eDiscovery Defensibility

Research Data, Inc.

The presenters.

Research Data, Inc.

eDiscovery Made Easy.

Sam Lewis

CTO, RDI

Kym Wellons

Associate General Counsel, WestRock Company and CEO, RDI

The agenda.

- Sedona Principles
- Basic goals of discovery defensibility
- A defensible protocol
- Ethics in eDiscovery

Sedona: What is it?

- The Sedona Conference is a nonprofit policy research and education organization comprised of judges, attorneys and other experts in eDiscovery.
- Over time, it has become a thought leader in the eDiscovery arena through working papers it has issued over time that are routinely cited as authority.
- The Sedona Conference provided guidance on the 2015 amendments to the Federal Rules of Civil Procedure

Basic Principles

Principle 1

- eDiscovery process is not required to be perfect
  - ➢ Reasonable is defined by issues of proportionally, including the benefits and burdens of the process

Principle 2

- eDiscovery should be reasonable under the circumstances
- eDiscovery process should be developed and implemented after reasonable due diligence
  - ➢ Due diligence is consultation with persons with subject-matter expertise and technical knowledge and competence.

Principle 3

- Responding parties are best situated to evaluate and select the procedures, methodologies and technologies for their discovery process.

Reasonableness is the Standard

- Rule 26(g) of the Federal Rules requires certification by a responding party that a "reasonable inquiry" has been made, consistent with discovery obligations under the rules.
- Comment 1.a. The duty to conduct a reasonable inquiry is satisfied "if the investigation undertaken by the attorney and the conclusions drawn therefrom are reasonable under the circumstances."

What is reasonable?

- A defensible e-discovery process does not have to be:
  - Perfect;
  - the best available option; nor
  - Able to identify all discoverable ESI.
- Risks are inherent in any method of identifying relevant ESI.
- Any process involving humans is prone to mistakes.

What is reasonable?

- Federal and similar state rules are based on the principle that:
  - the responding party has the obligation and right to make decisions concerning the processes they will employ to comply with their discovery obligations and
  - that responding parties are "best suited" to make a reasonable evaluation and selection of those processes
- An e-discovery process is not inadequate simply because an opposing party can demonstrate that a more accurate or complete process exists.
- The process and resulting production may be reasonable if the burden of identifying additional ESI outweighs the need for such discovery and its importance in resolving the issues in dispute.

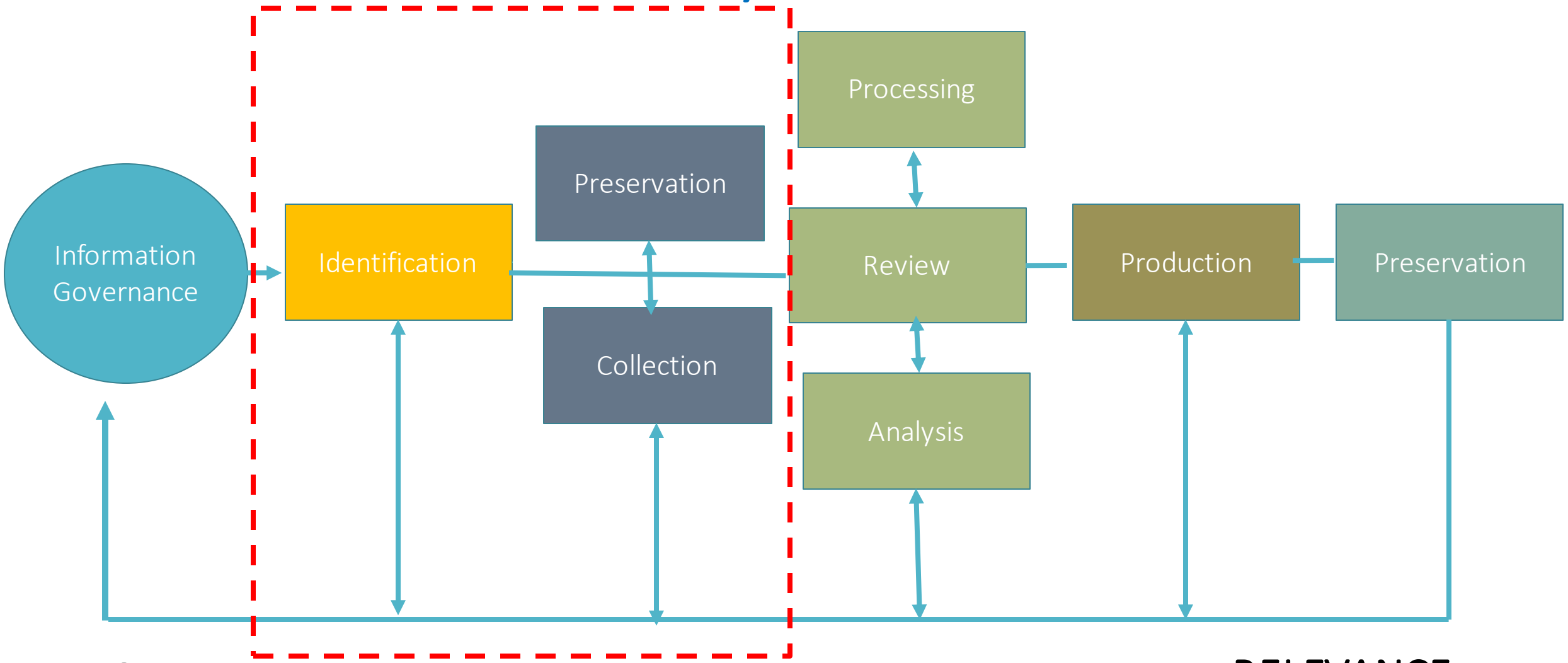
Is there a favored process?

- No. There are no bright-line rules about what processes are reasonable and proportionate.
- Each case requires its own assessment based on:
  - the information that is reasonably available;
  - a sufficient understanding of available technology and processes; and,
  - a good faith exercise of legal judgement.
- For any given case, there may be any number of possible discovery strategies and technological options available that, if implemented appropriately, could each meet the reasonable discovery standard.

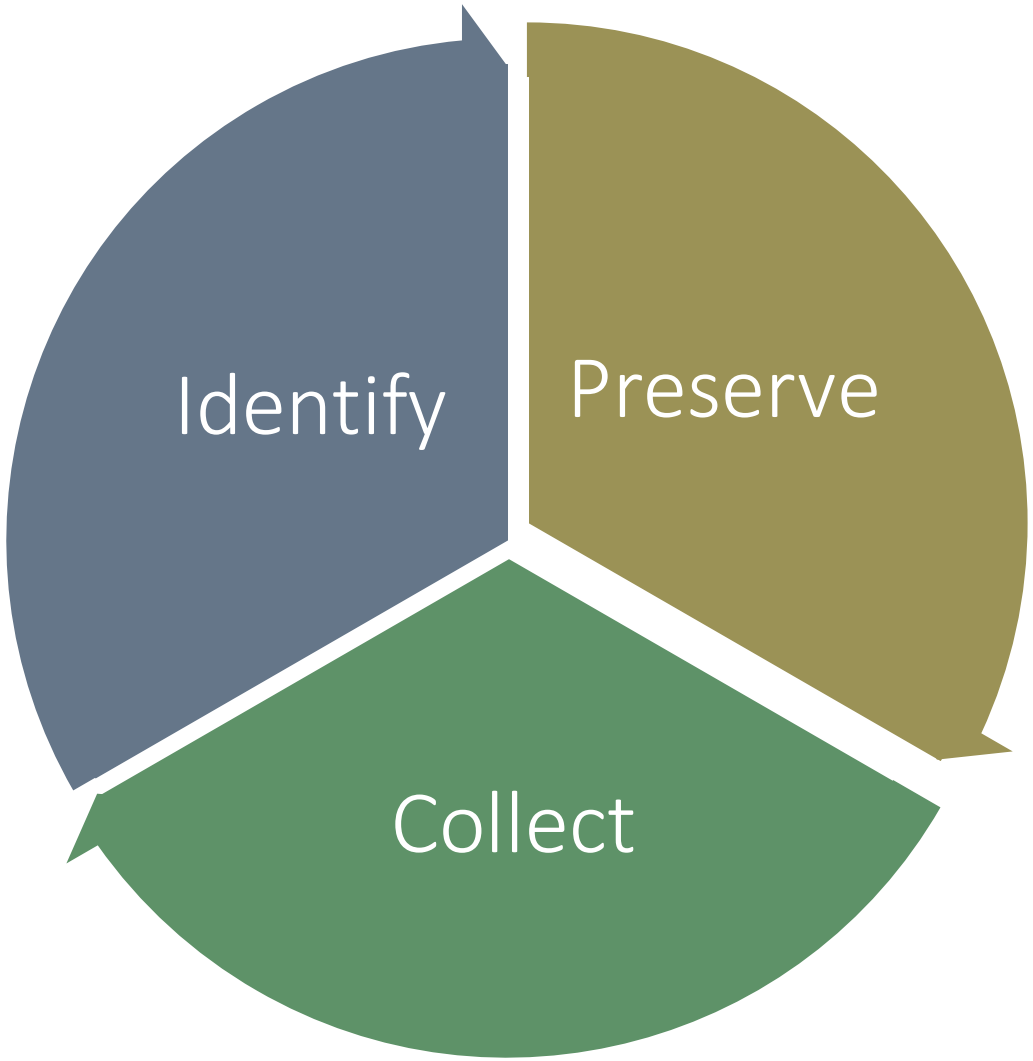
Protocol: Goals

- Choose a defensible method of eDiscovery based on your case.
  - Follow the Electronic Discovery Reference Model (EDRM).
- Prepare.
  - Understand your data.
  - Know the impact of your decisions about a production method based on your data -- threading, near duplicates, families, etc.
  - Establish a preferred form of production with consistent forms-based protocols.
- Leverage vulnerability of opposing counsel.
  - Assess your data and protocols early in the litigation process.
  - Be organized and able to articulate the reasonableness of your protocols.

Electronic Discovery Reference Model



Electronic Discovery Model/@2014/v3.0/edm.net



1. Discuss the theory of the case with your client.
2. Decide what facts are relevant to the case.
3. Identify those custodians and those systems that may possess or store relevant information.
4. Preserve the data.
5. Collect the data.
6. Do all of the above defensibly.

This is a cycle. It may happen many times over the life of a matter.

Protocol: Identify

- Review with your client all relevant document storage systems, such as:
  - Network structure;
  - Document retention and identification policies;
  - Email systems during the relevant time period;
  - Backup protocols; and
  - Data systems – PeopleSoft, SAP, SharePoint…
- This will help you understand the culture of the company and inform decisions when it comes time to collect.
- You want to know what questions to ask the custodians about where they have data. This is different for each IT network.

Protocol: Identify

- At this stage, you should define the information that might be relevant in the matter and required to respond to discovery:
  - Review court disclosure requirements
  - Likely discovery (affirmative and defensive)
- Compile lists of
  - Custodians;
  - Relevant data types and venues
    - Email
    - Smartphones and tablets
    - Home computers
    - Social media
    - Other on-premise and cloud-based platforms

Preservation: Legal Hold

- Duty to preserve data is triggered by knowledge of actual litigation or reasonable anticipation of litigation, such as:
  - Demand letter
  - Formal complaint
  - Regulatory proceeding (EEOC, DOL, etc.)
- Information preservation is an immediate requirement.
  - Identify who has information.
  - Discuss with your client the requirement to preserve.
  - Send preservation notices to:
    - People who possess information;
    - People who own the systems where information is stored; and
    - People who may have visibility to changes in custodian status.

Preservation: Legal Hold

- Litigation hold letter (or legal hold)
  - You should advise your client in writing to issue legal holds or do it yourself.
  - Legal hold notice should be written *in plain English*.
    - Ensure the notice describes the issue sufficiently for identification of relevant documents.
    - Provide examples of relevant documents.
    - Provide guidance for questions.
    - Explain the importance of the process.
    - Ask for identification of other witnesses.
  - Schedule for updating throughout the case!!

Protocol: Preserve

Interview the custodians.

Consider all devices: Computers, external hard drives, USB drives, cellphones, laptops and tablets.

Don’t forget hard copy document resources in file cabinets and desk drawers!

Be sure to ask them about other custodians, systems or document repositories.

Document the custodian interviews.

Keep interview notes.

Retain all documents.

Maintain a master list of all custodians, interview date(s) and efforts to preserve and to collect.

Follow-up on leads.

Follow up on any additional custodians identified through the interview process.

Ensure that all new custodians are instructed to preserve and are interviewed until there are no new leads.

Don’t forget to follow up as new facts or theories emerge! That may introduce new sources of data.

.

Protocol: Collection

Collection is not required for preservation… So, to collect or not to collect is a weighty question.

Do you collect to preserve?

Consider IT architecture and cultural topography of the client

IT managed by dependable professionals?

Are the custodians a part of a well-structured/best practice office?

Is the client reliable?

Is there a risk of spoliation?

Do you collect for Early Case Assessment ?

Do you need to “peek under the hood” before formal discovery?

Will data inform your protocols for review and production?

Could data inform early motions practice?

Protocol: Collection

- The preservation and collection of information must be proactively managed by the firm or company's staff attorney
- Aside from the documents, does metadata need to be tended to?
  - This depends on the facts of the case. Is metadata going to be critical?
  - Does there need to be a forensic component to the collection?
  - If not, do you have the resources to defensibly collect?
- Maintain a record of collection efforts
  - Track each custodian with their own folder
  - Always be able to go to the collection folder and answer collection questions
  - Helpful to break down data by folders: C Drive, Emails, External Drives, etc.

Protocol: Collection

- If a conventional copy (non-forensic), do you have the hardware (a USB external)?
- Do you have staff comfortable in executing a conventional copy
- Do you have a protocol that includes you?
- Do you have an approach that is "out of an abundance of caution?"
- Is any special expertise and/or equipment required (cell phones)
- Does adverse counsel have a history of leveraging e-discovery exposures? Conventional and forensic collection?
- Do you have write-block software? (keeps metadata as is)
- Think about relevant time period

Protocol: Collection

- Make a plan, stick to it.
  - If you need to make changes, make notes and tend to them at the end of the planned collection
- For any hardware collected on site, use a chain of custody sheet
  - The chain of custody sheet must be included with the hardware to be defensible
- Never work off a collected item, always work off a copy
- Did your client do the collection for you? They have potentially impacted metadata
- Have write-block software that you are comfortable with ready. (PinPoint Labs Harvester, etc.)

eDiscovery and Ethics

- Failure to preserve/spoliation
- Discovery abuses
- Competent representation
- Privileged ESI

eDiscovery and Ethics

- Failure to preserve/spoliation
- Discovery abuses
- Competent representation
- Privileged ESI

Discovery Abuses

- In Xterro's Federal Judges' Survey, their key takeaways included:
  1. Lack of knowledge of their client's eDiscovery environment.
     - Not skilled in search processes.
     - Lack knowledge of facts early on to identify search terms and custodians.
     - Don't understand the need for the iterative process.
     - 55% of judges surveyed believes that mistakes were most commonly made in identification phase.
  2. Lack of cooperation among counsel.
     - Overbroad requests.
     - Reluctance to disclose relevant available electronic data.
     - Resort to old, traditional adversarial practices.

Competent Representation

- The relationship between e-discovery and ethics (the competent practice of law) grows stronger each year.
- The state bar of California standing committee on professional responsibility and conduct formal opinion interim no 11-0004:

> "*An attorney lacking the required competence for the e-discovery issues in the case at issue has three options: (1) acquire sufficient learning and skill before performance is required; (2) associate with or consult technical consultants or competent counsel; or (3) decline the client representation.*"

Competent representation

- Issues in the opinion’s hypothetical:
  - "Attorney made no assessment of the case's e-discovery needs or his own capabilities...”
  - “He agreed to Opposing Counsel's proposed e-discovery plan under a mistaken belief as to its scope, and thereafter allowed that proposal to be transformed into a Court Order...”
  - “Attorney participated in preparing joint e-discovery search terms without expert consultation and was so inexperienced in ESI that he did not recognize the danger of overbreadth in the agreed upon search terms."

Competent Representation

- Before assuming representation in a case with an e-discovery component, ensure that you have the following resources in order to competently (ethically) represent the client
- Expertise in the components of e-discovery, from preservation to production. Lacking expertise in any area of the EDRM runs the risk of not representing the client's interests competently, therefore unethically
- If you personally do not have competency in e-discovery from preservation to production, ensure that there is a resource, either internally or from outside the firm, that does.
- ABA Model Rule 1.1 requires that competency exists in any area of law practiced, e-discovery or otherwise, to represent the ethical practice of law
- If there does not exist competency in the area of e-discovery and the matter for which the firm is retained will require it, it would be unethical to represent the client

Protection of Privileged ESI

- Sedona Conference Commentary on Protection of Privileged ESI (Nov. 2014) argued for more effective use of Rule 502(d).
- What is 502(d)? It generally provides that the "federal court may order that the privilege or protection is no waived by disclosure connected with litigation pending before the court – in which even the disclosure is not a waiver in any other federal or state proceeding."
  - A party agreement is not effective unless incorporated into a court order.

General Failure to Use 502(d) Orders

- A 2015 Exterro Survey of judges found that 45% of them reported that the biggest area where they believed parties could cut costs in litigation was with a privilege waiver under 502(d).
- 50% cited FRE 502(d) as the most underutilized e-discovery rule in their courtroom.
- The Sedona Conference also noted the failure of counsel to use the 502(d) order and attempted to "breathe life" back into 502(d).
- Some judges have suggested that failure to secure a 502(d) order is tantamount to malpractice.

Consider a 502(d) Order and Clawback

- A properly drafted order can address inadvertent waiver and intentional disclosure.
- Resulting in expedited discovery and cost savings.
- Potentially useful for limited disclosures of privileged communications.
  - For example producing document such as legal opinions substantiating reliance upon advice of counsel as an element of a cause of action.
- Any order should include:
  - Production is not a waiver of the privilege.
  - Be careful with “reasonable steps” language, production “whether inadvertent or otherwise” and specifically avoid any 502(b) analysis of reasonableness.
  - Use the word “inadvertent” carefully if you plan to protect intentionally produced documents.
  - Clawback process.
  - Procedures for privilege logs (if any).

But, be careful

- There is a difference between *disclosure* and *use* of privileged information produced in litigation.
- Don't rely on a 502(d) order to support a non-waiver argument if you permit use of a document at deposition or in motion practice.
  - Certain Underwriters at Lloyd's, London v. Nat'l RR Passenger Corp, 2016 WL 6875968 (EDNY Nov. 17, 2016).
    - Amtrak produced thousands of documents pursuant to a 502(d) order. At deposition, plaintiff questioned deponent about documents containing work product designation. Amtrak reserved its right to object but never asserted a privileged objection. The next day, Amtrak asserted privilege and clawed back the documents.
    - Court found that while the 502(d) order applied to the disclosure, it did not apply to the use during deposition, which, if unopposed, could constitute waiver.

The opposing view

- Once privileged data is viewed by the other party, it potentially provides the other party with critical information.
  - Your adversary could use the information to pursue legitimate discovery
- A 502(d) order doesn't limit review obligations because you still have to conduct a detailed review of documents prior to discovery.
- Multi-jurisdictional litigation may present challenges because of overlapping (and inconsistent) state and federal rules.

Questions?