White Paper presented by Tom O'Connor

"Technology is not the key to successful management of discovery in small cases. Informed application of technology, in harmony with and understanding of the risks, rules, and requirements are the keys"

# eDiscovery for the Rest of Us

## Contents




# Introduction

In 2010, noted e-discovery consultant Craig Ball wrote a fascinating article in Law Technology News entitled *"E-Discovery for Everybody*." That column came to be known as the "Edna Challenge" because in it, Craig posited a solo practitioner named Edna with an e-discovery budget of $1,000 and asked how she could possibly perform any e-discovery on that amount.

The problem as Craig defined it was simple:

> *"The vast majority of cases filed, developed and tried in the United States are not multimillion-dollar dust ups between big companies. The evidence in modest cases is digital, too. Solo and small firm counsel like Edna need affordable, user-friendly tools designed for desktop e-discovery -- tools that preserve metadata, offer efficient workflow and ably handle the common file formats that account for nearly all of the ESI seen in day-to-day litigation. "*

I first spoke on the subject at the 20011 ABA TechShow with Bruce Olson, a Wisconsin attorney and former Chair of the TechShow, and we coined the issue of the Small Case Dilemma. While it is not automatically true that small cases require different tools for managing e-discovery, the fact is that small cases often mean small technology budgets. Unless your practice is sufficiently mixed with big budget cases so that you already have a full complement of litigation support tools to use, you probably don't have the tools necessary to handle anything but the smallest e-discovery matter. And the small budget means you can't engage an outside consultant or vendor.

But the e-discovery rules at both the federal and state level do not apply to just large cases. They force civil litigants into a compliance mode with respect to the retention and management of electronically stored information or ESI. The risks that litigants face as a result of improper management of ESI can include findings of spoliation of evidence, summary judgment findings and sanctions, including adverse inferences, adverse jury instructions and even complaints filed with state bar associations.

There are several basic assumptions we should point out about small cases. First, we assume that you will be working with copies of live data in native format. It is also assumed that the types of files you are dealing with are typically files created by common programs used for email, word processing and other office functions. The more unique the file formats, the more likely it is that you need a higher-end solution.

Another assumption is that you want to work with the data yourself and that you have the equipment and skills to do so. There are many good Internet based hosted solutions that can fill your needs, and costs for them vary widely. However, the typical storage fees charged for a case that exists for any length of time can bust a modest

technology budget. So small cases demand applications that can be installed on one computer for processing and review. Typical examples would be files emailed from custodians, exported from a file sharing website, or produced on an external storage device, for example a USB thumb drive.

We're also assuming you are not dealing with terabytes of data – large volumes equivalent to millions of pages of paper or hundreds of thousands or millions of emails. Small cases typically involve smaller volumes of ESI. And finally, we're assuming you have a cooperative relationship with the other side, at least in terms of dealing with e-discovery. The single most effective way to keep e-discovery costs low is to work with your opposition in a cooperative manner so you can stipulate to the use of low-cost solutions.

The question then becomes, is there really a way to process and review a couple of hundred GB of data for a reasonable price? Are there really low cost but technically adept applications that attorneys can use themselves to host and review that same data? And if not, why?

The first barrier has been the traditional pricing models in the e-discovery market. Why is this? Because many, if not most, e-discovery vendors have their roots in the per unit commodity pricing days of photocopying and imaging. The standard practice for years now has been to charge hundreds of dollars per GB each time data is handled.

The result is that at each step of the EDRM process, an exorbitant per GB price is charged. $X per GB for processing, $X per page for OCR, $X per document for near duplicate detection, $X per page for Bates numbers, $X per user and per GB to host and so on. Each step is performed for different units (GB, page, document, user, etc) with different unit pricing that can run from a penny to $500 per unit.

The result was that a forensically sound forensic collection of 800 GB (the size of the hard drive of one typical computer) typically yielded about 200 GB of reviewable material, for which a standard charge would be $200 per GB for the processing ($160,000) plus $50 per month per GB ($10,000) and $90 per month per user for the hosting. If the case lasts 18 months, this cost alone will be just under $350,000.00. And if we accept the commonly cited statistic that the review process will account for 60-70% of the total project price, then we're looking at a project cost that will eventually be close to $1,000,000.00 for 200 GB of data!

Users balked at these prices, but large e-discovery companies had no interest in lowering prices because they had high overhead costs and needed large revenue amounts to support that infrastructure. Companies with revenue streams based on processing or hosting terabytes of data cannot easily adapt to projects consisting of several hundred gigabytes much as you cannot expect a 747 jumbo jet to be used as an effective or cost-efficient means of transporting commuters during rush hour traffic.

Additionally, their technology was often developed initially for large cases with large data sets. Products that have been designed to work with immense data collections

cannot easily scale down to small sets of information. A SQL based product working with terabytes of data on a distributed internet framework needs a certain hardware and software infrastructure to operate and simply can't be scaled down to load on a laptop or tablet.

When this cost is added to the legacy mind set of unitized pricing noted above, these vendors are locked into a system of set monthly costs and simply cannot, from their perspective, give away their services to small firms with small cases.

As a result, a simple license plus annual maintenance or a monthly subscription fee model for e-discovery products simply didn't exist. Instead, users were forced to sort through hundreds of products priced by varying and often widely divergent pricing methods.

That's the bad news. The good news is that low-cost programs designed for small cases do, in fact, exist. New pricing paradigms and lower technology costs have driven a new breed of e-discovery software that is not only modestly priced but structured in such a way as to allow precise budgeting and cost calculations for their use.

The purpose of this work is to show you how that process has evolved and how you can deal with it. A specific example - Digital WarRoom Pro software is designed for single users or small firms that would like complete control of their data and discovery. This software application is fully functional - offering the same key features as hosted subscriptions at a fixed software price. With DWR Pro, you can process, review and produce documents entirely on your own computer and take control of a variety of small to mid-size cases. Digital WarRoom also offers full feature hosted ediscovery for small matters with the same technology, but on a monthly subscription basis with very low price of entry.

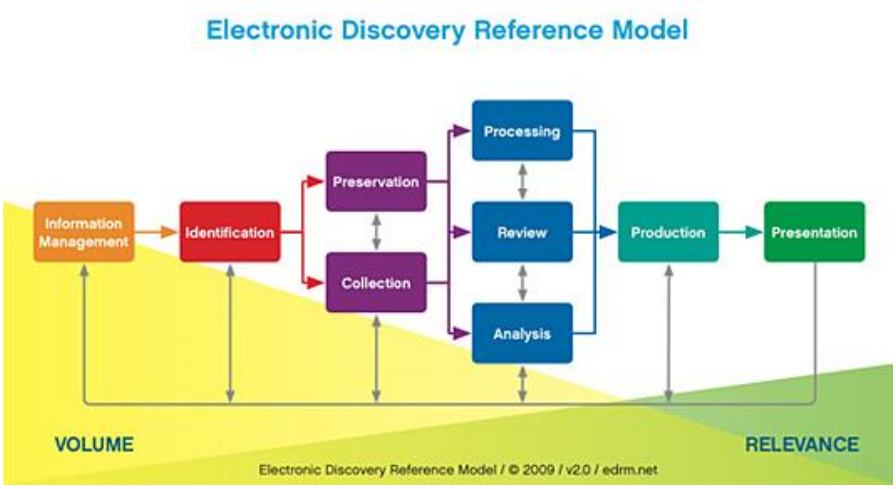
## Chapter 1: The Early Years

Formalized changes to the Federal Rules of Civil Procedure with regards to eDiscovery were made in December of 2006 as the culmination of a period of debate and review that started in March 2000. Prior to those codified changes, there were several landmarks in the development of the eDiscovery space.

The first was a series of discovery decisions in a lawsuit which became popularly known as the Zubulake case. (Zubulake v. UBS Warburg, 220 F.R.D. 212 (S.D.N.Y. 2003). Throughout the life of that case, the plaintiff claimed that the evidence needed to prove the assertions in her complaint existed in emails stored on the computer systems of the defendant. She had copies in her possession of some of those messages and when the defendants were not able to produce the originals the court found that it was more likely than not that they existed. Further, since the defendants corporate counsel had directed that all potential discovery evidence, including emails, be preserved, the court held that the employees who received that directive

were negligent in fulfilling their duty of preservation and levied significant sanctions against UBS.

Shortly thereafter, in 2005, the EDRM (Electronic Discovery Reference Model) was formed by attorney. George Socha and his partner Tom Gelbmann as an open-source standard with the goal of facilitating leadership, standards, best practices, tools, guides, and test data sets to improve electronic discovery workflow processes.[1] George and Tom devised the following chart to show a general workflow for eDiscovery projects.




The problems pushing these changes forward were the increasing volume and multiplicity of data in electronic formats. Examples of the types of data included in eDiscovery are not just standard business documents such as letters, agreements, memos and even spreadsheets but also e-mail, databases, web sites, instant messaging and any other electronically information stored in the ordinary course of business that could be relevant evidence in litigation.

The increase in digital activity has become even more pronounced in recent years with more people using digital information in all areas of their lives and the increased number of people working from home, especially during the COVID pandemic.

According to a report from the Georgetown University Law School, 88% of the US population uses the Internet every day and 91% of the adults use social media regularly.[2]

Additionally, "raw data", such as deleted files or file fragments left in unused space on a computer which could be retrieved by forensic investigators is potentially relevant as may be the myriad of data backup types ranging from tape systems to hard drive archives.

According to the Smithsonian Institution Archives, most documents created today are generated in electronic format, we have seen an enormous rise in ESI in all case

[1] https://www.digitalwarroom.com/blog/chapter-1-the-early-years#_ftn1
[2] https://www.digitalwarroom.com/blog/chapter-1-the-early-years#_ftn1

types. Litigators may review material from e-discovery in one of several formats: paper printed from images, PDF images (with or without searchable text) single- or multi-page TIFF images or the original format in which the documents was created and stored, the last type being commonly referred to as "native files".

That variety of file types and formats led to countless discovery disputes between the parties. Defense firms commonly objected to the perceived, or at least argued, shortcomings of native files. They preferred to use static images such as TIFF files, most often because they had invested in litigation support software systems that utilized that format. Plaintiffs preferred native files because they were most often a file type such as Word or a common email format that they already possessed and knew how to use.

These changes and the resultant tensions effectively forced civil litigants into a compliance mode with respect to their proper retention and management of electronically stored information (ESI). The risks that litigants then began to face because of improper management of ESI include spoliation of evidence, adverse inference rulings, summary judgment motions and sanctions, both monetary and procedural. In some cases, attorneys were even brought before their state bar association to answer to charges of misconduct., as was the case in the much-discussed matter of Qualcomm Inc., v. Broadcom Corp., 548 F.3d 1004 (Fed. Cir. 2008).

This atmosphere and those type of disputes became part of the reason that the court rules were changed. The Rules Committee of the Federal court system felt it necessary to implement changes which would reduce time consuming arguments over file formats that were leading to delays in the handling of litigation matters. We will discuss those rule changes in the next section.[34]

## Chapter 2: Rule Changes

The first formalized changes to the Federal Rules of Civil Procedure regarding eDiscovery were made in December of 2006. This was the culmination of a period of debate and review that started in March 2000 although discussions about the use of electronic documents in litigation had been underway long before that. As early as the late 1980s, U.S. Senate investigators in the Iran-Contra affair were able to retrieve 758 e-mail messages sent by Oliver North regarding his involvement in the operation.

[3] In 2016, Duke Law School acquired the EDRM in order to expand the involvement of Duke Law's Center for Judicial Studies as part of its mission to generate ways to improve the administration of justice. In 2019, Mary Mack and Kaylee Walstad, the former executive director and former vice president of client engagement, respectively, of The Association of Certified E-Discovery Specialists (ACEDS) acquired the EDRM from the Bolch Judicial Institute at Duke Law School.

[4] See Social Media Evidence in Criminal Proceedings: An Uncertain Frontier from Georgetown Law at https://www.crowell.com/files/Social-Media-Evidence-in¬Criminal-Proceedings-An-Uncertain-Frontier.pdf

North had believed e-mail messages to be deleted but after the email recovery, he was convicted of lying under oath to a congressional committee.

Roughly ten years later, then Vice President Al Gore's fundraising activities were under investigation by the U.S. Department of Justice. White House Counsel Beth Norton eventually reported that it would take up to six months to search through 625 storage tapes of White House e-mail

In 1999, the American Bar Association adopted new Civil Discovery Standards, which included provisions addressing preservation duties and cost shifting in relation to e-discovery. Those standards were cited thereafter in several federal cases, most notably Judge Shira A. Scheindlin's discovery decisions in the matter popularly known as the Zubulake case. (Zubulake v. UBS Warburg, S.D.N.Y. 2003, 220 F.R.D. 212)

Throughout that case, the plaintiff claimed that the evidence needed to prove her claims existed in emails stored on UBS' own computer systems. Because the emails requested were either never found or destroyed, the court found that it was more likely that they existed than not. The court found that while the corporation's counsel directed that all potential discovery evidence, including emails, be preserved, the staff that the directive applied to did not follow through. This resulted in significant sanctions against UBS.

The actual rule changes that were introduced in 2006 included:

- **Rule 34(a)** created a new category of discoverable information - electronically stored information or 'ESI' and gave the **r**eviewing party the right to 'test or sample' electronically stored information as part of the initial production process
- **Rule 34(b)** permits a requesting party to specify the form for producing electronically stored information as part of the initial production process
- **Rule 26(b)(2)(B)** provides that electronically stored information need not be produced if the source is not reasonably accessible on account of either undue burden or undue cost.
- **Rule 26(f)** was amended to include meet and confer requirements regarding ESI. These included specifically discussing with particularity any issues that are likely to arise and to develop a proposed discovery plan relating to disclosure of any ESI.
- **Rule 37**, sometimes referred to as the 'safe harbor' rule, provides that 'a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system.

These rule changes effectively forced civil litigants into a compliance mode with respect to their proper retention and management of electronically stored information (ESI). The risks that litigants then began to face because of improper management of ESI include spoliation of evidence, adverse inference, summary judgment, and sanctions. The best-known example is Qualcomm Inc., v. Broadcom

Corp., 548 F.3d 1004 (Fed. Cir. 2008) where plaintiffs were sanctioned $8.5 million for what the Court called "monumental" discovery violations in their conduct in the discovery and trial of the matter. In addition, six attorneys were reported to their state bar association. They were eventually found blameless by the Court but not until two years later.[5]

After the FRCP amendments, many states also changed their rules to follow and, in some cases, mirror the FRCP changes. At the time of this writing, over 2/3 of the states had established such a rule. coast-to-coast, from California to Florida and from states as populous as New Jersey to mostly rural states such as Louisiana and Alabama, e-Discovery is now a local issue.

The most up to date information on state rules can be found in a list compiled by Thomas Y. Allman, former Senior Vice President, General Counsel and Chief Compliance Officer of BASF Corporation and later Senior Counsel to Mayer, Brown, Rowe & Maw, LLP. He was an early advocate of amendments to the Federal Rules of Civil Procedure to achieve e-discovery reform and a leader in the formulation of the Sedona Principles.[6] The Sedona Conference has also published an overview of state discovery law.

More recently even criminal matters have been affected. In 2012, the Department of Justice/Administrative Office Joint Working Group on Electronic Technology (JETWG) developed a recommended ESI protocol for use in federal criminal cases. [7] Since then, attention to ESI has continued to grow and even bleed down to state and local criminal matters.[8]

In addition to formal court rules, many states are also pushing technical competence as an ethical requirement. From the well-known California Bar Opinion, "*9 Things Every Attorney Needs to Know About Ediscovery*" [9] to the Florida CLE requirement for technical training [10] basic technical competence in technical issues is now the rule in 38 states. Keep an eye on Bob Ambrogi's Law Sites blog for the latest on this issue. [11]

---

[5]https://www.ediscoverylaw.com/2010/04/court-declines-to-impose-sanctions-against-qualcomm-attorneys-absent-evidence-of-bad-faith/

[6] https://thesedonaconference.org/node/2046

[7] Recommendations for Electronically Stored Information Discovery Production in Federal Criminal Cases. https://www.fd.org/sites/default/files/Litigation%20Support/final-esi-protocol.pdf

[8] Social Media Evidence in Criminal Proceedings: An Uncertain Frontier from Georgetown Law at https://www.crowell.com/files/Social-Media-Evidence-in¬Criminal-Proceedings-An-Uncertain-Frontier.pdf)

[9]http://www.calbar.ca.gov/Portals/0/documents/ethics/Opinions/CAL%202015-193%20%5B11-0004%5D%20(06-30-15)%20-%20FINAL1.pdf

[10] https://www.floridabar.org/member/cle/cler-faq/

[11] https://www.lawsitesblog.com/tech-competence

At roughly the same time, the Electronic Discovery Reference Model (EDRM) was started to deliver leadership, standards, best practices, tools, guides, and test data sets to improve electronic discovery workflow processes. The original EDRM project (it has changed hands twice over the past several years and is now owned by consultants Mary Mack and Kaylee Walstead: www.edrm.net ) came up with the following chart to show a general workflow for eDiscovery projects.

More recently, the multiplicity of data in electronic formats and the increase in digital activity by people in all areas of their lives has led to more confusion regarding ESI and retention standards. According to Georgetown Law, 88% of the US population uses the Internet every day and 91% of the adults use social media regularly[12]and given that more than 90 percent of all documents created today are generated in electronic format, we have seen an enormous rise in ESI in all case types.

Examples of the types of data now included in e-discovery are not just documents but e-mail, databases, web sites, instant messaging, blogs, chat room recording, even audio and video recordings. In fact, any stored information that could be relevant evidence now needs to be reserved.

One result of the rapid growth in not just volume but types of data was a second round of amendments to the FRCP. Passed in 2015, these amendments include:

- FRCP 1 was amended to require the court and the parties (new wording) to construe, administer, and employ (new wording) the rules "to secure the just, speedy, and inexpensive determination of every action and proceeding.". The basis of the changes is to ensure that parties share with the court the responsibility to apply the rules properly. The term "cooperation" appears in the advisory notes[13] and not the rule itself but the notes specifically discuss cooperation as a mandated alternative to the "over-use, misuse, and abuse of procedural tools." (the process of cooperation in litigation will be discussed more in Section 5 below.)
- Rule 26(b)(1) changes the older language on proportionality ("Relevant information need not be admissible at the trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence.") to state that parties may obtain discovery regarding non-privileged matters relevant to any party's claim or defense "*and proportional to the needs of the case, considering the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in*

[12] See Social Media Evidence in Criminal Proceedings: An Uncertain Frontier from Georgetown Law at https://www.crowell.com/files/Social-Media-Evidence-in¬Criminal-Proceedings-An-Uncertain-Frontier.pdf)

[13] The advisory notes are essential to understanding the 2015 Amendments as many of the notes explain how the rules work in practice. Additionally, courts have, more and more, relied on the advisory notes in making rulings. A Comprehensive Overview: 2015 Amendments to the Federal Rules of Civil Procedure, Amii N. Castle https://kuscholarworks.ku.edu/bitstream/handle/1808/25513/5-Castle%2Bchart_Final.pdf?sequence=1&isAllowed=y

*resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit*."

- Rule 37(e) withdraws the earlier "safe harbor" provision with wording that if ESI that should have been preserved in anticipation of litigation is lost because a party failed to take "reasonable steps" towards its preservation, and it cannot be restored or replaced through other discovery, the court can enter Rule 37 sanctions, even without a finding of prejudice.

## Chapter 3: Cooperation

During the same period that the original changes to the FRCP were being implemented, some complimentary efforts were being undertaken by the Sedona Conference (hereinafter Sedona), a nonpartisan law and policy think tank. Sedona published the first edition of *The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production* in 2004 and the document became influential in the eventual recommendations of the FRCP advisory committee. The second amended version of *The Sedona Principles* was released in July of 2007 and a third edition was released in 2018, then updated in 2019.

On October 7, 2008, Sedona released its Cooperation Proclamation (hereinafter SCCP), endorsed by over twenty judges, including the Honorable Judges Shira Scheindlin, Andrew Peck, Paul Grimm, David Waxse, and John Facciola, all leading jurists in eDiscovery. The SCCP was designed to expedite reasonable, just, speedy, and less expensive approaches to e-Discovery mandated by Rule 1 of the Federal Rules of Civil Procedure. To that end, it hoped to shift the focus of the eDiscovery discussion from discovery disputes to litigating on the merits.

Their specific purpose was a reaction to what they termed "an unprecedented crisis" in the litigation arena where: "The costs associated with adversarial conduct in pre-trial discovery have become a serious burden to the American judicial system. This burden rises significantly in discovery of electronically stored information (ESI). In addition to rising monetary costs, courts have seen escalating motion practice, overreaching, obstruction, and extensive, but unproductive discovery disputes – in some cases precluding adjudication on the merits altogether – when parties treat the discovery process in an adversarial manner. Neither law nor logic compels these outcomes." [14]

Judge Paul Grimm extolled the focus of the SCCP shortly after its publication in his memorandum opinion in *Mancia v. Mayflower Textile Services Co.,* 253 F.R.D. 354, 358 (D. Md. 2008). *Mancia* was an employment litigation case in which the parties had reached a discovery impasse that did not even involve ESI. Judge Grimm wrote, however, that "courts repeatedly have noted the need for attorneys to work

[14] https://thesedonaconference.org/download-pub/3802

cooperatively to conduct discovery, and sanctioned lawyers and parties for failing to do so." *Mancia*, supra, fn. 3.

Judge Grimm went on to write that "[p]erhaps the greatest driving force in litigation today is discovery. Discovery abuse is a principal cause of high litigation transaction costs. Indeed, in far too many cases, economics—and not the merits—govern discovery decisions. Litigants of moderate means are often deterred through discovery from vindicating claims or defenses, and the litigation process all too often becomes a war of attrition for all parties." *Mancia*, op cit pp 6-7

He then set forth the essence of the SCCP, observing that:

> . .. there is nothing at all about the cooperation needed to evaluate the discovery outlined above that requires the parties to abandon meritorious arguments they may have, or even to commit to resolving all disagreements on their own. Further, it is in the interests of each of the parties to engage in this process cooperatively. For the Defendants, doing so will almost certainly result in having to produce less discovery, at lower cost. For the Plaintiffs, cooperation will almost certainly result in getting helpful information more quickly, and both Plaintiffs and Defendants are better off if they can avoid the costs associated with the voluminous filings submitted to the court in connection with this dispute. Finally, it is obvious that if undertaken in the spirit required by the discovery rules, particularly Rules 26(b)(2)(C) and 26(g), the adversary system will be fully engaged, as counsel will be able to advocate their clients' positions as relevant to the factors the rules establish, and if unable to reach a full agreement, will be able to bring their dispute back to the court for a prompt resolution. In fact, the cooperation that is necessary for this process to take place enhances the legitimate goals of the adversary system, by facilitating discovery of the facts needed to support the claims and defenses that have been raised, at a lesser cost, and expediting the time when the case may be resolved on its merits or settled. This clearly is advantageous to both Plaintiffs and Defendants." *Mancia*, op cit at p. 12

Shortly after *Mancia*, Judge Shira Scheindlin, in *Securities and Exchange Commission v. Collins & Aikman Corp.*, 256 F.R.D. 403 (S.D.N.Y., 2009) found that the SEC's "blanket refusal to negotiate a workable search protocol" was "patently unreasonable" citing both *Mancia* and the SCCP.

> "Rule 26(f) requires the parties to hold a conference and prepare a discovery plan. … Had this been accomplished, the Court might not now be required to intervene in this particular dispute. I also draw the parties' attention to the recently issued Sedona Conference Cooperation Proclamation, which urges parties to work in a cooperative rather than an adversarial manner to resolve discovery issues in order to stem the 'rising monetary costs' of discovery disputes." *SEC v Collins*, supra at p. 29

Since then, we have had a great deal of discussion about what cooperation means [15] with much of the focus on the challenges of search techniques and the need to confer and agree on search protocols including but not limited to, sampling. As Judge Scheindlin said in *SEC v Collins*: "The concept of sampling to test both the cost and the yield is now part of the mainstream approach to electronic discovery."

And the specific endorsement of Technology Assisted Review (TAR) as a means of speeding up the process was first endorsed by Magistrate Judge Andrew Peck in his order in *Rio Tinto PLC v Vale, SA* 306 F.R.D. 125 (SDNY 2015) We shall discuss that issue more in Chapter 5 below.

But amidst all this talk of search protocol agreements, data sampling and TAR, it seems to me we have overlooked an extremely significant portion of the SCP.

Paragraph 2 states:

> "With this Proclamation, The Sedona Conference® launches a national drive to promote open and forthright information sharing, dialogue (internal and external), training, *and the development of practical tools to facilitate cooperative, collaborative, transparent discovery.* This Proclamation challenges the bar to achieve these goals and refocus litigation toward the substantive resolution of legal disputes." (Emphasis added)

It seems to me we need more discussion about those "practical tools" which will then promote the ability to cooperate. We already have web-based applications which allow the posting and sharing of documents. These tools are now used routinely on large cases, and they are crucial for not only cutting costs but quickly and easily disseminating information to both sides of a case, which then allows quicker progress of the entire action.

But the culling down of enormous data sets to a manageable size for review is also an essential tool. Tools like these enable early low-cost access to any data set without the need to incur the full cost of native processing and thus make data available faster while reducing costs. This is the new generation of "*… practical tools to facilitate cooperative, collaborative, transparent discovery"* called for by the Sedona Conference Cooperation Proclamation.

For small cases, this approach is crucial. It means that the ultimate solution is more than just knowing the rules, avoiding e-jargon, and understanding the technology. The key is good lawyering and understanding the scope of *all* the procedural rules, not just those dealing with ESI.

[15] see a complete list at the Sedona site https://thesedonaconference.org/cooperation-proclamation

In fact, a good argument can be made that small cases require an even greater level of understanding of these factors than larger cases. With larger cases, you typically have bigger budgets and more room to make mistakes. In small cases, a targeted plan of attack must be developed from the outset that will be sufficiently thorough to provide relevant discovery yet cost effective so the more limited budget will suffice.

Given the discussion above, what is the average practitioner to do to effectively manage e-Discovery in small cases? There are some practical ways in which you can approach the issue that can help. The first thing you can do costs nothing apart from the time spent thinking as a good lawyer. It is probably the most important thing you can do to minimize costs.

Take the time to think through what you really want to accomplish in terms of discovery of ESI. Make your requests targeted and specific enough to elicit exactly what you need for your case. Too often lawyers use the all-encompassing approach of casting the widest net possible. This obviously magnifies the cost of discovery. It might be done as a strategy, but more often it is done because it is easier.

While asking for everything does not require you to think about your case and determine early on what you need to meet your burden of proof, if you carefully tailor your requests, you can limit the amount of work that must be done. Which will lessen the amount of data that must be processed and reviewed. You will also have a good argument to persuade your opposing counsel to do the same or a judge to allow your motion for a protective order, thereby lessening your client's costs in responding to e-Discovery requests.

How do you go about performing effective triage at the outset? In federal court, and many state courts as well, you have a great tool: the FRCP 26(f) meet and confer conference.

My recommendation is to meet early and meet often. Although there may be a mandatory requirement to have at least one meet and confer, you are not limited to one meeting. If you meet early with your opposing counsel, you can take steps to define what they have, let them know how you feel they should preserve it and discuss how it should be collected in the most cost-effective way possible. You can do the same for your client's ESI so you can minimize your own expenses in terms of preservation and production concerns.

Next, know what you really want to accomplish in working with ESI. If you are not concerned with deleted information, you probably do not need the help of a computer forensics expert. On the other hand, if you do need the help of such an expert, that determination should be made quickly, and collection efforts should occur as soon as possible to avoid the inadvertent loss of information due simply to the normal operation of computer systems.

If you are not really concerned with metadata, you might be able to use less expensive collection options that do not preserve the metadata associated with the ESI you are collecting. Often, you are only looking for a copy of a file and do not care

about the metadata of the original. If you know what you are doing and what you are giving up, you can minimize collection costs by stipulation.

Even if you do need to preserve metadata, there are relatively inexpensive options available that you can use without hiring expensive outside consultants. It may take a higher level of technical ability on your part, and you must determine if you are comfortable engaging in self collection methods. If you a comfortable with these options, then you can negotiate with the other side to use the appropriate software tools.

The point is that you never want to make these decisions in the dark, which is why the issue should be dealt with at a meet and confer.

One technique that can also be considered at a meet and confer is the use of phased discovery. Why demand the ESI from every potential witness in a case when a more targeted approach might better serve your need? Agree to limit initial collection efforts to the key custodians you want and that if discovery of their ESI proves fruitful, you can move on to collection from other, more peripheral players. If this does not produce much of value with the key witnesses, you can safely move on to other witnesses. Even with key witnesses, consider a phased approach by using sampling techniques. Before you demand production of an individual's full file shares from a company server, consider whether you should first review just their e-mail files. If that analysis turns up attachments that are relevant, then you can move on to file shares or other locations on the file server.

Limit the type of information you seek initially. If you are not looking for financial data**,** then do not demand production of all spreadsheet files. If there is a limited date range at issue, do not ask for every document on the server; ask only for those that fall within the pertinent date range. If you can limit the scope of what you are looking for using key words, try filtering on key words. It might get you what you want right away. If key word searching is unsuccessful, you can then consider broadening the search or abandoning it altogether.

If you are a lawyer who does not have a great deal of experience in eDiscovery, get some help—the earlier the better. Hiring a consultant who can help you develop a streamlined eDiscovery plan may cost some money up front, but in terms of avoiding the cost of spinning your wheels or making mistakes, the overall expense will be lessened.

And be sure to engage the right kind of consultant to help you. Vendor-neutral consultants typically do not have a vested interest in using one specific product or procedure. A vendor-affiliated consultant always has a biased agenda. The bias may be useful to your case but be aware of what you are getting.

Planning, a targeted approach to discovery, cooperation between counsel, and the use of the proper tools to meet your specific case needs can help you lessen the cost of e-Discovery in smaller cases. There are many practical technology options available short of a dedicated litigation support database solution to meet your needs in smaller cases. You must find what works best for you within the budget you have available and the particular ESI you must manage.

But the ultimate solution is more than just heeding to the admonition above about knowing the rules and understanding the technology. In my estimation, it is the process not the technology. As Craig Ball once said, "The key consideration is workflow" and another noted eDiscovery expert, John Martin, once remarked "it's the archer, not the arrow."

The fact is that technology is not the key to successful management of e-discovery in small cases. Rather, the single most effective way to keep eDiscovery costs low is to work with your opposition in a cooperative manner so you can stipulate to the use of low-cost solutions.

We all must change to the new paradigm of working in the digital world. In the words of The Hon. Lee Rosenthal, former Chair of the Standing Committee of the Judicial Conference, "Litigation habits and customs learned in the days of paper must be revisited and revised. The culture of bench and bar must adjust."

## Chapter 4: The Checklist Manifesto

Given all the discussion in the section above, it is my firm belief that the best way to proceed in handling eDiscovery matters is to have checklists for each step of the process. The eDiscovery Checklist Manifesto (EDCM) is a complete workflow for the steps every legal professional should consider as they conduct litigation and eDiscovery.

This guide was updated by Bill Gallivan, Managing Director at Digital WarRoom, and you can download the most current version at Digital WarRoom - The Checklist Manifesto.


Our EDCM diagram represents a conceptual, iterative process. One might repeat the same step numerous times, homing in on a more precise set of results. One might also cycle back to earlier steps, refining one's approach as a better understanding of the data emerges or as the nature of the matter changes.

The outer circle represents the generally prevalent common steps which may occur in the eDiscovery process while the inner circle represents more unique common steps which may occur at any point in the process.

The diagram is intended as a basis for discussion and analysis, not as a prescription for the one and only right way to approach eDiscovery.

## The eDiscovery Checklist Manifesto (EDCM) – Specific Unique Tasks

- **Client Consultation**: Points to consider and discuss in the initial client meeting There are consultation points that every attorney should cover or consider in the initial discussion with client. These may refer to the EDCM steps such as ID, Preservation, and Collection. Consultation can occur at any time but should occur before any specific litigation to adequately prepare the client in a proactive manner for issues that may arise should litigation occur. Consultation may then occur cyclically throughout any specific project and will flow into the Strategy checklist set out further below.
- **Identification**: Identify and validate potentially relevant ESI sources In the EDRM process, the legal team uses the identification phase to develop and execute a plan to identify and validate potentially relevant ESI sources including people and systems. The scope of this data may be uncertain in the early phases of a legal dispute and may change as the litigation progresses. But learning the location of potentially discoverable data is necessary to issue an effective legal hold in the Preservation stage.

- **Preservation**: Prevent potentially relevant data from being destroyed after litigation becomes apparent. Keep in mind, however, that the duty to preserve relevant data does not always flow from a litigation hold notice. It may arise under a common law obligation or under a statute or regulation. The Committee Notes to FRCP 37 (e) state, in part, "Many court decisions hold that potential litigants have a duty to preserve relevant information when litigation is reasonably foreseeable. Rule 37(e) is based on this common-law duty; it does not attempt to create a new duty to preserve." In the federal and most state

courts, there is no tort cause of action for the intentional destruction of evidence after litigation has commenced. [1] But since such destruction constitutes abuse of the discovery process, it is subject to a broad range of sanctions. These sanctions are, however, intended to remedy discovery abuse, not to punish the offending party.

- **Interview Custodian**: Identify and review all custodians who may be relevant to the litigation. Identify and review all custodians who may be relevant to the litigation. Simple and straightforward questions often elicit the most helpful answers and should be focused on the time frame and data questions at the center of the dispute.

- **Collection:** acquisition of potentially relevant ESI as defined in the Identification phase. Collection is the acquisition of potentially relevant electronically stored information (ESI) as defined in the Identification phase. The process of collecting ESI will generally provide feedback to the Identification function which may then influence or even expand the scope of the eDiscovery project. The needs of a case may require a forensic preservation of certain materials; other times, custodian our counsel directed self-collection and forensically sound copying of email containers (PST, MBOX) or making and archive from a hosted email service or file share may be appropriate. Keep in mind that collection is NOT the same as preservation, which is described above. Collection is the first step in th e ultimate review process and should be done subject to some specific review goal. Collection processes may be in person or remote and typically account for roughly 13% of the entire cost of an eDiscovery project. Do not fixate on the containers — the e-mail, spreadsheets and databases — with insufficient regard for the content. Some examples of common failure of producing parties and requesting parties include: Focus on getting the other side's tapes and hard drives when unable to articulate what they're seeking. Saying, "I want the e-mail" is as meaningless as saying, "I want the paper.". E-mail, voicemail, ledgers – even a mirror with Lipstick on it - is just media used to hold and convey information. Most importantly, it's the transaction and the content that make them evidence:

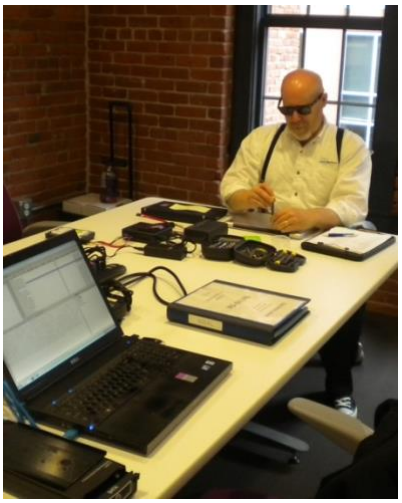


*Figure 1: Forensice Collection of Evidence*

    - Form only matters for reasons of accessibility (Can I view/hear it?)
    - preservation (How do I protect it?),
    - utility (Can I search and sort it?),
    - completeness (Is something added or absent?) and
    - authentication (Can I rely on it?).

- **Processing**: Electronically prepare ESI for review After collection, it is often necessary to "process" data to prepare it for review. This involves machine-based manipulation of all the various data sets collected into a common format for use in a software review tool.

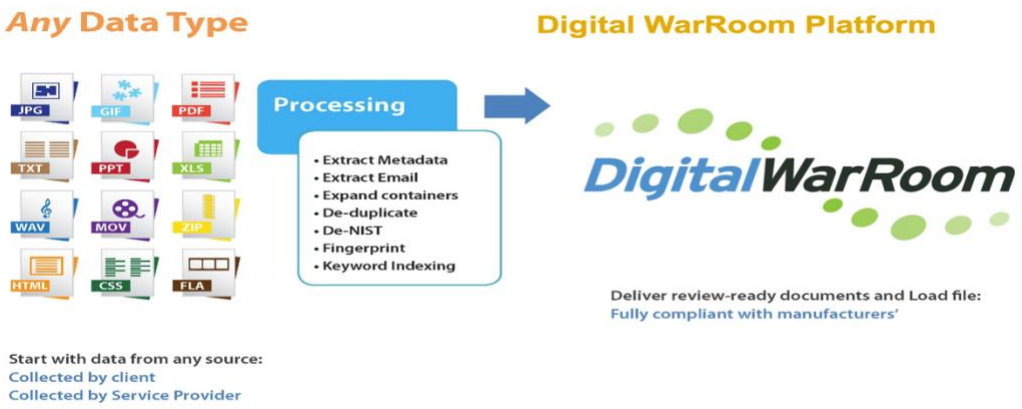



*Figure 2: Processing Data*

- **Review:** Search, examine, and assess processed ESI Document review is a critical component in the eDiscovery process and is used to identify, classify, categorize, and prepare for production a variety of document types. Most analyses of the eDiscovery process agree that this is the most expensive step in that process and can often account for as much as 70% of the eventual spend. Given that pricing prominence, it is critical that this stage be handled efficiently**.**

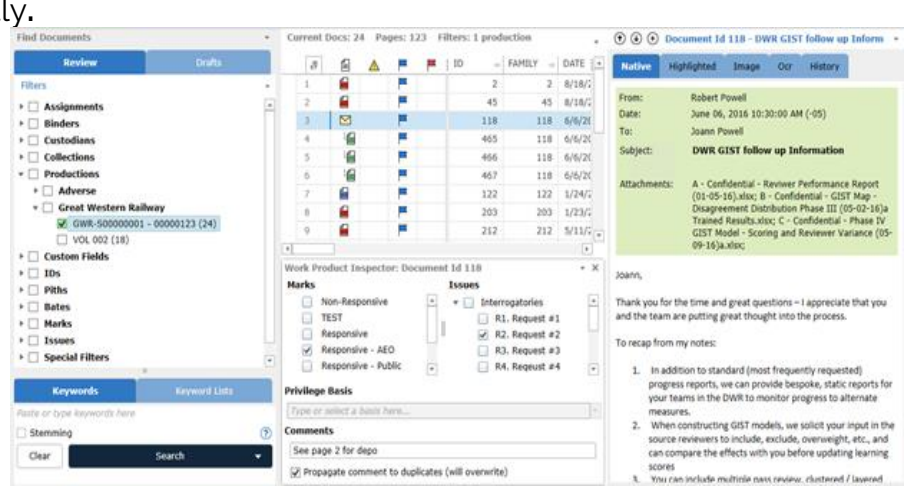


*Figure 3 Review Panel: Filter Tree, Result List, Document Browser*

- **Analyze:** Detailed examination and scrutiny of reviewed ESI In the original EDRM model, analysis was a standard function of the Review process and was primarily manual. But as more sophisticated analytics tools have emerged, this phase has drawn more attention as an area to increase productivity.

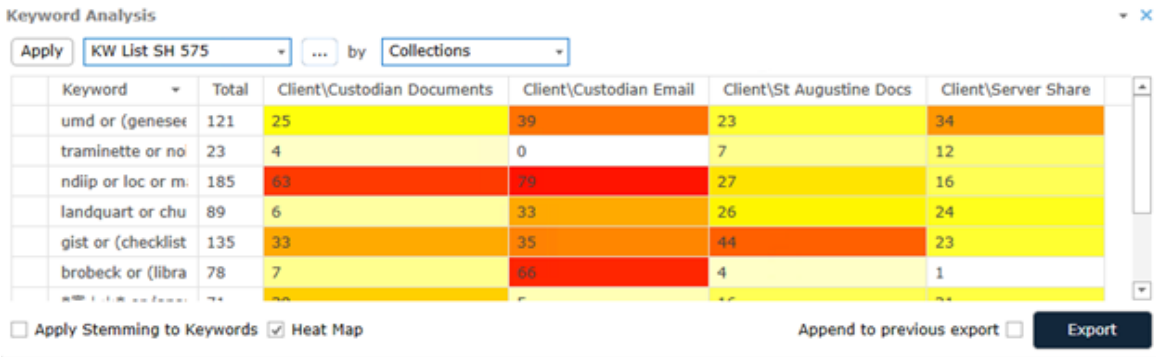



*Figure 4: Keyword Analysis - Hits by search string*

- **Production**: Proposed formats & methods - the production of ESI continues to present significant challenges in the discovery process. FRCP Rule 26(f) posits that the method and format of production shall be included in the discovery plan.

## The eDiscovery Checklist Manifesto (EDCM) – Common Tasks

These common tasks fall generally under the heading of Project Management. For a greater consideration of that topic, the author recommends that you read Project Management in Electronic Discovery: An Introduction to Core Principles of Legal Project Management and Leadership by Michael I. Quartararo

- **Strategy:** A comprehensive strategy will be the single greatest factor in controlling your litigation. It should be dynamic, flexible, and reviewed periodically. DWR has long been centered on risk analysis as a key component of their strategic approach to eDiscovery, not just in weighing relevant eDiscovery obligations but also exploring methods of managing cost vs risk. Tom O'Connor and Bill Gallivan have discussed that balance in webinars as well as a live presentation at the ABA TechShow 2020. A slide from that presentation is shown below and the entire presentation can be viewed at https://www.digitalwarroom.com/webinars.

- **Risk Analysis:** Cost vs risk analysis of case – Best Practices must support intelligent cost / risk decisions with Defensibility, Reasonableness, and Proportionality being your guides.

- **Budget:** Contemplated costs & damage assessment. FRCP 1 requires matters be handled in a manner that is "just, speedy and inexpensive." Having a budget will be important for discussions with not only your client but the Court when discussions arise about proportionality or eventual final cost awards. Once you have completed the various steps specific to your process in the EDCM checklist, you will be ready to proceed to using software to perform those tasks.

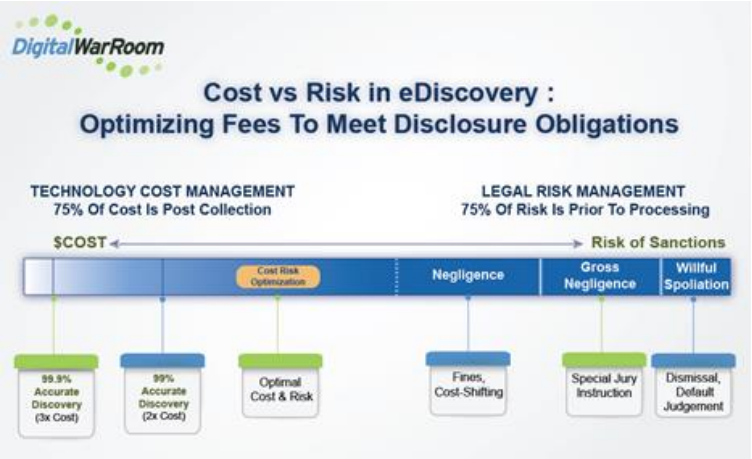



*Figure 5: Balance Legal Risk and Budget Risk*

## Chapter 5: Managing eDiscovery … meet Digital WarRoom

We will now turn to a discussion of strategic uses of Digital WarRoom (DWR) in the overall eDiscovery workflow. But before we get to a detailed list, let's get a sense of overall strategy. And what better sources of that than the co-founders of DWR, Dan and Bill Gallivan.

The Gallivan brothers have a deep and varied background in technology. Bill is a US Navy veteran and after completing his service he managed the commercialization of many technologies that were developed in the Ohio Supercomputer Center at The Ohio State University. Dan worked at several software startups, most notably as a graphic design software pioneer at Aldus.

After Adobe acquired Aldus, Dan helped Am Law 100 firm K&L Gates launch the eDiscovery software and services company Attenex in the early 2000s. Dan recruited Bill to help Attenex grow and after a successful stint there, K&L Gates decided it didn't want to be in the software business and sold Attenex. Realizing they made a good team in business as in life, Dan and Bill founded Digital WarRoom

What was their goal with DWR? Bill says "Our goal has always been to make dispute resolution affordable. We focus on FRCP 1 — ensuring client matters are Just, Speedy, and Inexpensive."

Dan says, "Whenever we learn about critical eDiscovery workflow errors, our product managers ask, "How can we code a "guardrail" that prevents that from happening? Guardrails are a product development priority for Digital WarRoom."

For more with the Gallivan brothers and their vision as applied at Digital WarRoom, please see the interview '[Making ediscovery Accessible, Safe, and Profitable for Law firms of All Sizes]'.

Digital WarRoom provides eDiscovery software which can be deployed as a cloud based, or installed on-premise. Digital WarRoom can accelerate processing, early case assessment, review, production and data management for law firms, legal departments, corporate legal teams, and government agencies. This software is fully do-it-yourself (DIY), meaning legal professionals can process, review, and produce electronic documents within a single end-to-end platform - without the need for a service provider or a third party to intervene.

Standard features include automated processing, duplication, and policy management, reviewing and tagging documents, creating privilege logs, redacting text as needed, producing responsive documents in a variety of formats, and creating document sets for expert interviews or deposition preparation. For small cases, you can often process data and review documents within a single day.

## Real World Strategy

Given this framework, what can the average practitioner do to effectively manage e-Discovery in small cases? There are some practical ways in which you can approach the issue that can help.

The first thing you can do costs nothing, apart from the time spent in thinking as a good lawyer. It is probably the most important thing you can do to minimize costs.

Take the time to think through what you really want in terms of discovery of ESI. Make your requests targeted and specific enough to elicit exactly what you need for your case. Too often lawyers use the all-encompassing approach of casting the widest net possible and this invariably magnifies the cost of discovery.

It might be done as a strategy, but more often it is done because it is easier to do. Asking for everything does not require you to think about your case and determine early on what you need to meet your burden of proof. If you carefully tailor your requests, you can limit the amount of work that must be done and lessen the amount of data that must be processed and reviewed. You will also have a good argument to persuade your opposing counsel to do the same, thereby lessening your client's costs in responding to e-Discovery requests.

How do you go about performing effective triage at the outset? In federal court you have a great tool: The meet and confer conference. Many states have similar provisions in their state civil procedure laws. Our recommendation is meet early and meet often. Although there may be a mandatory requirement to have at least one meet and confer, you are not limited to just one. If you meet early with your opposing counsel, you can define what they have, let them know how they should preserve, and determine how it should be collected in the most cost-effective way possible. You can do the same for your client's ESI and thus minimize your own expense in terms of preservation and production concerns.

Next, know what you really want. If you are not concerned with deleted information, you probably do not need the help of a computer forensics expert. On the other hand, if you do need the help of a such a professional, that determination should be made quickly, and collection efforts should occur as soon as possible to avoid the inadvertent loss of information due simply to the normal operation of a computer system.

If you are not really concerned with metadata, you might be able to use inexpensive collection options that do not preserve the metadata associated with the ESI you are collecting. Often you are only looking for a copy of a file and do not care about the metadata of the original. Even if you do need to preserve metadata, there are relatively inexpensive options available that you can use without hiring costly consultants.

It may take a higher level of technical ability on your part, and you must determine if you are comfortable engaging in self-collection methods, but there are lower cost options available. If you are comfortable doing that, then you can negotiate with the other side to use appropriate software tools to collect the ESI that you must produce and what you want produced by your opponent.

One technique that can be considered at a meet and confer is phased discovery. Why demand the ESI from every potential witness in a case when a more targeted approach might better serve your needs? Agree to limit initial collection efforts to the key custodians you want and agree that if discovery of their ESI proves fruitful, you can then move to collection from other, more peripheral players. If the process does not produce much of value with the key witnesses, you can safely skip other witnesses.

Even with key witnesses, consider a phased approach by using sampling techniques. Before you demand production of an individual's full file shares from a company server, consider whether you should first review just the e-mail files from the e-mail server. If that analysis turns up attachments that are relevant, then you can move on to the file server.

Limit the type of information you seek initially. If you are not looking for financial data**,** then do not demand production of all spreadsheet files. If there is a limited date range at issue, do not ask for every document on the server; ask only for those that fall within the pertinent date range. If you can limit the scope of what you are looking for using key words, try filtering on key words. It might get you what you want right away. If key word searching is unsuccessful, you can then consider broadening the search or abandoning it altogether.

If you are a lawyer who does not have a great deal of experience in eDiscovery, get some help—the earlier the better. Hiring a consultant who can help you develop a streamlined e-Discovery plan may cost some money up front, but in terms of avoiding the cost of spinning your wheels or making mistakes, the overall expense will be lessened. Hire the right kind of consultant to help you. Vendor-neutral consultants typically do not have a vested interest in using one particular product or procedure. A vendor-affiliated consultant always has a biased agenda. The bias may be useful to your case but be aware of what you are getting.

Planning, a targeted approach to discovery, cooperation between counsel, and the use of the proper tools to meet your specific case needs can help you lessen the cost of e-Discovery in smaller cases. There are many practical technology options available short of a dedicated litigation support database solution to meet your needs in smaller cases.

## Specific Tips

You must find what works best for you within the budget you have available and the particular ESI you must manage. Here are some specific tips for what to do on a limited budget.

1. Read the Rules: The Federal Rules of Civil Procedure (FRCP) lay out the framework for your obligations in handling e-Discovery and differ in several aspects from traditional discovery rules. In addition, your state may have its own eDiscovery rules which differ from the FRCP. You need to understand the procedural requirements for the various jurisdictions where you may have litigation arise so start there.
2. Read the Decisions: Federal judges have spent considerable time issuing opinions which give details on interpreting and implementing the Federal rules. Reading these decisions is essential to understanding how to handle e-discovery so start with a good book on e-Discovery basics and then subscribe to a good eDiscovery case update blog with an RSS feed that notifies you automatically every time something new is posted.
3. Know the Terms: eDiscovery isn't rocket science, but it is technical in nature. You learned the Rule against Perpetuities in law school so believe me you can handle this. Judges do not want to waste time settling arguments between attorneys who don't know the difference between a PST and an MSG file so get a good eDiscovery glossary (EDRM has several at http://www.edrm.net/resources/glossaries )
4. Know Where Your Data Is: You can't find it to identify, collect and preserve if you don't know where it is. So, get with your clients' IT folks and make a map of their network with locations, custodians, OS, and applications lists and descriptions of data amounts. Why? Because a map shows us how to go places, we haven't been before without getting lost. Additionally, they are incredibly useful in court to show a judge the complexity of your data collection problem.

5. Talk to The IT department: You're Lewis and Clark, they're Sacajawea. They know how to make the map. You cannot …absolutely cannot … navigate without them.
6. Talk to The Records Management (RM) people: Records Management is the flip side of the eDiscovery coin, and your clients RM staff can help avoid the need to waste time and money restoring backup tapes that don't contain relevant data. Wait, your client DOES have a Records Management Policy, right?
7. Make a Records Management Policy: Good records management will save time and money when clients need to collect data and will help avoid sanctions when you have to explain to a judge why some documents are no longer available because they were deleted in the ordinary course of business as outlined by the records retention policy.
8. Make A Litigation Hold Policy: Every client needs to have a clear and concise litigation hold policy to deal with procedures for data retention when the litigation hold letter arrives. And it will.
9. Enforce the Litigation Hold Policy. Repeat after me: "repeatable, defensible process". Don't put the lit hold policy in a manual that just goes on the shelf. This is the biggest mistake you can make, and more cases are lost here than in any other phase of electronic discovery. Your opponent marks up a motion for sanctions, you say, "but Your Honor, we have a lit hold policy" and the judge says, "show me how you implemented it in this case." And you can't.
10. Meet with inside counsel. Why? To discuss all the above. They will need to understand, and be able to explain, all of it in order to work with you. And you need to be sure they can do exactly that.

## Working With the Data

The next step is how to work with the data. In that regard, there are several basic considerations for working with eDiscovery in small cases. They are:

Work with data in its native format. The types of files you will be dealing with are likely typical or standard files created by common programs used for email, word processing and other office functions.

Control the data yourself. There are many good, hosted solutions that can fill your needs, but the typical storage fees charged for a case that exists for any length of time can bust a modest technology budget. DWR is specifically designed and priced to solve that problem.

Keep the data sets manageable. This means getting agreements to dedupe and cull data down BEFORE you receive it, whenever possible.

Agree on exchange protocols. The single most effective way to keep eDiscovery costs low is to work with your opposition in a cooperative manner so you can stipulate to the use of low-cost solutions.

## What do Users Say?

The above sections discussed my analysis of eDiscovery workflow strategy. But what do actual users say about how they work? One source is the annual eDiscovery Business Confidence Survey conducted by Rob Robinson of Complex Discovery (https://complexdiscovery.com/). The top five concerns of respondents in the 2020 survey are:

1. Increasing Volumes of Data
2. Data Security
3. Increasing Types of Data
4. Lack of Personnel
5. Inadequate Technology

For only the second time ever (and the second time in a row), one of the factors – Budgetary Constraints – was selected by a majority (**56%**) of the respondents as being most impactful over the next six months, breaking its previous high of 51.2% and 25.7% above average.

Increasing Volumes of Data and Increasing Types of Data were tied at a very distant second at **14%**, over seven percent and two percent lower than lifetime survey averages of 23.1% and 16.3%, respectively. Data Security was fourth at **7%** (which is nearly seven percent below its lifetime average), Lack of Personnel fell from third to fifth at **6%** (over six percent lower than its lifetime average of 12.6%) and Inadequate Technology (once again) brought up the rear at **3%** (over five percent lower than the lifetime average of 8.4%). (Source: https://ediscoverytoday.com/2020/07/16/is-business-confidence-optimism-heating-up-in-the-time-of-covid-19-ediscovery-trends/)

The general distinction between plaintiff and defense firms with regard to eDiscovery was best noted by eDiscovery blogger, Attorney Craig Ball who said:

> "The challenges faced by plaintiffs' lawyers confronted by e-discovery flow from structural differences in practice. Plaintiffs' lawyers operate as small firms and solos who finance their cases and are compensated on contingency. So, plaintiffs' lawyers tend toward frugality (as they are spending their own money) and shy away from capital expenditures that cannot be reliably expensed against the matter. Plaintiffs' lawyers tend not to possess (or need) the costly in-house IT operations of large defense firms and, crucially, plaintiffs' lawyers don't have large support staffs for IT and litigation support because the cost of same can't be spread across hundreds or thousands of lawyers."
>
> "Without in-house e-discovery teams at the ready, plaintiffs' lawyers are more apt to "wing it" or seek expertise only when obliged to do so on an *ad hoc* basis."

In a separate study I ran in 2019, I asked a number of plaintiffs' attorneys to describe the general differences between plaintiff and defense firms in eDiscovery and their top three eDiscovery pain points in eDiscovery work.

And the following were their specific replies

1. **Short Sightedness, Competence, No tools/training**
2. **Cavalier Attitude, No knowledge of IT, Lack of tools**
3. **Cooperation, Protocols, Motion practice**
4. **Producing party issues, Protocols, Search terms**
5. **Competence, Data Dumps, Search terms**

The most popular answer was cooperation but also of concern was the protocol issue. As one attorney said,

> "... there is, it seems, frequently, an almost cavalier attitude to understanding eDiscovery technical aspects and a lack of necessary skills in connection with the subject of forms of production, for instance. This sometimes extends to eDiscovery jurisprudence, as well and leads to inefficiencies and lack of defensibility in the production of ESI."

Project Management

Finally, we should not overlook project management. Mike Quartararo, the President of ACEDS, is well known for his book, "Project Management in Electronic Discovery: An Introduction to Core Principles of Legal Project Management and Leadership in EDiscovery" in which he states that

> "… eDiscovery PM comes only after you have a firm grounding in general project management principles. Those principles are ideally suited to a project which has repetitive and dependent tasks, a variety of people and organizations involved and the need to better manage scope, timing, and costs."

Which of these principles can we use in eDiscovery? I'd suggest the following points made by Mike as being the most critical:

1. **Cost**: The ability to estimate, budget, and manage the costs of the project.
2. **Scope**: What Mike calls "What does "done" look like?"
3. **Time**: The Project Management Lifecycle to avoid missed deadlines and fragmented schedules which lead to added cost
4. ***Tools & Techniques****:* What tools are required, including written protocols or best practices?
5. ***Output:*** requirements during and at the conclusion of an ESI project

## Closing Thought…

The ultimate solution is more than just knowing the rules, avoiding e-jargon, and understanding the technology. In our estimation, it is the process not the technology.

We are not alone in this appraisal. Technologist John Martin once commented, "It's the archer not the arrow." Craig Ball says, "The key consideration is workflow".

The fact is that technology is not the key to successful management of discovery in small cases. Rather, the single most effective way to keep eDiscovery costs low is to work with your opposition in a cooperative manner so you can stipulate to the use of low-cost solutions.

We all must change to the new paradigm of working in the digital world. In the words of The Hon. Lee Rosenthal, former Chair of the Standing Committee on the Rules of Practice and Procedure, "Litigation habits and customs learned in the days of paper must be revisited and revised. The culture of bench and bar must adjust."