



# Failing to Plan is Planning to Fail: Guide to Practical E-Discovery

by Jennifer Baumann; Thompson Coburn LLP; St. Louis, MO and  
Julia Voss, Greenfelder, Hemker, and Gale, P.C.; St. Louis MO

(Reprinted with permission of the Bar Association of Metropolitan St. Louis and the *St. Louis Bar Journal*.)

**Ignoring the capabilities which ESI allows the parties to search for and produce factual information ... is like pretending businesses still communicate by smoke signals.”**

*In re Domestic Drywall Antitrust Litig.*, 300 F.R.D. 228, 229 (E.D. Pa. 2014)

Counsel and clients cannot ignore the reality that technology is an essential component in modern litigation. Even a small lawsuit is likely to have relevant e-mails, voicemails, text messages, social media posts, or other electronically stored information (“ESI”).<sup>1</sup> In a large case, the volume of relevant ESI can be staggering. Having a practical plan for managing ESI is essential to successfully and competently handling a case of any size.

Both the Federal and Missouri Rules of Civil Procedure call for “the just, speedy and inexpensive determination of every action.” FED. R. CIV. P. 1; Rule 41.03. This means parties need to cooperate and have translucency to focus on what is really needed to support claims and defenses, minimize motion practice, and get the case to a decision point based on case merits (whether that is settlement, mediation, arbitration or trial), rather than making the case about the discovery process. Establishing an ESI plan is a crucial part of your case and should start as soon as litigation is reasonably anticipated. This article provides a series of checklists for practical consideration of the process that is involved in preserving, identifying, collecting and producing ESI. These checklists are intended to provide a framework or roadmap for E-Discovery, but they do not address all issues that may be encountered in a case. Use them as a starting point for understanding and discussion, and scale them as appropriate for your case.

## I. Assessment/Initial Discussions

### A. Client Assessment

1. Assess your client’s sophistication regarding ESI and appoint a contact at the client for data and document preservation/collection issues.

2. If you already know who the key witnesses will be, identify them to start to get an idea of how many witnesses’ documents you will need to gather.
3. Discuss whether preservation will be by collecting the data or by preserving it in place.
  - a. Consider issues of ESI being overwritten or automatically deleted if left in place.
4. Establish a timeframe for preservation, including issuance of litigation hold (see below).

### B. Obtain from the client:

1. A data map (if none exists, work with the client to create a map of where all ESI exists)
  - a. What hardware/software impacted?
  - b. Relevant communications (email, text, instant message, twitter, blog, etc.).
  - c. Mobile devices implicated?
2. Who is the most knowledgeable about the client’s ESI and associated technology?
3. Organizational charts for corporate clients
4. Document retention/destruction policy(s). Review any retention policies and determine whether they have been complied with and determine what policies will need to be suspended so that ESI is preserved. May need to confer with:
  - a. IT Department
  - b. Records managers
  - c. Human resources

“E-Discovery” > p25

<sup>1</sup> Throughout this article, if we use a term of art with which you are not familiar, we encourage you to review THE SEDONA CONFERENCE

GLOSSARY: E-DISCOVERY AND DIGITAL INFORMATION (4th ed. 2014), available at <https://thesedonaconference.org/download-pub/3757>.

- d. In-House counsel
  - 5. List of potentially privileged individuals/entities (including domain names for outside counsel).
  - 6. Password/encryption lists, if applicable.
- C. Discuss with the client:**
- 1. Stopping the routine data destruction of relevant ESI, including backup tapes where applicable.
  - 2. Who will do the collection (the client or a vendor).
    - a. Assess whether a vendor needs to be retained (possible reasons to retain a vendor: to prevent spoliation, possible bad actors with the client, limited knowledge or capabilities by counsel/client in preventing data destruction/ESI collection).
      - i. If you are using vendors for any portion of the ESI process, make sure to get quotes early on in the process. Check with the client to see if they have any preferred vendor agreements that will impact vendor selection.
      - ii. For smaller cases/firms, there is reasonably priced software and services available to allow counsel to affordably manage ESI.
    - b. A sophisticated client may have the capabilities to preserve and collect the ESI.
    - c. Consider whether the case warrants forensic collection instead of copying ESI (possible reasons include: deleted items are at issue; trade secrets involved; non-user information is important; potential bad actors; when an external drive was connected is important).

## II. Detailed Preservation Planning by the Legal Team:

### A. Who:

- 1. Which people (commonly referred to as *custodians*) are likely to have relevant documents and data.
  - a. This may include considering whether assistants or family members have access to the custodian's documents and need to be identified as part of the preservation effort.
  - b. May need to consider if a "custodian" is not a particular person, but a shared departmental drive or a database, where multiple people may have access/add/modify the information.

- c. The burden for preserving documents and data will relate to these individuals, but the duty to preserve is required by the individuals **and** by the organization.
    - i. Ex.: Divorce Case: Family members may share a computer, with access to documents, email and social media. All household members must be informed of the duty not to delete anything.
    - ii. Ex.: Commercial Case: An employee may be the keeper of a document, but the commercial entity has an obligation to make sure the documents are preserved, even if they are created and maintained by the individual employee. Or an employee's home computer may need to be preserved if the employee works at home or accesses the employer's network from home.
  - 2. Other departments, such as Accounting or HR, may have relevant information.
  - 3. Third parties over whom client has control.
    - a. Identify whether you have the practical or legal ability to obtain documents from a third party. Examples may include outside accountants and suppliers/vendors.
    - b. Identify nonparties that may have relevant data/documents and issue a notice to preserve; this includes any data that is stored in a cloud based solution.
- B. What is the case about?**
- 1. Define the scope of what is relevant to the claims and defenses at issue in the case.
- C. Where (to locate the potential sources of ESI and documents for the relevant custodians)?**
- 1. Reference the data map.
  - 2. Interview key custodians.
  - 3. Provide custodians with surveys to determine what type of data/documents they generate, what devices they use, and how they store data and documents.
  - 4. A non-exhaustive list of potential sources of ESI:
    - a. Network files
    - b. Shared or Departmental Drives
    - c. Desktops
    - d. Laptops

"E-Discovery" > p26

- e. Company Email Systems (e.g. Outlook, Lotus Notes)
- f. Voicemail
- g. Shared or Departmental Drives
- h. Surveillance Tapes
- i. Cell Phones/ Tablets
- j. The Cloud
- k. Instant Messaging
- l. BackUp Tapes
- m. Portable Devices: hard drives, CDs, DVDs, Thumb Drives
- n. Social Media (e.g. Facebook, MySpace, Twitter, Instagram, YouTube, LinkedIn, Flickr, Tumblr, Vine, etc.)
- o. Legacy Systems
- p. Databases
- q. Unstructured Data Repositories
- r. Personal Computers
- s. Personal Email Accounts (e.g. Gmail, Yahoo, Hotmail, etc.)

### D. When:

1. What is the relevant time period for the data and documents you need to identify?
2. Will documents and data created after the date of the suit be implicated?

### E. How: How are you going to collect the ESI and produce it?

### F. How long: How long will it take you from collection to production?

### G. How much:

1. After consultation with opposing counsel, narrow the ESI to be preserved by identifying specific custodians, date ranges, sources, and search terms. Litigation costs can be reduced by reducing preservation and collection required. The comments to the 2006 Rule Amendments for FRCP 26 recognize the value of targeted preservation and urge parties in litigation to reach agreement. FED. R. CIV. P. 26 cmt. subdiv. (f) (2006). A defensible E-Discovery process, litigation hold procedure and an agreement about ESI protocol

are reasonable steps to reducing ESI and litigation costs.

2. The duty to preserve requires reasonable efforts to collect potentially relevant information. As stated by the Delaware Court of Chancery: “Parties are not required to preserve every shred of information. **Act reasonably.**” *Guidelines for Persons Litigating in the Court of Chancery – Ex. 10, DELAWARE STATE COURTS, § I(C)*, <http://courts.delaware.gov/chancery/docs/SampleDocCollectionOutline.pdf> (last visited Apr. 17, 2015) (emphasis added).

## III. Litigation Hold

**A. Triggering Event:** Determine if a triggering event has occurred that requires a litigation hold notice to issue. A litigation hold should occur whenever litigation can reasonably be anticipated. The facts in each individual case will influence when this occurs, but it could be when your client *receives* a claim, demand letter, preservation letter, subpoena, notice of government investigation, or service of a lawsuit. However, a litigation hold should also be *issued* when your client anticipates filing litigation or sends a notice of breach of contract or a cease and desist letter.

**B. Suspend deletion** of potentially relevant documents and data. Work with your client’s IT Department or retain an IT vendor to assist, including identifying and halting any documents and data that are subject to regular and/or automatic deletion.

**C.** As you are investigating **what** needs to be preserved, it needs to be determined **who** a litigation hold notice should be issued to for preservation of data and documents.<sup>2</sup> These may include:

1. Key custodians
2. Supervisors of key custodians and any department that may have relevant records.
3. IT Department
4. HR Department (to manage any litigation hold to help manage preservation of data/documents in light of any new or departing employees).

---

“E-Discovery” > p27

<sup>2</sup> Be mindful that at least one court has found that a litigation hold notice was not privileged or attorney work product when the notice was too broadly disseminated and lacked any detailed confidentiality instructions. Several courts have found that a litigation hold may be

discoverable upon a preliminary showing of spoliation. It is advisable to mark the notice an attorney-client privileged communication and as confidential.

5. Records managers
  6. Third parties, including vendors and cloud providers, with relevant data/documents.
- D. How will the litigation hold be issued?**
1. Does the client have litigation hold management system or procedures to handle this?
  2. Do you have software available that would send and track?
  3. Email and/or memo sent internally from client?
- E. How will the litigation notice be followed up on and reminders given?**
- F. Best practice is to issue a written Litigation Hold Notice (and some jurisdictions require it). You may need to give an oral instruction sooner if destruction is imminent before a written hold can be disseminated.**
- G. Draft the Litigation Hold Notice to:**
1. Identify the scope of relevant data by topic and date.
  2. State that the notice is privileged and confidential.
  3. Explain that the notice, its language and the directions therein are confidential and should not be shared inside or outside of the company without express approval.
  4. Instruct that data/documents related to the scope of the hold should not be destroyed or deleted.
  5. Explain the potential ramifications for failing to comply with the litigation hold.
  6. Explain that the duty to preserve documents/data is continuing until instructed that the Litigation Hold has been terminated.
  7. Request the recipient identify other potential custodians not included in the initial hold.
  8. Provide a contact for questions regarding preservation.
  9. Request confirmation of receipt and understanding.
  10. Tailor your litigation hold notice to provide information regarding what needs to be preserved and what issues are in the case without disclosing information that may be confidential or damaging should the notice need to be produced.
- H. As litigation progresses:**
1. Follow up with periodic reminders of the litigation hold.
2. Communicate any changes in scope of preservation.
  3. Keep track of the litigation hold notice:
    - a. To whom it has been issued;
    - b. Acknowledgment of receipt;
    - c. Follow-up and update communications; and
    - d. Reminders that the hold remains in place.
  4. Release the Litigation Hold at the end of case when there is no longer a duty to preserve.
- I. Consider sending a Document Preservation Notice to the party to put them on notice of the duty to preserve, identifying any documents or data that you are specifically aware of that should be held. Follow up later with opposing counsel regarding what documents and data the other party has and what should be and should not be preserved. Do not demand preservation of unwanted or unneeded things, consider if you really need “any or all” of the ESI. Overbroad preservation requests likely will be seen as obstructionist, inviting motion practice that could easily be avoided.**
1. Following the preservation demand, communicate with opposing counsel regarding what each party reasonably needs from the other.
  2. Serve discovery (or an early draft of discovery that you are contemplating serving) on the opposing side, to allow meaningful discussion of the issues. Recognizing the difficulty in having meaningful ESI discussions without knowing what will be requested, the proposed FRCP amendments allow for discovery to be delivered before the Rule 26(f) conference, but it is not considered served until the conference.
  3. Set a timeline for the meet and confer process.
  4. Provide opposing counsel with a proposed protocol to aid discussion. Many states and federal courts have developed model protocols. *See infra note 3.*

## IV. Meet & Confer Process

### A. Plan and Prepare

1. Meet and confers, if used properly, are more than just a perfunctory requirement that you check off after a phone conversation.
2. Prior to a meet and confer, meet with your client to understand what ESI exists, what ESI is likely relevant

## E-Discovery (from page 27)

---

to the claims in the case, and what burdens may exist in collecting and producing the ESI.

3. Meet with an IT person either at your client or one retained that can help you understand the technology and data the client has. Discuss bringing your IT person to the meet and confer.
4. Know what you need, what your limits and burdens are prior the conference and understand why.

### B. Creating a Structured Meet & Confer Process

1. Depending on the size and complexity of the ESI involved in your case, you may need to discuss with opposing counsel how the meet and confer process will be structured and how much time it will take.
2. Do you need multiple conferences? In person/by phone?
3. At one or all conferences, should you have a client representative and/or IT person available or present?
4. Define the scope of the meet and confer.
5. Determine how much information will be shared at the meet and confer, and what information will be provided beforehand? Consider:
  - a. Potential custodians or number of custodians
  - b. Volume of ESI
  - c. Sources, content, and storage of ESI
    - i. Location of data sources: cloud, portable media, server, backup tapes, etc.
  - d. Accessibility of data (if it is inaccessible, how?)

### C. Have Court Involvement:

1. Courts are finding with regularity that active case management, not micromanagement, is making the review, identification and production of relevant documents and data much more efficient for the parties.

2. The scheduling of monthly or quarterly telephonic status conferences and the requirement that parties file joint stipulations regarding ESI issues greatly improve discovery cooperation and timeliness.

- a. The scheduling order should include specific requirements that the parties need to discuss and report back. This brings the issues to the forefront early in the case; having the parties agree that certain ESI is not at issue or does not need to be preserved is just as valuable as the parties agreeing on custodians, ESI needed, search terms, and application of technology assisted review.
- b. Consider an ESI protocol that requires that any disputes be brought to the court's attention before motions are filed. A phone call with the court may resolve a dispute without the need for motions and formal hearings.
- c. Consider the practice rules of the court where your case is pending and review court wide forms that are available from court websites. Several federal courts have available forms.<sup>3</sup>
- d. If the parties are in agreement that a status conference with the court is not needed, they can so notify the court.

3. The ultimate goal of involvement is to encourage, promote, and enforce cooperation among parties during discovery so that costs are reduced, unnecessary motion practice is eliminated, and the early trial setting is preserved.

### D. The Meet & Confer and Creation of an ESI protocol

1. **Purpose:** to establish an ESI protocol that gives the parties a framework for addressing ESI issues.
2. **Consider proportionality:** The parties should weigh the nature of the claim, the amount in controversy, agreements of the parties, the relative ability of the parties to conduct E-discovery and the burden that may be imposed.

---

"E-Discovery" > p29

<sup>3</sup> Several courts have protocols, forms, model orders and other information available for your reference including (but not limited to): N.D. California, available at <http://www.cand.uscourts.gov/eDiscoveryGuidelines>; Delaware Chancery Court, available at <http://courts.delaware.gov/Chancery/docs/CompleteGuidelines2014.pdf>; 7th Circuit Ediscovery Pilot Program, available at <http://www.discoverypilot.com/>; E.D. Texas (for patent cases), available at <http://www.txed.uscourts.gov/page1.shtml?location=attorney> (follow "Order Regarding

E-Discovery in Patent Cases" hyperlink); S.D. New York (pilot project for complex case management in civil cases), available at [http://www.nysd.uscourts.gov/rules/Complex\\_Civil\\_Rules\\_Pilot\\_14.11.14.pdf](http://www.nysd.uscourts.gov/rules/Complex_Civil_Rules_Pilot_14.11.14.pdf); E.D. Michigan, available at <http://www.mied.uscourts.gov/pdf/SteehEsiOrderChecklist.pdf>; W.D. Penn. (ediscovery special masters program), available at <http://www.pawd.uscourts.gov/Pages/ediscovery.htm>.

## E-Discovery *(from page 28)*

---

### 3. Discuss:

- a. What types of relevant, nonprivileged accessible ESI will be preserved?
- b. What will be the production format (native, tiff, pdf, other)? Will hard copy documents be produced in paper or scanned to pdf? Will ESI be in a searchable or non-searchable format? What content will be included in a load file?
- c. Number and identity of custodians; who is the opposition interested in as a custodian?
- d. Are there issues in the case that are not disputed that you can agree NOT to conduct any eDiscovery on? Federal Rule of Civil Procedure 26(g) states that discovery should not be taken if it's not needed. Missouri Rule of Civil Procedure 55.03(c) similarly states that nothing submitted to another attorney or party shall be for an improper purpose, such as harassment or to increase the costs of litigation.
- e. Are there accessible ESI sources that are not relevant to the case and do not need to be preserved (text messages, GPS data, etc.)? Have this as part of your written agreement or seek entry of a protective order.
- f. Are there types of ESI that may not be reasonably accessible? If potentially relevant, discuss why the data is not accessible, the type of ESI, costs and burden of preserving, retrieving and who will bear those costs.
- g. Proportionality and if costs/burden of requests outweigh needs/benefit of the case.
- h. Search and retrieval protocols: custodians, file types, sources, key word searches, use of computer analytics, and use of Technology Assisted Review.
- i. Costs and potential for cost shifting/sharing?
- j. Point of contact on each side for ESI: who will be in contact on these issues?
- k. What is the anticipated timeframe for collection, processing, review, and production of ESI? Is a rolling production advisable? How will this be structured in the scheduling order? What will be the impact on depositions and other deadlines?
- l. How will disputes regarding ESI be resolved, including claims that ESI is inaccessible?

- m. Determine if there are foreign privacy or export restrictions.
- n. What ESI will specifically not be discoverable? Such as:
  - i. Deleted, slack, fragmented or unallocated data on hard drives
  - ii. Random Access Memory (RAM) or other ephemeral data
  - iii. On-line access data (usernames/passwords)
  - iv. Data in metadata fields that are frequently updated automatically
  - v. Backup data that is substantially duplicative of data that is more accessible elsewhere
  - vi. Legacy data
  - vii. Information that requires substantial additional programming/transforming before search & retrieval can be achieved.
  - viii. Other ESI forms that would require extraordinary affirmative measures.

### 4. How will privileged communications and confidential documents be protected?

- a. Federal Rule of Evidence 502(d) order: An order, entered separately or as part of a scheduling order, protective order or ESI protocol signed and entered by the court, which states the production of privileged documents will not waive the privilege in the current case or in other federal or state proceedings. Some states, but not Missouri, have adopted a comparable rule.
- b. Clawback processes: Agreement about how inadvertently produced documents will be sequestered or returned if/until a determination can be made as to whether the documents are privileged.
- c. Privilege logs:
  - i. Agree that communication after a certain date (filing of lawsuit or when litigation was reasonably anticipated) need not be logged.
  - ii. Discuss logging emails only by the last in a string or in a thread.
  - iii. Discuss providing a log by category or ranges of privileged materials.

"E-Discovery" > p30

- d. Will there be levels of confidentiality and is there a need for entry of a protective order?
5. Come armed with information.
  - a. For example: If search terms were previously exchanged and run, and the results are too voluminous and need further negotiation, come armed with information about the process. Do not just say that the terms returned “too many hits.” Have the data to back-up that statement and be willing to share that data if necessary. Be prepared to explain that X term across Y custodians returned Z hits, and that such results create a pool that is too burdensome given the scope of the case. Come prepared with a plan to solve the problem. Propose to modify X term, which then gives us we get W results, which we find acceptable. Can we agree to modify terms?
6. Federal Rule of Civil Procedure 26(a)(1)(C): The Rule 26(f) conference should occur as soon as practical, but at least 21 days before a scheduling conference. Items to be discussed at the conference include preservation of discoverable information and developing a proposed discovery plan (including discovery of ESI and the production format).
7. Plan on being **reasonable**: “[T]o allow [plaintiff] to now seek shelter from a fallback position that [third party respondent] previously tendered in good faith would make a mockery of both parties’ obligation to meet and confer in good faith from the start. The time to tap flexibility and creativity is during meet and confer, not after.” *Boston Scientific Corp. v. Lee*, No. 5:14-mc-80188, 2014 WL 3851157, at \*7 (N.D. Cal. Aug. 4, 2014). “[T]o accommodate [plaintiff’s] demand would ‘encourage litigants to demand the moon thinking they can always fall back to something reasonable. They should be reasonable from the start.’” *Id.* at \*7 n. 59 (quoting *Straight Path IP Group, Inc. v. Blackberry Ltd.*, No. 3:14-mc-80150, 2014 WL 3401723, at \*1 (N.D. Cal. July 8, 2014) (emphasis added).
8. Reduce your meet and confer to a written plan or protocol and present to the court.

### V. Collection Plan

- A. **What** is the scope of the collection?
  1. Will paper documents be produced as hard copies or scanned to pdf?

2. ESI from identified custodians/source: will all data that has been preserved be collected or have the parties agreed to limited or targeted collections?
3. What format does the ESI exist natively in and does it need to be converted to a usable format to be collected?
4. What metadata needs to be collected?
- B. **When** will the data/documents be collected and **how long** will the collection take?
- C. **What** are the possible issues with the data being collected?
  1. Difficult source material:
    - a. Database (dynamic, how to collect/preserve; can you export it to Excel, xml, Access)
    - b. Proprietary software/system
    - c. Encryption
    - d. Email source: outlook v. web-based pose different collection issues; make sure that emails are collected appropriately and not just forwarded to counsel in a way that impacts metadata and implicates redaction.
  2. If using search terms, discuss how non-searchable documents will be treated. Does non-searchable ESI need to be processed and made searchable, do the parties accept limitations of searching in the native application, or does manual review of these non-searchable documents need to occur? This issue may arise where a non-searchable pdf is attached to an email or where pictures or images are at issue.
- D. During collection, address any spoliation concerns that may become apparent.

### VI. Processing

- A. **Purpose**: Processing is the ingestion of ESI into a program to allow for extraction of metadata and text. In applicable cases it may include the creation of static images and application of specifications such as deduplication and filtering based on date before loading to a review database.
- B. **Who** will be handling the processing of ESI (Client, Vendor, law firm)?

## E-Discovery (from page 30)

---

### C. What:

1. **Is the cost?** Costs can vary. Get estimates from several sources or investigate purchasing programs/services to be available within your firm. Make sure you understand what is and what is not included in the prices, and evaluate what will work best for your case.
2. **Timeframe:** Do not underestimate how long this can take. Work to set realistic timelines that you have confirmed before agreeing to deadlines with opposing counsel.
3. **Workflow:** Establish the process for transfer to the vendor, and what services will be provided.

### D. How much can the volume of data be reduced by:

1. De-Duplication: within a custodian or across custodians (global deduplication).
2. De-NISTing
3. Exclusion of certain file types or domain names
4. Date range application
5. Keywords/phrases: test reliability of search results and agree with other side that after search terms are run, anything that produces odd results (too voluminous, not returning what anticipated) will be discussed and terms refined.
6. Data sampling

## VII. Review

### A. Who will review (Vendor, Client, Law Firm, Outsource)?

### B. How will the documents be reviewed?

1. If you have a large volume of documents needing review, you should take advantage of a review platform. There are a variety of programs on the market that may be used internally or hosted by a vendor.
2. Linear Review, Search Terms, Analytics, and/or Technology Assisted Review? These tools are not mutually exclusive, and may be used contemporaneously. Some tools to consider are:
  - a. Email Threading: Maintains emails by conversation.
  - b. Near Duplicates: Identifies documents that contain a set level of identical text.
  - c. Clustering: Creates clusters of documents that are conceptually similar.

d. Categorization: Extrapolates coding done by reviewers to conceptually similar documents.

e. Technology Assisted Review (predicative coding and/or analytics): The process of using categorization until the legal team is satisfied that the coding calls made by the computer are satisfactory.

### 3. Coding: Categories to consider include:

- a. Responsiveness
- b. Privilege
- c. Confidentiality
- d. Issue Coding

### 4. How will families be treated?

- a. A family is a group of separate documents that have been grouped together: e.g., an email (parent) and its attachments (children).
- b. Families are generally produced together, even if some of the documents in the family are not responsive. If you are going to deviate from this practice, discuss with opposing counsel and get an upfront agreement as to how this will be handled.

5. Redactions: Redact privileged information and personal identifiable information (e.g. Social Security numbers). Review platforms will have built in redacting capabilities, but if you are working with pdf's, only redact in a program where the redactions are permanently burned into the image (such as AdobePro) so that opposing counsel cannot remove the redaction.

6. Confidentiality: Documents need to be coded according to any agreed confidentiality as set forth in a protective order.

## VIII. Production

### A. What Format:

1. Native, Tiff, searchable PDF, other image format
2. Load file for images produced
3. Bates numbers and/or file naming for unique or native documents
4. Overlays/branding for confidentiality

### B. How will the data/documents be produced:

"E-Discovery" > p32

1. Delivery by: paper, disk, external drive, online website, FTP transfer
2. Encryption: encrypted files, drives, or access for electronic delivery
  - a. What safeguards will be in place for treatment of the documents once they are received? The security you have put in place will not do any good if there is not an agreement by opposing counsel on how the documents will be treated once they are received and unencrypted.

## IX. Requests for Production and Interrogatories

### A. Requests For Production

1. Make sure your RFP definition of “documents” includes ESI.
2. Make sure you define ESI to include the relevant sources needed for your claims/defenses, which may include: standard Office products (Word, Excel, PowerPoint), email (client or web based), databases, voice recordings, video, industry specific software or data, websites, social media, portable devices (including cell phones, tablets, thumb drives, etc), and related metadata.
3. Social Media should include any potential postings, comments, messages or other content relating to the

allegations from Facebook, Twitter, YouTube, etc, as well as the social networking providers, social profiles, and handles.

4. Specify (if not agreed upon in an ESI protocol) the format of production (native, paper, PDF, TIFF) and the metadata to be produced (author, create date/time, file type, etc.).

### B. Interrogatories

1. What ESI do they use during the relevant time period that would be relevant to claims?
2. Email address(s) or domain name(s) used by the party.
3. Some courts may limit how early in the case social media inquiries may be posed, *see, e.g.*, S.D.N.Y. Local Civil Rule 33.3, but where you can, inquire as to:
  - a. Social media platforms/accounts established/used/maintained;
  - b. Email address(s) associated with any accounts; and
  - c. Names/user names/pseudonym/handles for those accounts.

Of course no checklist can account for every contingency that may occur in litigation. But if you have planned and prepared as suggested above, you will have laid the groundwork to handle any E-Discovery issue that presents itself in your case.



## Recent Developments in Missouri Law

by Rick Wuestling and Adina Johnson; Wuestling & James, L.C.; St. Louis, MO

### I. Eastern District Court of Appeals

The Eastern District Court of Appeals recently decided two cases involving very different aspects of premises liability litigation.

#### A. Independent Contractor

In *Woodall v. Christian Hospital NE-NW*, the Eastern District decided premises liability issues raised by an independent contractor’s injury claim.<sup>1</sup> In this case,

Christian Hospital NE-NW (the hospital) contracted with Envirotech for asbestos abatement in one of its buildings.<sup>2</sup> The plaintiff, Clyde Woodall, was an Envirotech employee.<sup>3</sup> Envirotech was allowed unfettered access to the entire building. But the hospital retained ownership, and had the right to be in the building even though no medical services were being provided there.<sup>4</sup> And hospital employees regularly accessed the building.<sup>5</sup>

“Recent Developments” > p33

<sup>1</sup> *Woodall v. Christian Hospital NE-NW*, No. ED 101777, 2015 WL 5025123, ---S.W.3d --- (Mo. Ct. App. E.D. Aug. 25, 2015).

<sup>2</sup> *Id.* at \*1.

<sup>3</sup> *Id.*

<sup>4</sup> *Id.*

<sup>5</sup> *Id.*