

Module 11: Preservation of Electronically Stored Information

Learning Outcomes

Upon completion of Module 11, students will be able to:

- Defend the need for integrity and availability of any electronic evidence that will potentially be included in an e-discovery process.
- Classify any data that are part of an e-discovery process
- Rank data based on its sensitivity, privilege or need for confidentiality as part of a risk management process.
- Compare and contrast the options for access control and management for electronic evidence that needs to be preserved and protected.
- Evaluate the categories of an entity's data and recommend the most appropriate strategies for organizing that data, including how to manage the data over time and to prepare for litigation or an audit.
- Assess the options for storing data, including using cloud computing vendors.
- Justify the need for robust solutions for storing data for litigation readiness as well as disaster planning and business continuity.
- Illustrate the steps in a litigation hold process.
- Outline what should be covered in a service level agreement with a cloud computing vendor.
- Summarize the important points in Module 11 and the reading assignment.

Please read Chapter 6 in *Electronically Stored Information: The Complete Guide to Management, Understanding, Acquisition, Storage, Search, and Retrieval*, 2nd ed. See also Appendix III on pages 291-292.

Please also read the following, included as part of Module 11.

- The Duty to Preserve Extends to 3rd Parties and Their Texts (*Ronnie Van Zant, Inc. v. Artemis Pyle*) – from Exterro (for all of you who remember the band Lynyrd Skynyrd)
- Preservation/Legal Hold Workflow – from Exterro
- Want to Save Money In eDiscovery? Here's a 3-Step Plan – from *Above the Law*
- Have I Got a Deal for You: Selling TAR Like a Pro – from *Peer to Peer*
- See also the website for Pinpoint labs, which offers a variety of software and services, including SafeCopy2 and Harvester, as tools for collecting ESI <http://pinpointlabs.com/>

By Wednesday, November 13 at 11:59 P.M., please respond to the questions for Discussion Forum #6 (covers Module 10 and Module 11):

- Of the various kinds of data described in Chapter 5 of *Electronically Stored Information: The Complete Guide to Management, Understanding, Acquisition, Storage, Search, and Retrieval*, 2nd ed., select one and describe. How is this data generated and where does it reside? Is it easy or difficult to collect and why? What are any special considerations with collecting this data?
- Describe a document/data/electronic evidence that you would want to avoid having to produce to the opposing party. What kind of information does this item contain and why do you want to protect it? Under what doctrine (attorney-client privilege, attorney work-product, another confidentiality doctrine)? If you were the lawyer, what arguments would you make and what would you have to show?
- Have you used any of the techniques/tools/methods outlined in Chapter 5 to look for data (hidden, deleted, corrupted, encrypted, created using proprietary software, stored on obsolete media)? If so, what did you use and how did it work out? If not, I invite you to try some of the suggestions from the author using features of the software that you already have available to you. Were you surprised by how easy/difficult this was and what you were able to access?
- What are some of the considerations for storing data? What should we do to be certain that our data is secure in the event of a disaster or threat? What are some of the issues with choosing a cloud computing vendor for storage versus using physical devices?
- Please **REPLY** to another student who participated in the questions for Discussion Forum #6. What options did the student recommend for controlling access to information/data? What else did the student identify that could add an extra measure of protection, particularly for truly sensitive information/data? What else would you suggest?
- Any other surprising or interesting points from Module 10, Module 11 or the reading assignment.

Please read the following mini-lecture.

Cartoon Caption Contest



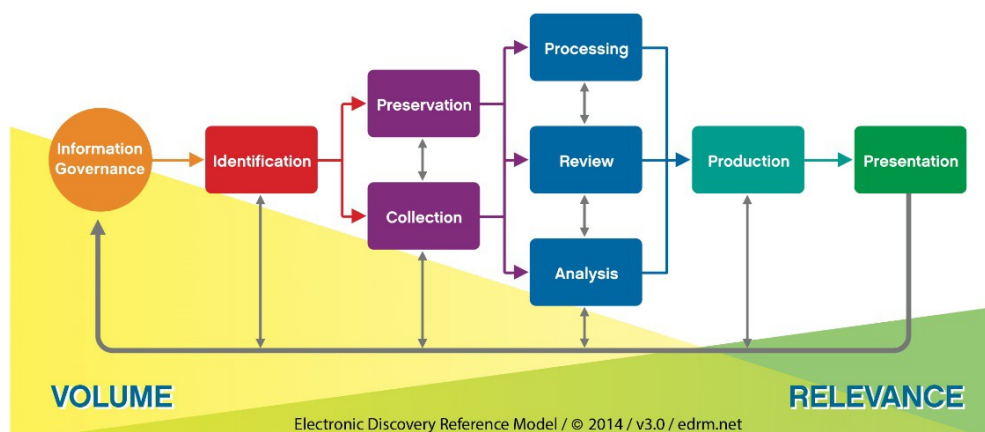
“Unwilling to adapt to current law office technology, Fred was forced to relocate his practice.”

—Milena Capezzuto of Scottsdale, Arizona

This cartoon is particularly appropriate. On July 31, 2017, the Indiana Supreme Court issued an order amending Comment [6] to Rule 1.1. Effective January 1, 2018, Comment [6] to Rule 1.1 states “To Maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with the technology relevant to the lawyer’s practice....”. This is a significant addition to Indiana’s Rules of Professional Conduct.

With Module 11, we move to the preservation stage of an electronic discovery process. It is helpful to visualize this process using the EDRM, which we were introduced to earlier in the semester. Recall that Module 9 was devoted to information governance/litigation readiness and that Module 10 covered collection of electronically stored information. Note that the preservation and collection steps are iterative and not linear. The volume of electronic evidence that we might have to handle has been reduced, but the relevance of that evidence has increased.

Electronic Discovery Reference Model



Our reading assignment, Chapter 6 in *Electronically Stored Information: The Complete Guide to Management, Understanding, Acquisition, Storage, Search, and Retrieval*, 2nd ed. covers the procedures for preserving electronic evidence. As stated on page 223, “[o]ne of the most important tasks an organization or individual will face when dealing with electronic evidence is the preservation of that data in a way that ensures the integrity (guaranteeing that nothing about the data changes as you move and manage the data) and availability (ensuring that the data are easily and efficiently accessible) of the data.” As indicated on page 223, the first thing to consider is the actual classification of the data, because this will inform you as to the degree to which you need to secure it. For example, private information about a client, intellectual property or critical infrastructure, attorney work-product or information that could be protected under attorney-client privilege or another confidentiality doctrine will need to be classified as sensitive or confidential.

As the author indicates on page 224, making decisions about how to secure information will always be a classical risk management exercise, wherein we weigh the risks in terms of the vulnerabilities and threats that the information could be lost, compromised or revealed. As the author notes on page 225, in other instances, we will not only have the motivation, but also a legal/ethical responsibility to secure the data that we have acquired. The author provides an example of a patent for technology that enables one of the features of a new smart phone on pages 225-226. An analysis of the risk indicates a greater need to expend resources and time to secure the data and mitigate the risks. As he observes on page 226, once we have completed a risk management assessment, we are ready to consider the procedures and protocols for actually protecting the data.

In terms of access control and management, the author indicates that the actual storage media for data is of relatively little consequence compared to the considerations for preservation. As long as the media are reliable, physically robust and accessible, we might consider a number of options, such as DVDs, CDs, hard drives and even cloud computing vendors. He goes on to state that when we consider the security and integrity of the data, what really matters are the controls around who can access the data and how those controls are managed. Approaches for managing access to the data include:

- Authentication – see pages 227-228 and Figure 6.2. Note that when the classification of data justifies a higher level of authentication, we may want to use two- and even three-factor authentication.
- Encryption – see pages 228-229
- Identity management – see pages 229-230
- Logically compartmentalize the data – see pages 230-231
- Physical separation of data storage – see page 231

As indicated on page 232, “to ensure the efficient availability of your electronic data, you need to consider the management of that data and how the data are best organized.” As indicated in the caption for Figure 6.3, managing our files carefully is one of the main foundations of data control. The author provides several use cases to illuminate our choices about how to manage data.

- Simple day-to-day organization of data for business or personal use – see pages 232-236
- Management of data over time – see pages 236-238
- Response to litigation or audits – see pages 238-241. As the author notes on page 238,

one of the most compelling reasons for careful and consistent management of our electronic data is the inevitable need to produce those records for a legal action or audit. As the author describes how only a small part of the data “pie” will be relevant and required for litigation or an audit, recall the EDRM and how the volume of potentially relevant electronic evidence has decreased as the relevance of the remaining electronic evidence has increased. Note the important point on page 239: “The fact that you have well-documented records management rules means nothing if your employees either do not know about them or have not been following them.” See the information on page 240 about Judge Peck’s approval of the use of predictive coding and computer-assisted review (which could also be called technology-assisted review, or TAR) and the article about TAR from *Peer to Peer*, included as part of the supplemental materials for Module 11.

The author devotes a number of pages in Chapter 6 of *Electronically Stored Information: The Complete Guide to Management, Understanding, Acquisition, Storage, Search, and Retrieval*, 2nd ed. to considerations for safe storage, which he asserts is one important component of establishing and ensuring the integrity of the data. As he notes on page 241, securing access to data through good identity management systems, encryption and segregation of different systems is our first line of defense. A second consideration is the actual physical storage, which includes disaster recovery and business continuity planning and encompasses backup and restoration procedures and emergency readiness and resilience. (You would be shocked at the percentage of law firms that do not have these kinds of plans in place.)

One thing people forget about is security for the physical space where their data reside, whether this is the room housing the network server, a laptop or a mobile device. This may include not only limiting access by using robust security measures such as cameras and authentication measures, but also sufficient cooling capacity and redundant power supply or backup. The author suggests that you try to visit a large data center, if you can obtain the security clearance to do so. As he notes on page 242, “[w]hatever your physical storage medium, you should ensure that it is safe from intruders and disasters to whatever extent is possible and makes sense from a risk management perspective.” He recommends testing these systems on a regular basis.

There are many options for backup systems, including cloud computing vendors. As he cautions on pages 242-243, we need to be cognizant of a number of risks with storing our data with cloud vendors because of the loss of control and other risks, such as cross-border transmission of information and confidentiality. A comprehensive service level agreement (SLA) that covers a multiplicity of issues, which the author lists on pages 243-244, is essential (especially for law firms). Under Indiana Rules of Professional Conduct (as well as the ABA Model Rules) Rule 5.3, the lawyer retains responsibility for overseeing internal law firm employees as well as third-party vendors, consultants and contractors. The author recommends that the cloud computing provider demonstrate that its system can withstand security testing and how it will handle data recovery in the event of a disaster or other threat. Other considerations for backup systems are scheduled - and even automated - dates and times for backup as well as full and incremental backup processes. You want to make careful decisions on where the backup data will be stored and whether multiple copies are needed. The author observes that an overlooked part of backup systems is the actual procedure for restoration, noting that these systems can be complex and subject to failure. He recommends doing a live-fire test of these processes and that even individuals should use off-site storage (because if your house or

apartment is burglarized or there is a flood or fire, your backup media is also likely to be stolen, damaged or destroyed).

The next section in Chapter 6 of *Electronically Stored Information: The Complete Guide to Management, Understanding, Acquisition, Storage, Search, and Retrieval*, 2nd ed. focuses on litigation holds. Recall that our duty to begin preserving potentially relevant electronic evidence starts when we reasonably anticipate litigation (what has been called zero minus one). (See the Preservation/Legal Hold Workflow from Exterro included as part of the supplemental materials for Module 11.) The author cites a case where a company received a telephone call regarding patent rights, with the court determining that this established the date where the company should have put a litigation hold in place and begun preserving its potentially relevant electronic evidence. The author recommends that lawyers assist in developing a policy on what constitutes a trigger for preserving evidence. He notes that it is a risk management decision about how much time, money and resources are appropriate to spend on preservation, management and secure storage of data that might possibly become relevant electronic evidence. As indicated in the caption to Figure 6.5, creating a good litigation hold process will help protect your organization from liability. Note that third parties who might reasonably anticipate that they will be drawn into litigation also have a duty to preserve potentially relevant evidence. (See the summary of the *Ronnie Van Zant, Inc.* case from Exterro included as part of the supplemental materials for Module 11.) The author lists a number of elements that should be in a litigation hold policy and procedures on pages 247-248. On page 248, the author describes the litigation hold process in his former organization, including the personnel who are involved and the processes that take place. As he asserts on page 248, “[t]his type of system and policy go a long way in complying with what the courts and auditors expect of you and your organization. It will be of value to you to create such a system and put it to use when appropriate.”

Spoliation is covered on pages 248-250 of *Electronically Stored Information: The Complete Guide to Management, Understanding, Acquisition, Storage, Search, and Retrieval*, 2nd ed. The author provides an example of spoliation by quoting from the *West v. The Goodyear Tire and Rubber Company* case from 1999, which found that spoliation is “the destruction or significant alteration of evidence, or the failure to preserve property for another’s use in evidence in pending or reasonably foreseeable litigation.” The author asserts that the procedures and policies for keeping our data safe and preserving its integrity are the most important ways that we as individuals or organizations can avoid spoliation of relevant evidence. Note that sanctions can be ordered in cases whether or not the loss of data was intentional or inadvertent (but be sure to review the 2015 amendments to the Federal Rules of Civil Procedure (FRCP), which clarify under what kinds of behavior are considered spoliation, when a party can be sanctioned for it and the types of sanctions that the court can impose. As he observes on page 250, the possibility of sanctions because of spoliation is simply another good reason to take the time to develop policies, procedures and practices that have been outlined in this chapter as well as previous chapters.

The final section of Chapter 6 of *Electronically Stored Information: The Complete Guide to Management, Understanding, Acquisition, Storage, Search, and Retrieval*, 2nd ed. considers some of the automated solutions that have been developed that can assist in an e-discovery process, including for information governance/litigation readiness. We will be looking at some vendors who provide services and software for small cases. (See SafeCopy2 and Harvester from Pinpoint Labs as tools for collecting ESI and Appendix III on pages 291-292). As the author advises on pages 250-251, the primary consideration for any solution is whether it can:

- Ensure the integrity and security of the data

- Create a methodology to expedite and enhance your ability to locate data
- Assign and manage ownership and authentication
- Assist with the secure storage and preservation of electronic evidence
- Manage notification and messaging systems
- Enhance your ability to analyze and categorize data

The author offers a checklist for guidance in developing the capacity for managing data and for being prepared for preservation and production on pages 251-252.

- List and engage your stakeholders.
- Create a business justification. Note that possible specifications could include data-mapping tools, secure transport and storage capabilities, authentication and identity management, cataloging and indexing features, and notification and messaging systems.
- Research possible solutions or combinations of solutions, which could include off-the-shelf products, something developed in-house or a hybrid of off-the-shelf and in-house systems, operated from either within your organization, on the Internet or by a contracted vendor.
- Assess all of the possible solutions with your team of stakeholders.
- Document the decision and ensure that there is buy-in from all stakeholders, especially those who must approve the funding to pay for the system that is selected.

As the author asserts on page 253, “[i]t is absolutely worth your time to consider what options are available to automate the procedures necessary to provide for the integrity and security of your electronic information.”

Next Steps

With Module 12, we will consider the processing step in an electronic discovery process.

Please let me know if you have questions about Module 11 or the reading assignment.



Have I Got a Deal for You: Selling TAR Like a Pro



by Oliver Silva

Whether you are a project manager, technologist, attorney, or paralegal, if you are pitching the use of technology-assisted review (TAR), you are in sales.

It's your job to sell the customer (case team) tools that will make document review cheaper and faster. These tools have been around for over a decade and are proven to reduce the time and cost associated with document review. Easy sell, right? Wrong.

Through the use of TAR, we can eliminate lesser inclusive portions of an email thread, find near-duplicate documents to streamline the redaction process, cluster conceptually similar documents, visualize communication patterns and use machine-learning techniques to rank documents based on human review. But if you think the benefits of using TAR sell themselves, you'd be mistaken. Despite being around for some time, these tools are foreign to many case teams, or applying TAR is theoretical and difficult for them to put into the context of their matter. To become successful in the adoption of TAR technologies, you must sell TAR like a pro.

Time Shares and TAR

If you have never attended a time share sales pitch, it involves a salesperson who drives you to a destination, gives you a presentation and spends an hour or more going over scenarios of how purchasing a time share will save you money in the long run.

I'm not advocating for driving your case teams to a secluded office building and holding them hostage while you (and several other individuals) try to convince them to use TAR, but what I suggest is that you use some of the tactics salespeople employ during the time share pitch.

The time share sales pitch involves three parts:

- 1 A demonstration of what you are selling and how great it is;
- 2 A projection of costs and cost savings over time; and
- 3 Convincing the buyer to step out of their comfort zone and invest.

Get the Case Team To Take the Tour

Just like selling a time share, you can't sell unless you get the customer to take the tour. This is the first step to achieving buy-in. Have a 15-second (or less) elevator pitch. Your goal is to get the case team to the demo, not to explain how the product works. You can try something like this: "I thought you might be interested in hearing how we reduced our reviewable data set by 40 percent using technology-assisted review. We saved thousands in review costs, prioritized the most relevant documents and shaved days off the review. I'd love to see if we can do the same thing with your case. Can we set up a time to demonstrate these savings for you?"

Any flavor of this will work. The important things to include in your elevator pitch are a quantifiable cost savings to get their attention, reference to a past success with another case team and an actionable item — ask to set up a demo. If you have no prior experience with TAR, ask your preferred service provider for a success story and use that as your elevator pitch.

If the person you're pitching to seems skeptical, have a credible reference ready to go. Provide the names



of one or two attorneys who would be willing to discuss their positive TAR experiences with colleagues. Having an impartial third party to validate your success is a great tool — especially for attorneys, who are risk-averse by nature.

Once someone agrees to the demo, lock in a date immediately. It's important to strike while the iron is hot. Send a calendar invite to block off time in their busy schedule. After you've secured a date, it's time to plan for the demo.

Hold a Successful Demo

Over the last 10 years, I've attended countless demos. The most memorable and effective were those that were tailored to fit my case or focused on the features and workflows purported to be most beneficial.

Although it doesn't matter which method you choose, the most important things about the demo are that it happens smoothly with little to no delay, the process you are pitching is easy to understand and avoids industry jargon, and you are confident it will improve the workflow in a meaningful way.

Be prepared for the following scenarios:

» ***"My computer is operating a little slow today."***

How many times have you heard this at a demo? Stalling a demo because the software "isn't responding normally" might kill the deal. When an attorney picks up his/her phone and checks email, you know the deal is probably blown. There's nothing wrong with using an effective PowerPoint presentation to show workflow or screenshots instead of using the application in real time.

» ***"We can use a combination of clustering and removal of lesser inclusive threads to organize and reduce the data volume."***

After you finish this article, say that sentence to someone in your family. That glazed-over look you're likely to get is probably what you will see from the case team. The explanation of the process needs to be done with no industry jargon. This is something I struggle with daily. But it is crucial if you want to ensure the case team feels comfortable and in control of the process.

» ***"Our tool has every bell and whistle you would ever need to reduce time and costs."***

You can't get more general than that. Case teams want to know that you put thought into how the solution will help them with their specific case. Try starting the demo with this: "What would you define as a successful outcome for this review?" The answer to this question will help you tailor the demo to fit that particular goal. End the demo with an affirmation of how you can meet their goal.

Demonstrate the Savings

After the case team sees how the tool works, it's time to get down to brass tacks. You need to have a few scenarios ready to demonstrate possible cost- or time-savings. I provide time/cost scenarios for conducting a straight linear review using keyword culling versus document review using keyword culling and TAR. I do this using Excel calculators developed over the years. When presenting estimated costs, always include a section for the total savings. This really gets their attention.

Close the Deal

The most important part of selling TAR is closing the deal. This can also be the most difficult. Here are a few tips to help you close.

- » Stress the importance of learning about their case faster by focusing on what is most relevant and discarding what is not.
- » Instill confidence that this process will work for them.
- » If they are wavering, ask what gives them pause, and quickly address those issues.

Finally, if you fail, don't give up! Even if the case team goes in another direction, you've accomplished your goal of starting the conversation regarding TAR. Just like buying a time share, they are likely to tell their colleagues about the experience, which increases your chances of success going forward. **P2P**



OLIVER SILVA

Oliver Silva is the Litigation Support Manager for Nutter McClennen & Fish LLP — one of the 10 largest law firms in Massachusetts. He has worked primarily in litigation support for the past 10 years and is a Certified E-Discovery Specialist. Contact Oliver at osilva@nutter.com.

If the person you're pitching to seems skeptical, have a credible reference ready to go.

Preservation / Legal Hold Workflow



Step 1

In-House Counsel:



Review and identify potential custodians, data types and data sources

Step 2

Paralegal:



Enter matter information into matter management and/or electronic billing system

Step 3

Paralegal:



- a) Enter matter information into legal hold notification tool
- B) Draft legal hold and apply custodian interview questionnaire
- c) Identify additional custodians/data sources

Step 4

In-House Counsel:



- a) Review legal hold and questionnaire
- b) Approve/makes changes

Step 5

Litigation Support:



- a) Identify additional custodians/data sources
- b) Review final legal hold
- c) Push legal hold and questionnaire to custodians
- d) Send copy of legal hold and questionnaire to in-house counsel and outside counsel

Step 6

Custodian:



- a) Receipt and review legal hold
- b) Acknowledge legal hold
- c) Respond to questionnaire
- d) Identify additional custodians

Step 7

Custodian:



Receive reminder if the legal hold has not been acknowledged within seven (7) days

Step 8

Litigation Support:



Review custodian responses to questionnaire

- a) Identify potentially responsive data; consult with legal team on whether to collect
- b) Push legal hold to newly identified custodians

IT/Compliance/Security:



Collect data stored on hard drive and/or external media

Interested in seeing what a custodian interview questionnaire looks like?

[Download a Custodian Interview Template now](#)

exterro



E-Discovery Case Law

The Duty to Preserve Extends to 3rd Parties and Their Texts

Ronnie Van Zant, Inc. v. Artemis Pyle
(S.D.N.Y. Aug. 28, 2017)

Why This Case is Important

With the increasing amount of information stored on various data sources, it's paramount when implementing legal holds to consider including third parties who may have relevant data.

Overview

In this action for a breach of a consent order involving the famous Southern Rock band, Lynyrd Skynyrd, the defendant is accused of failing to have a third party preserve relevant text messages when the third party switched to a new phone after the lawsuit commenced.

The defendant argued that they should not be sanctioned for spoliation of the text messages, because the alleged lost data was from a third party, making the text messages outside their custody or control.

Ruling

1. PRESERVATION DUTY EXTENDED TO THIRD PARTY.

Even though the third party was not a party in the case, the court imposed adverse inference sanctions on the defendant for the third party's failure to preserve the text messages.

2. DEFENDANT HAD "CONTROL" OF THE TEXT MESSAGES.

Under FRCP 34, a party must produce documents in its "custody, possession, or control." Based on the "practical ability" test for "control," the judge ruled that the defendant had the practical ability to ensure the third party's preservation of the text messages.

3. INTENT TO DEPRIVE BASED ON DELETION OF TEXTS, BUT NOT PHOTOS.

To issue an adverse inference under FRCP 37(e), the judge must find that the offending party acted with an intent to deprive. The basis for this intent stemmed from the fact that the third party did not have the texts but kept photos from the phone, which was "evidence of deliberate behavior that sanctions are intended to prevent."

CASE LAW TIP

Have questions on how the FRCP applies to e-discovery?

[Download this FRCP E-Discovery Quick Guide Collection to get all your questions answered.](#)



**Measure your
with Legal T**

Fearless confidence to run
like a data-driven business

Request a demo 📞

The intelligence, technology and human
you need to find trust

EDISCOVERY, MONEY

Want To Save Money In eDiscovery? Here's A 3-Step Plan.

eDiscovery doesn't have to be a mad scramble. Cost-effective, smart discovery means taking a logical, thoughtful approach.

By KELLY TWIGGER

Oct 10, 2017 at 4:10 PM

27
SHARES





I'll be in seven different cities speaking at events over the next six weeks, and inevitably, I'll get asked the same question over and over: How can I do discovery with ESI more effectively for less money?

Nothing like an easy question to answer. I've handled hundreds of matters from a \$7,000 insurance case about nail polish to \$100 million class action about engines, and yes, you are correct that every matter is different. But over 20 years of practicing and focusing exclusively on discovery for the better part of that time, I can tell you this: saving money in discovery is a three-step process that's pretty common sense. 1) breathe, 2) plan, 3) use technology wisely.

Step 1: Breathe.

The tendency is to dive head first into discovery, drafting up overbroad requests and then wondering why you got dumped with tens of thousands of documents. Or, to not engage with discovery until the last minute and then scramble. Instead, just stop. Sit back and think about what you need to do with your case, what the client's goals are, and the most efficient path forward.

Now, I'll tell you that if you can start this process before the next complaint hits your desk, you'll do an even better job of being efficient and effective. I also know that you are thinking I'm crazy to even suggest that, and I'm okay with that. But you know that time when the case suddenly goes away and you have a schizophrenic week of being both euphoric that your insane pace is over and fear that you'll not have work to do? This is a perfect time to breathe. Now go to step 2.

Step 2: Plan.

Yes, I know I had the gall to suggest being proactive instead of reactive in litigation. But you asked, so there it is. What does planning mean, you ask? In this context, it means thinking about the decisions that you are going to have to make on the fly for a client when a new matter arises and knowing what you'll have to consider.

Creating a plan for each client for the different types of matters and working

MENU

through them on a matter ensures that you are making comprehensive, reasonable decisions on the scope of preservation, collection, and production. Then track them.

So what do I mean by planning? Good planning for discovery involves five key elements. If you are planning proactively, meaning before a matter hits your desk (yes, that's a thing), then think generically about these five points. Obviously, if the matter is on your desk or you are filing it, you will have a specific case plan.

1. People (or custodians) at each party. Who are the key people? Your list of legal hold recipients is likely much longer than the list of people you talk to and ultimately collect information from. Be sure to track your decisions about why you chose not to talk to a custodian for later.
2. Identify the date range of relevant information. Stay focused on the time period where relevant information lives. Tell your PM so a date range filter can be set on review software. Often, keeping that date range in the front of your mind will allow you to ignore sources of voluminous ESI with a clean conscience as long as your date range is reasonable. I suggest getting agreement from the other side before you commit to it.
3. Identify the sources of ESI at issue. This is a two-part process — knowing what the source is, who manages it, how you get at it, and the date range of information in it is part one. Part two is understanding any complexities involved in collecting and handling that data. For example, we are working with a project management tool for a client that requires extra work to pair the metadata back up with the PDFs after exporting it. That's time and money. With planning, it's done cost-effectively. *This part of planning is usually the most involved — getting out ahead of this stage is crucial.*
4. Identify third parties. Having to go to other parties for data is one of the biggest time sucks in the discovery process. Have a plan for what you need and see if you can work together with them cooperatively. Be narrow in your requests and talk to the third party about issues with their ESI, getting it, etc. Help them help you where possible.

5. Formalize agreements between the parties. I firmly believe that even the smallest matter needs some type of formal agreement as to how ESI will be handled, and don't forget the ever important FRE Rule 502(d) order.

Planning and modifying your plan as you move through discovery will give you a framework for new matters going forward. It also helps identify the issues that need to be addressed in an ESI protocol between the parties. Every case involves different complexities that have to be addressed. Planning is the best way to stay out in front of them so they don't cost more down the line.

Okay, you've planned and gotten targeted data from your client and the other side. Now the cost kicks in and you have to load and handle the data. You're ready for step 3.

Step 3. Use Technology Effectively.

This step can be an entire article in itself, so here are some main points:

1. Choose your technology wisely. You don't always need the biggest and the baddest. But better features that will let you manage the type of data you have are super important. The upfront cost saves considerable time downstream.
2. Have a plan for loading and looking at individual custodians data vs. loading everything and doing one large scale review. I like to spend some quality time with the data of the truly 1-3 key custodians to get a feel for who really has the data on specific issues and what we need to load and focus on. Pay attention to how much data de-duplicates out of your set and use that to improve your planning.
3. Set up a tagging structure in your review tool and include a timeline checkbox. Tag documents that should go in a case timeline so you can find them quickly. I haven't seen a review platform yet that has a good timeline feature (tell me if you have), and I really need one. Hint, hint developers. Use the tagging structure to quickly issue code documents during review.

4. Use the features of your platform to do better review. I see a ton of money wasted on inefficient reviews. Work with your team or your review provider to gather metrics and monitor the review to see where the dollars are slipping through the cracks. You don't need to be doing separate reviews for relevance and issues — they can go together. Get a good, solid review team and educate them.
5. Avoid getting lost in the data. Just because you have thousands or millions of documents doesn't mean that should control your thought process. Stay focused on the claims and the elements of those claims that matter. Remember the money documents? That's what you're looking for.

Cost-effective, smart discovery means taking a logical, thoughtful approach. Planning is good on so many levels — it allows you to make reasonable, logical decisions, to cooperate better with the other side, and to keep your client apprised of costs and budget issues. eDiscovery doesn't have to be a mad scramble. Try this three-step approach and let me know how it goes.

