Paper Title: Making Your Way Through the Wilderness of e-Discovery

Sarah Thomas Pagels [author]
Julia Helmer [author]

Sarah Thomas Pagels
Partner
Laffey, Leitner & Goode LLC
325 E. Chicago Street, Suite 200
Milwaukee, WI 53202
(414) 312-7003
stpagels@llgmke.com

Julia Helmer
Senior Solutions Consultant
Relativity Expert
Advanced Discovery
(312) 462-1784
julia.helmer@advanceddiscovery.com

Session Title: Making Your Way Through the Wilderness of e-Discovery

Presented by Sarah Thomas Pagels, Laffey, Leitner & Goode LLC, and Julia Helmer, Advanced Discovery

Biographical Information

Sarah Thomas Pagels is a Partner at Laffey, Leitner & Goode LLC in Milwaukee, Wisconsin. Sarah advises her clients on how to creatively and cost-effectively navigate the e-discovery process in preparation for trial or alternative resolution. She specializes in leading a team of attorneys and paralegals in high volume, document intensive cases, utilizing technology to manage costs and locate key facts. She focuses on the details while keeping the big picture in mind.

Julia Helmer is a Senior Solutions Consultant at Advanced Discovery. Julia creates process flows for the enterprise e-discovery workflow from identification of relevant data sources, to creation of legal holds, to execution of ESI collections and productions. Julia consults clients in preferable collections, processing, review and production options to best meet their e-discovery goals and conform to budgets and best practices. Julia specifically concentrates on introducing Technology Assisted Review and Analytics into e-discovery workflows to streamline review, promote efficiency and save on costs.

Making Your Way Through the Wilderness of e-Discovery

Congratulations! A senior partner just walked into your office and asked for your assistance on the firm's newest case. This firm client has never been involved in a large litigation like this one before, and the partner wants a young, energetic, and digitally savvy lawyer to assist in the discovery process, especially with the e-discovery piece. You are excited to jump right in, but where should you start?

While the e-discovery process can seem scary and overwhelming, creating a successful e-discovery plan and process is really no different than preparing for any other facet of trial: it takes a solid plan. (In geek speak/e-discovery language, this is often called your ESI, or Electronically Stored Information Protocol). Regardless of what you call it, no plan would be complete without learning the lingo, checking the relevant rules, assembling your team, maintaining regular communication and reassessment, obtaining cooperation from your client, and seeking expert advice from a technology partner (either an outside e-discovery vendor or a litigation support team member). A few tips from the trenches we have learned are below will get you well on your way to successfully navigating the e-discovery wilderness and providing value to your clients and your team.

Build Your Infrastructure.

The best e-discovery plan is worthless if you do not have the infrastructure to support it. The best infrastructure requires three distinct components: people, process and platform. Depending on the scope of your project, it is unlikely one lawyer can do this alone. From the legal side, consider assembling a team of lawyers and paralegals now. Don't wait until you have collected the data and have a looming production deadline. Getting even a few of these folks on board early helps to ensure consistency down the road and makes sure that everyone is invested in the case.

You also will need multiple contacts with your clients, including contact persons outside the legal department. Ask the primary client contact to help you identify folks that work in information technology, human resources, operations and/or in the divisions or departments that are involved in the dispute. Identifying early on who the likely persons with relevant data (or "custodians") will be, and having access to personnel in multiple departments, is critical to ensuring effective communication and implementation of protocols and processes.

On the technical side, a knowledgeable vendor or in-house Litigation Support team is necessary to advise you on proper preservation, collection, review and production process. Regardless of the scope of the project, you will need some kind of review platform or database to evaluate and analyze the material that has been collected. Relativity is one of the most powerful platforms out there, but it is not the only game in town. Consider what options work best for

your case. Just make sure that the platform you choose is secure and allows you the flexibility you need as the case evolves.

Having a service provider you trust and that communicates early and often is invaluable. Now is the time to have a conversation with your support team and your client about various budgets, identifying the rough scope of the project, and identifying potential concerns or red flags with respect to data integrity and accessibility. Once you have assembled your defense team, you are ready to outline your ESI plan – which should be guided based on several factors, including the size/scope of the case, and of course, the rules of your particular jurisdiction.

Identify and Preserve.

Unlike even five years ago, Courts now expect *all* lawyers to know e-discovery lingo. References to Electronically Stored Information, or "ESI," is now commonplace in almost all state, federal and local court rules. In case you did not already know, ESI is the catch-all term for any electronically stored data – and encompasses all things electronic. While your clients may think this just covers their employee or company email, it covers much more than that – it can include any of the following: emails, data on its server, cloud storage, data saved on flash drives, data saved on company or personal computers, employee text messages or voicemails, information on backup tapes, cell phones, tablets, wearable devices, and more. In fire, personal injury, and transportation cases, this may also include data from black boxes in vehicles or equipment, as well as data stored in location or support services like OnStar or wearable GPS data, social media profiles or posts, and even mobile phone applications.

Since the Federal Rule of Civil Procedure were amended in 2015, more and more courts provide lawyers and litigants with guidance on what judges in their jurisdiction will expect in an ESI plan. For example, the Seventh Circuit has its own specific ESI guidelines. *See* 7th Circuit Principles Relating to the Discovery of Electronically Stored Information (2nd Ed. January, 2018) *available at* https://www.discoverypilot.com/sites/default/files/7thCircuitESIPilotProgramPrinciplesSecondEdition2018.pdf

Before having your Fed. R. Civ. P. 26(f) conference with the Court, you need to confer with your client and the other side to identify what kinds of information may be relevant to your case, and who on the client side will be your contact to assist in data collection, who the likely custodians are (the persons who will have discoverable information), as well as where and how the information may be stored. You are also expected to identify your client's document retention policies for various systems (if they exist). If they do have them, it's a good time to determine if they are followed. If they don't follow them, it's better to know that fact now than to find out two years into your case. If they don't have retention policies – consider whether it's time to create them.

If it was not already implemented before the case was filed, now is also the time for outside counsel to consider preparing a litigation hold letter instructing your clients to implement policies to preserve the data – either by copying it to a secure location or collecting it as well as disabling any automatic deletion or archiving features. For example, the default setting on Microsoft Outlook, unless it is disabled, only preserves deleted mail for 14 days.

It is also incumbent on outside counsel to ensure that everyone who is likely to have discoverable information is told to preserve it in a litigation hold notice – either a written letter or other communication that expressly tells identified personnel (custodians) what they are required to save and in what format. Involving your client's IT staff or other outside technology vendor is also a critical step. For example, your custodian may be following the directions in the hold by never deleting any of her emails; however, she would not be able to control an automated IT policy that rolls any email older than 60 days off the corporate email server. The Seventh Circuit guidelines caution that while a preservation hold letter is not expressly required, if you are going to send one, it cannot be vague and overbroad. While it may not technically be required, it is certainly good practice.

The Seventh Circuit recommends that litigation hold notices contain the following information: (1) names of the parties to the dispute; (2) factual background of the legal claims at issue; (3) names of potential witnesses and other people likely to have discoverable evidence; (4) relevant time period; (5) geographic scope; (6) other information to assist the responding party in assessing what information it should preserve. *See* 7th Circuit ESI Pilot Program Principles, Second Edition, 2018 at 3.

Involving your vendor or litigation support person is also critical in this step. They can help you identify the who, what, where, and how much is available – either through in-person interviews, data mapping exercises, or completion of a custodial questionnaire. Custodial questionnaires should ask individuals likely to have discoverable information about what kinds information they have, whether they think they still have access to it, how it is organized, who might have received copies of it, how the information was communicated and more. Your vendor or litigation support person is also attuned to other areas where data might be stored in the digital business world – think personally-owned devices, cloud storage, third-party platforms, text messages and chat applications.

This is also a good time to obtain background information from your key client contacts to find out what key words, topics, or phrases may have been used in reference to the issues in dispute – these may be useful in sorting and/or eliminating data later during the collection and review process.

Check the Rules.

After you have a handle on the scope, depth and breadth of your client's data, you can start to think about what you will need from the other side, as well as what your client will be willing to produce.

Federal Rule of Civil Procedure 26, 33 and 34 have all recently been modified in an attempt to adapt to set rules of the road for both sides, to serve a dual purpose – to ensure that discoverable information is preserved and produced, but also to address the proportionality (both volume and expense) of the information that is being requested. *See generally,* Advisory Committee Notes, December 1, 2015 Amendments to Fed. R. Civ. P. 26.

Remember, not every single electronic scrap of data is discoverable or relevant to a claim or defense in the case. *Marshall v. Dentfirst, P.C.*, 313 F.R.D. 691, 697 (N.D. Ga. 2016) ("[I]t is well-settled that 'a corporation under a duty to preserve is not required to keep every shred of paper, every e-mail or electronic document, and every backup tape. ... In essence, the duty to preserve evidence extends to those employees likely to have relevant information—the key players in the case, and applies to unique, relevant evidence that might be useful to the adversary.'")

The Seventh Circuit guidelines advise that certain kinds of data, such as deleted or "fragmented data," temporary internet files or "cookies," metadata fields that automatically update (such as time stamps or last accessed information), duplicative data (the infamous backup tapes), as well as data that requires "extraordinary affirmative measures" may not need to be preserved and produced in every case. 7th Circuit ESI Pilot Program Principles, at 4.

Local rules may also include guidelines on crafting your ESI plan. Again, doing your homework with respect to your client's ESI prepares you for what you may want to request or offer to the other side. If you don't have access to a particular type of data (or your client doesn't want to give it up), perhaps you don't ask the other side for that type of data either. And, Courts are far more likely to approve limits on ESI if both sides are willing to agree to it.

Consider whether you want a written ESI plan. Note that many federal courts have their own that they require that you use and present a joint report at the Rule 26(f) conference or Rule 16 conference. Issues to think about when you are crafting your ESI plan:

1. What format should the data be provided in?
    a. If you want the data to be searchable, at a minimum, you should ask for PDFs that are OCR'd ("Optical Character Recognition")
    b. Do you want to exchange native data?

i. You may not want to exchange native data for all types of documents, but for spreadsheets or other financial information, consider whether you are willing to exchange records in Excel or even exchange documents in other applications, like Quickbooks format.

c. What about videos or dynamic data?

d. What review platform are you using?

i. Agree to exchange load files in the format that allows you to upload it immediately into your review platform.

ii. Consider now whether you want to use trial software or exhibit software in depositions – make sure the data formats you request are compatible.

e. How will the data be exchanged?

i. Hard drive or other physical media?

ii. Electronic cloud platform or link through an FTP (File Transfer Protocol) site?

f. What about documents that are originally in hard copies? How will they be treated?

2. What kind of metadata are you willing to share?

a. If you are exchanging native documents (documents in their original format), more metadata is likely to be exchanged with the other side. Addressing it in a written ESI agreement means that you are both getting the same information.

b. If you are not producing native data, consider whether you are willing to provide at least the following types of metadata:

i. Author and Email Sender/Recipient Information

ii. Custodian

iii. Date

iv. Email Subject and File Name

v. Attachment Information

vi. File Types

vii. MD5 hash – this is a unique identified that helps to determine whether or not a document is a duplicate.

3. Rules with respect to duplication

a. Global de-duplication (across the entire dataset)

b. Vertical de-duplication (within a particular custodian)

c. No de-duplication?

d. Email Threading or Near-de-duplication (not identical, but similar)

4. Rules with respect to searching or filtering

a. Agreed upon search terms?
b. Date or time filters?
c. Custodial/sender/author filters?
d. What about analytical tools?
    i. Clustering (sorting data into clusters or "buckets" based on textual similarities)
    ii. Email threading (gathering all the email messages on a particular subject or thread into a single chain including original message, replies, and forwards)
    iii. TAR" or technology assisted review – predictive coding where a reviewer or team of reviewers trains the review platform on issues with responsiveness and privilege
    iv. Sneak peeks – letting the opponent see a segment of unfiltered or unreviewed data to evaluate the responsiveness/effectiveness of search terms

5. Timing with respect to production
    a. Rolling productions
    b. X days before a particular deposition
    c. How long before the close of discovery?

6. Supplementation Agreements
    a. Beyond the requirements in the local or jurisdictional rules?
    b. Consider data that is still being created like financial records or invoices

7. Protective Orders/Limitations
    a. Do you need a confidentiality agreement or protective order?
    b. What kinds of documents can be designated confidential/attorneys' eyes only?
    c. Who can look at documents with those designations?
        i. Consider carve-outs for both testifying and non-testifying experts and third-party witnesses or authors of a document that are no longer current employees or individuals within your client's control.
    d. Establish a clawback policy
        i. How long do you have to claw a document back?
        ii. What happens to a clawed back document?
        iii. Is there a process for the other side to challenge it? How long do they have to raise a challenge?

While the above is not an exhaustive list, it does identify many key issues to be considered. For other examples, there are many good resources available, including the Duke Law EDRM website, (www.edrm.net) and the Sedona

Conference (www.thesedonaconference.org) publications. Your e-discovery vendor may also have their own list – ask them!

Collect and Process the Data.

Once you have identified your key witnesses or custodians, sent your litigation hold notice, ensured that document retention policies are followed and/or that automatic deletion features are disabled, interviewed your custodians or reviewed your completed questionnaires, the next step is collection.

The legal field tends to be the last to embrace technology, but the same principles that apply to paper discovery should also apply to electronic discovery, even under the recent modifications to Fed. R. Civ. P. 26, 33, 34, 37 and 45. The biggest issue with electronic discovery has to do with the sheer volume – because we are no longer talking about boxes of paper or filing cabinets, and because cloud storage is relatively inexpensive, it is far more likely than not that your clients will have terabytes upon terabytes of data. While most of this data is probably not relevant or responsive –you still have to evaluate it in some way, and make a determination of whether some or all of it should be collected, processed, and produced.

Your vendor or litigation support person is also invaluable in this process. They can help you find the ESI and evaluate its scope, breadth, and depth. There are multiple ways to sift through data in the collection process that can help you reduce costs for storage, reduce the volume that needs to be reviewed, as well as make sure that only data that needs to be preserved is preserved. Preserving everything is not only *not required*, but also not always advisable. After all, your client still needs to be able to run its business. The key witnesses may not all be current employees, and/or their job responsibilities may change. Much like issue-spotting in a law school exam, you need to be able to issue-spot key issues like this and look to your vendor or litigation support person to help you address them.

Using an outside vendor or litigation support person to handle the collection serves multiple purposes that will help you in your case. As a neutral party – unlike having collection performed by your client (who has just been sued), they have no incentive to destroy or manipulate the data as it is collected. Often, a technology expert will also have access to collection tools and professionals that make the process faster, easier and results in less interruption to the business and its employees. Vendors are also more likely to be up to date on technologies for collecting unusual types of data – while most IT departments can collect emails from an Outlook or cloud-based program, they may not have the technology or skill to collect text messages, chat apps or GPS data. And, using an outside party to collect the data can make sure that the data is fully and completely collected (including the metadata), and provides you with yet another defense to any argument that the data was improperly destroyed or manipulated. It also provides you with someone who could be an expert if there is a need to defend your collection and preservation processes later. Data may also be filtered

during the collection process, using custodian filters and date filters – hopefully something you discussed with the other side and included in your written ESI plan. Although it may be possible to filter your data using search terms, that is generally not recommended at the initial collection stage as early on in your case, you may not be in a position to isolate all the key phrases or words or identify documents that may not be searchable because they are corrupt, password protected or don't have searchable text like scanned PDFs and image files.

Your vendor or litigation support person can also assist you in evaluating how much data to collect, how to process and convert it into a format that is suitable for review and analysis, and provide storage solutions that work for your client and your budget.

Review and Produce.

Once your data has been collected, there are multiple options on how to process, sort and review the data. Again, your ESI plan should guide you here. Your vendor or litigation support team can help you consider whether to load all the data and then offer culling options, commonly known as "analytics." Depending on your case and your data, it may be prudent to simply apply search terms and then load the resulting hit data for review. Most times, however, you should consider applying other types of analytics such as clustering, email threading, or de-duplication. This allows you to use fewer attorney or paralegal reviewers, and process the data more efficiently. As the legal discovery manager, your job is to help identify what key issues you think will come up in the case, and then communicate the same to the review team, your clients and your vendor. The most important skill in managing a large-scale e-discovery practice is effective communication. Prepare a document review team memo identifying the key players, the key issues, and the timeline. Provide every reviewer with a list of persons that are in-house or outside counsel – you can even ask your vendor to apply filters to individual names or domain names (like a law firm's email domain) to highlight potentially privileged communications in the review platform.

Establish coding guidelines. Does your jurisdiction require you to designate specific documents to a particular document request? Incorporate a workflow to flag or elevate "hot docs" for more senior attorney review. What about redactions? Does your jurisdiction require redaction of personally identifiable information like Social Security numbers or financial account numbers? Don't forget about compliance with HIPAA requirements for any potential patient data. Establish who is in charge of quality control. If you plan to prepare a privilege log from your database, determine how your privileged information should be coded or analyzed now – it makes segregating and preparing your privilege log much easier later.

Re-Evaluate.

Just like any other kind of discovery, the case needs and the evaluation of the data will constantly evolve. Work with your review team, your client and your vendor or litigation support person to improve and re-evaluate as needed. Constant and regular communication is key to this process. Consider adding exhibit numbers into your database as key documents are marked in deposition. Keep a production log that contains the Bates-ranges and dates of production (including volume numbers) for every production made. Above all, be flexible. It's not unexpected to run up against issues you didn't previously consider, like gaps in your data collection or the dreaded stub email from an improperly restored archive system. Trust your team and allow your plan to have fluidity in order to pivot when necessary.

Win.

A successful e-discovery plan requires front-loading a lot of the work and expense. Most clients do not like being told before their answer is due that they need to spend significant time and resources on locking down their data, giving access to an outsider (your vendor or litigation support person), and spending company personnel time on something other than their business. But, doing it correctly with a willing and competent vendor sets you up for success, and is infinitely cheaper than defending a sanctions or spoliation motion or paying a fine for failing to properly preserve, collect or produce the data.