

Although ESI has vastly expanded the universe of documents that are relevant to any dispute, technology provides ways to manage that volume. Even the relatively simple technology of keyword searching was little known 20 years ago. Since then, technologies that are far more sophisticated have emerged.[64] Section IV of this *Primer* discusses further the use of such technologies in small cases. Sedona Principle 11,[65] which recommends the use of technology to achieve cost savings, also has particular application to small cases. When considering technologies in the meet-and-confer process, counsel should consider the technologies available to all parties. Particularly in asymmetrical litigation, a party with greater resources at its disposal may be better positioned to deploy technology, even in a small case where it might not otherwise be available.

2. Combine technology with good process

Consideration should be given in small cases to how best to design the collection and search process to save costs and limit volume. Tools are only as effective as the skill of the user. Cost-effective and defensible use of tools requires intelligent processes and workflows.[66] For example, it can be more efficient to target a search against a selected universe of documents from the sources most likely to have relevant data, rather than applying search technologies to a broader universe of ESI that includes sources unlikely to contain relevant data or that contain data that does not lend itself to the search methodology. Counsel should understand the different types of searching available and whether searches will be effective given the tools they intend to use and the form of the data received. For example, some searches may be fielded, meaning they can be run against specific categories of information contained in file metadata (e.g., the subject line of an email, date, To/From, etc.). However, such searches require the fields to be intact when counsel handles them, and an application that allows searching the specific fields.

---

63 *See* The Sedona Conference, *Commentary on the Effective Use of Federal Rule of Evidence 502(d) Orders*, 23 SEDONA CONF. J. 1 (2022); See also The Sedona Conference, Commentary on Protection of Privileged ESI, 17 SEDONA CONF. J. 95 (2016).

64 The Sedona Conference, *Best Practices Commentary on the Use of Search & Information Retrieval Methods in E-Discovery*, 15 SEDONA CONF. J. 217 (2014); The Sedona Conference, TAR Case Law Primer, 18 SEDONA CONF. J. 1 (2017).

65 *The Sedona Principles, Third Edition*, *supra* note 4, at 164 ("A responding party may satisfy its good faith obligations to preserve and produce relevant electronically stored information by using technology and processes, such as sampling, searching, or the use of selection criteria.").

66 The Sedona Conference, *Commentary on Achieving Quality in the E-Discovery Process*, 15 SEDONA CONF. J. 265 (2014).

E. Discovery Motion Practice

Discovery motions are a frequent—and costly—element of pretrial practice and litigation. Courts encourage parties to resolve such disputes informally through mandatory meet-and-confer requirements. When motion practice is necessary, parties should continue to look for ways to reduce the cost and complexity of ESI-related motions.

1. Consider agreeing to streamlined motion procedures, if allowed

Courts differ in how they ask parties to present discovery motions. Because ESI can often be time-sensitive, consider agreeing in advance to use expedited motion procedures. These may include letter briefs, joint presentation of issues in a single filing, or shortened timetables for filing the motion and response. Where allowed, these procedures can save time and cost.

2. Avoid the jargon

Electronic discovery can be daunting because of the wealth of technical information and specialized terminology. Advocates should aim to cut through these obstacles to make issues clear and accessible for clients, opposing counsel, and the court.

3. Pick your battles

Strategic prioritization of high-impact issues is always good advice, but be mindful that electronic discovery can be costly. Especially in a small case, the cost of discovery may outweigh the value of the case. The parties' ability to cooperate, reach agreement, and limit issues in dispute will avoid motion fights. When a discovery motion is filed, showing the court that an honest effort was made to resolve the dispute informally may convince the court that counsel's discovery demands are reasonable.

F. Deploying ESI as Evidence in Small Cases

As with all evidence, ESI must ordinarily meet the requirements of admissibility and authentication. Modern courtroom technology is generally geared toward the use of ESI, so know ahead of time how to use it to present the case.

1. Plan for authentication and presentation

Until recently, the Federal Rules of Evidence governing admissibility did not separately address the admissibility of ESI.[67] The primary difference between ESI and other evidence is the process of authentication.[68] In some ways, ESI makes it easier for parties to stipulate to authenticity—e.g., it is

---

[67] FED. R. EVID. 901-903.

[68] FED. R. EVID. 902(13)-(14).

likely that an email produced from a server is an authentic representation of the original document. [69] On the other hand, ESI can also present unique authentication challenges, and the parties and courts should discuss whether the parties should stipulate to the authenticity of all or some ESI produced, depending on the data source, form of production, and/or availability of metadata or other indicia of authenticity.[70] To keep costs low, parties should stipulate to authenticity when reasonable. Such stipulations, of course, depend on the proportionality factors and should be delayed until *after* the ESI has been produced.[71]

Because ESI is used in different ways at different points throughout a case, different forms of production may be better or worse suited than others. For example, some technologies for producing text messages can export the relevant communications to an Excel file. This may make them easier to review, especially at large volumes, but the resulting report does not look at all like the text message that the user actually sent or received. So, when introducing the message as an exhibit, the witness may be less likely to recognize it. At trial, too, an entry in an Excel file may have far less visual impact than a text message that is in a form most jurors are familiar with.

On the other hand, some files are less likely to be presented at trial but will be important to other needs in the case and thus require different forms of production. For example, data compilations that will need to be sorted or analyzed by an expert are often best produced in an Excel or .csv file.[72]

Take these needs into account when negotiating forms of production. If documents are less likely to be used as exhibits at trial, as in the data example above, then authentication by certificate is likely sufficient. If a given document is important for visual impact, as in the case of text messages, be sure to seek it in a form that will meet those needs and can be easily authenticated by the relevant witness.

2. Know and use the authentication rules

In instances where a stipulation is not possible, authenticating ESI has become more efficient and cost-effective. On December 1, 2017, Federal Rule of Evidence 902 was updated to allow parties to authenticate certain electronic evidence by methods other than the testimony of a foundation

---

[69] *See* U.S. v. Safavian, 435 F. Supp. 2d 36 (D.D.C. 2006) (finding email communications authentic under Federal Rule of Evidence 901 on the basis of characteristics such as domain).

[70] *See* FED. R. CIV. P. 36 (permitting a party to request admission of the "genuineness of documents" from an opponent); FED. R. CIV. P. 16(C)(3) (allowing parties to request that an opposing party stipulate "regarding the authenticity of documents"; FED. R. CIV. P. 26(a)(3) (requiring that parties raise within 14 days any objections to the authenticity of documents and exhibits in pretrial disclosures).

[71] *See, e.g.,* Rossbach v. Montefiore Med. Ctr., 19cv5758 (DLC), 2021 WL 3421569 (S.D.N.Y. Aug. 5, 2021) (dismissing plaintiff's wrongful termination claims after finding plaintiff perpetrated a fraud on the court by introducing as evidence a fabricated text message).

[72] CSV: Comma Separated Value, *The Sedona Conference Glossary, Fifth Edition*, *supra* note 22, at 281.

witness.[73] The updated rule provides that electronic data recovered "by a process of digital identification" is self-authenticating and does not require the trial testimony of a forensic or technical expert where best practices are employed, as certified through a written affidavit by a "qualified person" who utilizes best practices for the collection, preservation, and verification of the digital evidence sought to be admitted.[74] This can help reduce costs by avoiding expensive and burdensome in-person trial testimony.[75] Because the amended Rule 902 requires that ESI contain information needed for "digital identification," counsel should consider such requirements early on, especially when undertaking any proportionality analysis that could later affect authentication.

3. Consider the Costs for ESI Presentation at Trial

In a small case, counsel likely will need to operate trial technology themselves. The good news is that there is a wide range of software available for this purpose, at relatively low cost, and much of it is very user-friendly. One caveat is to ensure that the ESI being presented is in a form that the presentation software can use—e.g., if an application uses only PDFs, an Excel file may call for a different solution.

4. Consider the form of presentation when determining the form of production

ESI can be presented in the traditional static form (PDF or TIFF[76] images), hard copy, or in native form—the form in which the ESI was created and maintained. So long as it is proportional to do so, counsel should request ESI in the form in which it will be most usable for case preparation and presentation.[77] For example, a PowerPoint presentation that includes dynamic slides may be more effective when presented at trial in its native form. In contrast, a static image of a text message sent via smartphone may be more useful for counsel to present at trial, as it will look more "familiar" than an extracted SMS message.

---

73 FED. R. EVID. 902(13)-(14).

74 The Sedona Conference, *Commentary on ESI Evidence & Admissibility, Second Edition*, 22 SEDONA CONF. J. 83 (2021).

75 FED. R. EVID. 902(13)-(14) advisory committee's notes to 2017 amendment.

76 TIFF: Tagged Image File Format: A widely used and supported graphic file format for storing bit-mapped images, with many different compression formats and resolutions, *The Sedona Conference Glossary, Fifth Edition*, *supra* note 22, at 377.

77 *See* Sedona Principle 12. Moreover, "[p]arties should not demand forms of production, including native files and metadata fields, for which they have no practical use or that do not materially aid in the discovery process." *The Sedona Principles, Third Edition*, *supra* note 4, at 173.

V. MANAGING SMALL-CASE DISCOVERY FROM THE BENCH

Judicial management is critical to efficient discovery in small cases. Different courts have different philosophies concerning the management responsibilities of the judge. Some courts have rules-driven approaches concerning when and how small cases proceed.[78] Upon filing, discovery rules are triggered either by case type or value.[79] Some courts rely on judges or nonjudicial case managers to conduct some type of triage and issue directives incorporating the discovery plan. In general, small-case discovery is largely a product of local rules and legal culture, and the court sets expectations for practitioners. Regardless of the source of direction for discovery, it is incumbent on the court to provide early guidance.

Electronic discovery presents an opportunity for judges to engage with counsel to promote efficiency and keep costs down. ESI and the technology associated with it is ever-changing. Judges may consider asking counsel questions about the ESI at issue in the case. Courts should be open to information and education about ESI from the parties and should feel free to request letter briefs or additional information about the parties' data, systems, and potential ESI challenges. Practitioners should be prepared to bring the court's ESI questions to their clients for further information and explanation.

1. Mandatory Disclosures

Initial mandatory disclosures are critical to determining whether a case is "small." Courts should require disclosures sufficient to determine whether small-case rules and procedures are appropriate, either through general jurisdiction practice rules or individual case management rules.

2. Query Parties about Data Needs, Technology Tools, and Plans

Judges should be sure that the parties have discussed the form of production and the use of technology for production. Information from this discussion may inform the likely scope of discovery and production format.[80] Judges should question counsel about the technology resources at their disposal. If firms or clients have already invested in discovery tools, the capabilities of the tools may inform appropriate discovery processes for the case. A discussion of file types is key for a potential native production, especially when the files originate from proprietary applications, and native file production may result in a loss of metadata without the correct tools and collection process.

---

78 CIVIL JUSTICE COMMITTEE, CALL TO ACTION: ACHIEVING CIVIL JUSTICE FOR ALL, APPENDIX D: PILOT PROJECTS, RULE CHANGES, AND OTHER INNOVATIONS IN STATE COURTS AROUND THE COUNTRY (2016), *available at* https://www.ncsc.org/__data/assets/pdf_file/0022/25681/ncsc-cji-appendices-d.pdf.

79 Commercial Court, Maricopa County, Experimental Rule 8.1 (2017), https://superiorcourt.maricopa.gov/media/1098/rule-81.pdf; Minnesota Special Rules For The Pilot Expedited Civil Litigation Track 1-4 (2017), https://www.mncourts.gov/Documents/0/Public/Rules/Special_Rules_for_Pilot_ELT.pdf; UTAH R. SMALL CLAIMS P. (2018), https://legacy.utcourts.gov/rules/srpe.php.

80 *See* ESI Protocols, *supra* Sec. IV.B.6, discussing production format.

3. Apply Common Sense Preservation Obligations

Judges may want to encourage counsel to confirm that clients understand preservation obligations and how to take steps to preserve data. Preservation of ESI in small cases should be understood to include metadata for disclosed documents. For example, while data from mobile devices and USB drives may not be required for initial disclosures, counsel should be sure that clients understand that preservation requirements might mean they cannot upgrade devices, change retention on devices, or clean off storage drives during the pendency of the litigation.

4. Provide Orders

The first key order in a small case is the Scheduling Order, which should direct the timing of all events, including mandatory disclosures (if applicable), motion practice (e.g., discovery and dispositive motions), exhibit and witness lists, and objections. While this may be the norm in federal court cases, it may not be likely in state court cases. The timing and deadlines should be scaled in a manner consistent with jurisdictional disposition expectations.

5. Expedite Resolution of Discovery Disputes

In small cases, it is helpful for the judge to provide expedited discovery dispute resolution.[81] This allows the parties to quickly and cost-effectively get a decision on discovery disputes in a manner that does not require a formal motion. The meet-and-confer process is important but is not a panacea. Judges may want to encourage the parties to engage with the court during the meet-and-confer process before the issue escalates to motion practice. The court can be helpful in establishing the goals, benchmarks, and timetables (see Section III.B.1.c above) that will move the parties toward a stipulation that avoids later disputes and facilitates the resolution of the case.[82]

---

[81] There are many examples (*see* MINN. GEN. R. PRAC. 115.04 (d) (2019); S.D.N.Y. R. 37.2 (2018).

[82] Additional Materials:

- FEDERAL JUDICIAL CENTER, PILOT PROJECT REGARDING INITIAL DISCOVERY PROTOCOLS FOR EMPLOYMENT CASES ALLEGING ADVERSE ACTION (2011), *available at* https://iaals.du.edu/sites/default/files/documents/publications/federal_employment_protocols_pilot_project.pdf.
- RONALD J. HEDGES, BARBARA JACOBS ROTHSTEIN & ELIZABETH C. WIGGINS, MANAGING DISCOVERY OF ELECTRONIC INFORMATION, THIRD EDITION (2017), FEDERAL JUDICIARY CENTER, *available at* https://www.fjc.gov/sites/default/files/materials/38/Managing%20Discovery%20of%20Electronic%20Information_Third%20Edition_Second%20Printing_2019.pdf.
- TIMOTHY T. TAU & EMERY G. LEE III, TECHNOLOGY-ASSISTED REVIEW FOR DISCOVERY REQUESTS: A POCKET GUIDE FOR JUDGES (2017), FEDERAL JUDICIAL CENTER, *available at* https://www.fjc.gov/sites/default/files/2017/Technology-Assisted%20Review%20for%20Discovery%20Requests.pdf.
- *Commentary on ESI Evidence and Admissibility, Second Edition*, *supra* note 74.

VI. COST-EFFECTIVE USE OF DISCOVERY TECHNOLOGY IN SMALL CASES

As discussed above, the types and volumes of ESI are ever expanding. Even in small cases, electronic discovery may implicate significant amounts of ESI, of which only a small fraction may be relevant. For example, an employment matter may require an email collection spanning the employee's tenure and multiple custodians, capturing ESI unrelated to the claims and defenses in the case. A personal injury or medical malpractice matter may require the production of photos, text messages, and social media. Each year, new technology is developed to improve electronic discovery efficiency and reduce overall litigation costs. This section discusses the effective use of technology for small cases for certain phases of the Electronic Discovery Reference Model.[83]

A. Collections

With multiplying data types and data sources for collection, this area of eDiscovery offers a wide variety of technologies. One application or software may collect some data sources or types, but there is no one technology to collect all data types across all data sources. The varied data types and collection technologies add to the complexity of collecting data for small cases. This *Primer* does not include an exhaustive list of every possible collection type, source, and corresponding collection tool, but it is meant to provide practical tips and suggest technologies commonly used in small cases. The attached Appendix also provides a nonexhaustive list of various technologies that may be beneficial for eDiscovery needs in small cases.

1. Reach agreement early as to data types, sources, and production format

All technologies have limitations regarding what data types they can collect. It is important to reach an agreement with the other parties regarding what is being collected and in what format it is being produced so that the appropriate collection technology can be used. This should be done to avoid producing data that is incomplete and may require an additional collection and review, which would be costly. Counsel should be wary of agreeing to collection and production formats for data with which they are unfamiliar or about which they have not consulted with their clients.

2. Do serial data requests seek unique, relevant information?

When the number of custodians increases, ESI volume balloons, so counsel should assess whether a potential custodian or data source includes unique content. If there are several custodians with the same role, consider collecting ESI from one key custodian before collecting from other custodians who may have the same or similar responsive content. This is also true for data sources. For instance, if a custodian mentions that she sent responsive emails from her phone after work hours, it is likely those emails are also stored on the mail server, making the collection of email from the

---

[83] *Electronic Discovery Reference Model* (2020), EDRM, https://edrm.net/resources/frameworks-and-standards/edrm-model/.

phone duplicative. For each data source, ask if the source contains unique information or there is a more accessible source from which to collect the same information.

Issues of personal privacy make these considerations even more important. The data on an individual's mobile device generally includes significant personal data, including personal banking, health care, social media, family photos, geographic tracking, and text messages. Collection of a mobile device should be made only when the device contains unique information that is responsive to the document request.[84] If the information can be collected from another data source other than a personal mobile device, collection from that other source is recommended.

If collection from mobile devices is necessary, counsel should be aware of the cost and complexity and discuss the need with their clients. Mobile device software makers update operating systems and applications frequently, sometimes without the user's knowledge. Mobile device collection technology tools may not be capable of collecting from upgraded operating systems or applications. In practice, this means that a tool used to collect data from a mobile device may not behave consistently or work at all following operating system or other software upgrades.

Always check the collected data before production to confirm an appropriate collection, regardless of the collection method or tool.

3. Choose the collection method reasonable and proportional to the given matter

Text messages are commonly relevant in small cases. There are multiple ways to collect text messages that are reasonable and proportional to the needs of the case. The parties should agree to an appropriate collection method in advance.

Custodians may self-collect using screenshots or photos of messages, as long as the parties are aware that the images do not include metadata—such as when the message was sent or received—and agree to this form of production. Such images do not provide sender and recipient information unless the custodian provides these names with the production or the image contains the custodian's saved name for the other text participants. Group messages with multiple text participants may require that the custodian manually identify each participant in each image of the messages. This collection method may be cumbersome for the custodian, depending on the number of messages to be produced, and may subject the custodian to questions regarding the method of collection. These questions may implicate the chain of custody, or make authentication difficult or impossible.[85] In some circumstances, a neutral non-party mobile device forensic expert may be worth the cost, even in a small case. The use of forensic vendors is discussed further below.

---

84 *See, e.g.,* Lewis v. Archer Daniels Midland Co., No. CV 17-14190, 2018 WL 6591999, at *2 (E.D. La. Dec. 14, 2018) (stating that permitting forensic examination of personal cell phones must be weighed against inherent privacy concerns).

85 *See Commentary on ESI Evidence & Admissibility, Second Edition*, *supra* note 74.

Another option for collecting text messages is PhoneView, an application that can be used to view, save, and print messages from mobile devices. The cost of the PhoneView application is minimal, especially compared to the cost of forensic collection of a mobile device for extracting and producing text messages. Use of this application or others like it still requires the custodian to self-collect or collect with the assistance of counsel, but the process is much less cumbersome. Beware that these applications may not extract all information, such as images or photos that are sent via text message. The collection and subsequent production may be incomplete if nonextracted information is responsive to the document request. It is important to understand the limitations of collection tools and discuss these with opposing counsel so that an agreement can be reached regarding the format of the data being produced.

If custodians use cloud backup for their mobile devices, they may be able to log into their cloud storage account to collect the requested data, including text messages. The timing of the storage backup is key for this collection method. This method likely involves custodial self-collection unless the client provides counsel or an eDiscovery technology provider with access to its cloud account.

If a more comprehensive approach is needed, the use of a forensic collection tool or vendor such as Cellebrite may be necessary. Cellebrite is a forensic collection tool that will extract all information on a mobile device, including metadata. Purchasing Cellebrite is likely cost-prohibitive for a small case, but many vendors offer collections services using similar tools. Mobile device collection by vendors is typically billed either by hourly rate or on a per-device rate. If mobile device collection is warranted for a small case, seek a cost estimate from a provider for a forensically sound collection. If only certain data is needed from the device, independent forensic consultants may provide a more complete collection than a self-service application, such as PhoneView or the custodial screenshot method, while keeping costs lower than a complete mobile collection.

4. Some data source applications may contain their own extraction/collection capability

Some social media applications, such as Facebook and LinkedIn, include data extraction capability. These built-in tools require account access for self-collection by the custodian, but the resulting data may not be easy to review or produce because of the format in which it is downloaded. The screenshot or photo method discussed for text messages may also be employed for social media data, with the same caveats. Some social media sites include a separate messaging application, such as Facebook Messenger. It is important to understand what social media applications the client uses and to explore whether those applications provide for a download of the data by the user.

If self-collection of social media is not possible or desirable, vendors offer sophisticated collection tools. X1 is one example of a collection tool for social media. As with Cellebrite, licensing X1 may be cost-prohibitive for one or two small cases, but vendors offer similar tools and social medial collection services. As with mobile devices, it is always a good idea to seek a cost estimate from a vendor with expertise in social media collection.

5. Be mindful of maintaining the original metadata when copying files

When collecting and copying files for production purposes, it is important to maintain the original metadata. Several collection tools help to maintain metadata without substantial cost. Robocopy is a free Windows utility accessible from the Windows command line (START→ Windows System → Command Prompt → type "Robocopy" at the prompt). If counsel is guiding custodians through self-collection, the custodian can maintain metadata by "zipping" or compressing the files using common applications like 7-zip.

A common metadata collection pitfall causes the "Date Last Modified" field to change to the collection date. Date metadata fields for template files are also problematic, as the "Date Created" field reflects the date the template was created as opposed to the date the individual saved a new copy of the document. Counsel and clients should be mindful of changing metadata values like "File Path" and "File Name" when collecting data by copying or forwarding in email.

6. Be mindful of maintaining the original metadata when collecting emails

As discussed above, small cases do not always warrant forensic data collection. Custodial self-collection may be appropriate. When appropriate, counsel should guide custodians carefully as to collection methods. For instance, custodians should not forward emails to counsel for review. Doing so will change the metadata of the email, modifying the original "Sender," "Recipient," and "Date" fields. Rather, dropping emails as attachments into a new email, rather than forwarding them, is a useful way for counsel to collect the original emails. Forwarding sensitive emails and attachments may create data security risks as well, which goes beyond the scope of this *Primer*. Attention to data security is always critical when collecting sensitive or personal information.

Discussions of the collection and production format for cell phone, social media, and text message data are important. Cost is the primary driver in any plan to collect and produce these data types. Without planning, parties may have to re-collect and reproduce, increasing the overall discovery costs for the case.

B. Document Review, Analysis, and Production

1. Determine when an electronic discovery review tool is appropriate

Depending on the form of production, reviewing the collected data can be done in many ways. For instance, if the potential production comprises PDFs and a small number of images of documents, counsel may want to review simply by viewing the files in the application that created them. Under these circumstances, counsel may be able to review and produce using Adobe Acrobat to redact, Bates stamp, and print the production to PDF without incurring the expense of a vendor. It is important to make sure that the redactions are permanent before producing or using the redacted document.

If the potential production set comprises several file types or a larger set of data, utilizing an electronic discovery review tool may be appropriate. This can be especially true for a requesting party who receives a large document production from a corporate defendant. Several cloud-based review tools are available on a monthly subscription or per-gigabyte cost basis. Some examples include Everlaw, Logikcull, and RelativityOne. While investing in an eDiscovery review tool may not be economically feasible for small cases individually, spreading or sharing the costs across multiple cases and multiple clients may have a significant cost-saving benefit. This is a growing industry, so practitioners are advised to research the current market for pay-as-you-go, no-commitment review tools. Small cases do not often require data analytics, but in the event counsel must search through large volumes of documents, some of these products can include advanced analytics tools that may also be useful. Such tools may help identify responsive documents more quickly than human review without unreasonably increasing the cost but may require more training to use.

For corporations with small cases, tools that are already licensed for purposes other than discovery might have capabilities that also support litigation. One example is Office 365, which has electronic discovery capabilities for some license levels. Consult with the corporate Microsoft representative or information governance partner to discuss whether the Microsoft license allows collection, review, analysis, and production of data without the need to export to a non-party vendor.

2. When applying redactions, be mindful of embedded images and metadata

Unless the parties agree that metadata production is not required, be careful that redacted material is not produced inadvertently. This can happen in several ways. When a non-email document contains embedded images, such as a screenshot from another application, the embedded image or screenshot is extracted as a child to the parent e-file. When applying redactions to a parent document that includes an embedded image, remember to redact the child image document if it contains material that should not be produced. Similarly, when applying redactions to imaged files (PDFs or TIFFs of native files), remember that any redacted text must also be removed from a separate metadata or text file. Otherwise, the information redacted from the image may be inadvertently produced. For those unaccustomed to producing documents with text or load files, consult with an expert to quality-check production redactions. Several new tools on the market offer "auto-redaction" of data such as Personally Identifiable Information.

3. Determine production format early

This *Primer* does not recommend any specific ESI protocol or form of production but does provide some tips and caveats for productions in small cases.

- Acrobat DC Pro can be used to Bates stamp and redact productions.

- Produce documents in a readable form. Produce each document as a discrete image file instead of combining multiple, individual documents into a single large PDF document.

- The most common production format is a TIFF image, but some file types are better suited for a native production (for definitions of these production formats as well as other electronic discovery related definitions, please see *The Sedona Conference Glossary*).[86]

- Excel spreadsheets and PowerPoint presentations are examples of file types that are commonly produced natively. When a single Excel spreadsheet is imaged, it can result in hundreds or thousands of pages, with columns and rows spanning multiple pages, making it not readily readable. Thus, these file types are typically produced natively even if they require redactions.

- PowerPoint presentations are also often produced natively to maintain slideshow effects. Once the presentation is imaged, any animations or special features incorporated into the presentation are no longer viewable. While there may not be a one-size-fits-all approach when it comes to production format, it is important to discuss production format along with data types and sources during the 26(f) conference as outlined above.

---

[86] *The Sedona Conference Glossary: Fifth Edition*, *supra* note 22.

VII. CONCLUSION

While small cases may not suffer from the complexities of large-scale litigations, small case discovery can be complex, as explored in this *Primer* and illustrated by the efforts to develop it. While some of the tips outlined above apply to cases of any size, they are all particularly helpful in small cases where prevailing standards of proportionality, reasonableness, and cooperation must be applied to the management of ESI and discovery processes. This *Primer* is meant to be a tool to aid in the process of fulfilling Rule 1's duty of a "just, speedy and inexpensive determination" when it comes to fulfilling discovery obligations in small cases.

APPENDIX

I. Collection Software

A. Text Messages: Screenshots and Merge Together

Parties may consider collecting and producing text messages by taking screenshots of the messages and using an app like Tailor or Stitch It to combine and render them in a readable form. This is not a forensic collection, and metadata of the original message will be missing from the collection. This is a self-collection method and relies on the owner of the phone to do the heavy lifting of identifying and collecting responsive text messages (under the supervision or guidance of counsel). This approach may address concerns that irrelevant personal data has been disclosed to a third party. It is important to document the time and date of the screenshots. The following two videos show how to best utilize this method:

- iPhone
- Android

B. Phone Collections: Apps or Software for your iPhone or Android

iMazing is another product that that can be used in collecting text messages or other phone data. This is software installed on a Windows or Mac computer. When an iPhone/iPad is connected to the computer, it allows the user to search and filter messages that can be exported to a TXT or PDF file.

This blog post from iMazing describes how to use the product for legal purposes. The software is around $50 for a single license.

For Android devices, similar products such as SMS Backup & Restore or Dr. Fone export messages as CSV files.

.Below is a list of various technologies depending on the phone at issue:

- iPhone: "Decipher TextMessage," "Keepster," "imazing," "iTunes backup"
- Android: "SMS Backup & Restore Pro," "SMS Backup+"

C. Cellebrite

Cellebrite is a leading tool for collecting mobile data. Cellebrite allows users to unlock devices by bypassing pattern, password, or PIN locks and overcome encryption challenges on both Android and iOS devices. In addition to extracting data from mobile phones, it also allows extraction from

drones, SIM cards, SD cards, GPS devices and so on. Cellebrite can further utilize various recovery methods.

In addition, an examiner can use Cellebrite Physical Analyzer to generate a report in Cellebrite Reader format to share with others who do not have the software. This allows end users to review the data without the need for specialized Cellebrite software (which costs thousands of dollars) and to search, sort, filter, search within results, reorganize data within columns, and create customized tags that can be saved and reviewed later. End users can obtain a free copy of the Cellebrite Reader software either from the examiner or by creating a free account with Cellebrite.

D. X1 Social Discovery

X1 Social Discovery is a software tool for collecting and searching data from social networks and the internet. It aggregates comprehensive social media content and web-based data into a single user interface, collects metadata, and preserves the chain of custody. Unlike archiving and image capture solutions, X1 Social Discovery preserves information in searchable native format**.** Besides social media content, it is useful tool for collecting webmail and YouTube videos. This software works only with a PC operating system.

Both Cellebrite and XI Social Discovery are used by many eDiscovery providers, so in cases where it may not be cost-effective to license the tool directly, it may be cost-effective to reach out to a provider who is able to spread the software licensing costs across clients.

E. PhoneView

PhoneView is a no- to low-cost software that allows users to remotely view mobile device content from a computer. It also allows users to view, save, and print all iPhone and iPad messages, WhatsApp messages, voicemail, and other data directly onto a computer. In comparison to full collection software mentioned above, it may have limitations as to the data that is extracted and thus may not extract and/or recover the complete data on a device.

F. AnyDroid or Droid Transfer

Both AnyDroid and Droid Transfer allow users to remotely control content on an Android-based device. Both programs allow users to extract data, including text messages and call logs, from devices using the Android operating system. Because these are not forensic collection tools, there are limitations to the output of the data collected.

G. FTK Imager

FTK Imager is a free tool for previewing data and creating disk images. It offers searching capabilities, produces a case log file, and provides bookmarking and reporting features.

H. Magnet ACQUIRE

Magnet ACQUIRE lets digital forensic examiners quickly and easily acquire forensic images of a wide range of potential digital evidence sources, such as any iOS or Android device, hard drive, removable media, and cloud data. It supports both logical and physical acquisition. It is available at no cost to the forensic community.

I. Google Takeout

Google Takeout is a free tool used to export Google data for backup. It supports 51 types of data, including mail, drive content, calendars, browser bookmarks, and activity on YouTube. In essence, it retrieves and downloads all the information Google has about a user.

J. PinPoint Labs Harvester

Harvester is an eDiscovery collection software suite by Pinpoint Labs. This software allows searching, filtering, and copying files, folders, and documents from local and cloud environments. The collected data can be loaded into popular review platforms.

K. Paladin

Paladin and Paladin Toolbox allow various forensics tasks, including triage and imaging of drives, to be performed in a forensically sound manner.

L. Message Crawler

Message Crawler is an application that will convert data from numerous file formats to Relativity's "Short Message Format" (RSMF). Users can choose how data will be split, selecting either one day, one week or one month per conversation, allowing them to see the data in the most convenient presentation for their needs.

M. Oxygen

Oxygen Forensics Suite is a forensic software that is used to acquire data from mobile devices, their backups and images, SIM card data, messenger logs, and cloud storage.

II. End-to-End Discovery Software

The following software are cloud-based, end-to-end eDiscovery solutions. The Sedona Conference does not recommend any solution over another. This list represents some of the many options that may be helpful in resolving eDiscovery needs in small cases.

- DISCO

- Everlaw
- LogikCull
- RelativityOne
- Reveal Data
- CasePoint
- NextPoint
- Lighthouse Spectra
- Zapproved ZDiscovery
- siConect

III. General Software

A. Adobe Acrobat Pro

Adobe Acrobat Pro is a Portable Document Format (PDF) editor tool that allows users to view, create, search, edit, annotate, convert, redact, print and manage PDF files. It is particularly useful in allowing text searches on otherwise nonsearchable PDFs (typically PDFs that are scanned paper) by running Acrobat's optical character recognition process on the files. Making PDFs searchable assists users in identifying relevant information in a large set of PDF files. Being able to annotate and bookmark PDFs gives users the opportunity to more easily identify and find documents of particular interest and provides a basic means to organize these documents. It also has the ability to redact and bates stamp documents and create a PDF index to improve the ability to search multiple files at the same time. This software works with both PC and Mac operating systems.

B. Microsoft/Office365

Core eDiscovery in Microsoft 365 provides a basic eDiscovery tool that organizations can use to search and export content in Microsoft 365 and Office 365. Core eDiscovery can also be used to place an eDiscovery hold on content locations, such as Exchange mailboxes, SharePoint sites, OneDrive accounts, and Microsoft Teams. Nothing is needed to deploy Core eDiscovery, but there are some prerequisite tasks that an IT administrator and eDiscovery manager have to complete before Core eDiscovery can be used to search, export, and preserve content.

C. dtSearch

dtSearch is a search and retrieval program that is useful for searching discovery productions and viewing many different file types, including searchable PDFs, Microsoft files (Word, Excel, etc.), web data, and email. It includes a near-native viewer that allows end users to search and view what a document looks like even when they don't have the associated application installed on their device (e.g., users can view a PowerPoint file and even when they do not have PowerPoint on their computer). The program provides multiple ways of searching, including key word, fuzzy, and Boolean searching. This software works only with a PC operating system.

D. CaseMap/TimeMap/DocManager

CaseMap is a fact and case organization and analysis tool that allows users to track and organize case information regarding facts, persons, documents, and issues in one database. Documents relevant to the case are linked to the database, which allows end users to quickly search, sort, and filter case information. Various PDF reports, including fact chronologies, lists of persons, issues, and documents, can be easily produced to provide snapshots of critical case information. Users can embed into the PDF reports the source documents that have been linked to the database to allow sharing of key information with people who may not have access to the database.

TimeMap creates case-related visual timelines. The program allows users to create a variety of timelines useful for courtroom presentations and team and client meetings.

DocManager is a near-native image viewer specifically designed for CaseMap. It allows users to review and annotate documents linked to the database without having to open the source file, making it easier and faster to navigate through the documents.

E. ReadySuite

ReadySuite is a tool for creating and converting eDiscovery review database export and import files, including Relativity, Ipro Eclipse SE, Summation, Concordance, and TrialDirector formats.

F. Beyond Compare

Beyond Compare is a data comparison tool that is useful for comparing and identifying differences between various files, including load files. It is helpful in identifying and syncing original and copy folders where the copy has failed (for example, due to overlong file names, or files sizes that are too large). It can do side-by-side comparison of directories (including FTP, SFTP, Dropbox, and Amazon S3 directories). This software works with both PC and Mac operating systems.

G. IrfanView

IrfanView is an image viewer that allows users to browse through images quickly or watch them as a slideshow. IrfanView also includes a photo editor, a batch file converter, and a scanner interface.

H. 7Zip

7Zip is a free, open-source file archiver used to compress or zip files secured with encryption. It is useful for reducing the file size and securing files when emailing.

I. Notepad++

Notepad++ is free software used for text and source-code editing.

J. Treesize

TreeSize Free is a free disk space manager for Windows that is used to display drive and folder sizes, including all subfolders, and to create reports on the findings. It allows users to sort files by fields such as file age and size.

K. Arsenal Image Mounter

Arsenal Image Mounter is a forensic disk image mounting solution that mounts the contents of disk images as shares or partitions, rather than complete, physical, or real disks.

L. PST Walker

PST Walker is an app that provides a portable PST viewer and data recovery for Microsoft Outlook. It is also used to restore corrupted or encrypted PST files and OST files.

M. Safecopy

Safecopy is a data recovery tool that is used to extract as much data as possible from a damaged source, such as floppy drives, hard-disk partitions, compact disks, and tape devices.

N. Foxit PhantomPDF

Foxit PhantomPDF Editor is similar to Adobe Acrobat Pro. It is software that lets users view, create, edit, comment, secure, organize, export, employ optical character recognition on, and sign PDF documents and forms.