§ 6.10

E-Discovery

Requesting and Responding

THE FRONTIER IN DISCOVERY

A paralegal today needs to be familiar with the concept of E-Discovery, including the process and potential techniques. While a paralegal will not typically be involved in the forensic duplication, copying, or search of an opposing party's computers and data drives, a paralegal may be intimately involved in the process of requesting information and evaluating information that has been produced as a result of E-Discovery.

The following is not intended to provide every aspect of E-Discovery. That would take an entire volume. Because E-Discovery is evolving and is approached differently from jurisdiction to jurisdiction, sometimes even from county to county, a paralegal must be open to frequently new developments. The goal in this textbook is to provide students with a solid foundation in the issues involved in, and possible procedures to implement, the process of E-Discovery. The paralegal who can speak the language of electronic data retention and acquisition has a definite advantage.

THE TERMINOLOGY OF E-DISCOVERY

Terms with asterisks (*****) are particularly important to know.

ESI *****
Electronically stored information. Basically, it means digital data.

Media
A device capable of storing electronic data, such as a computer, floppy disk, flash drive, tape drive, server, etc.

Forensic examination *****
In E-Discovery, forensic examination is the analysis of data on a computer, including readily accessible files and hidden files, such as metadata or embedded data.

Discovery plan *****
Even in states where rules do not require it, courts are emphasizing the importance of parties working together to establish a plan for exchanging discovery. The plan usually includes dates for responding to discovery and may include dates for a second round of discovery. The discovery plan that includes E-Discovery would typically include agreeing to a litigation hold, setting dates for examination of data or for examination of media sources by experts (if the native files are requested), a plan for dealing with private or privileged material, and the all-

important *Non-Waiver of Privilege* agreement.

Metadata *****
Visible data is that which is readily observed on a computer. Almost all visible data generated by computer includes "invisible" *metadata*, which stores such information as who created the document, when it was created, when it was last opened, when it was last altered, and so forth. The metadata is very difficult to alter or fake and is generally used to help determine the validity or authenticity of the visible data. In addition, computer systems have their own metadata. Thus, a forensic examination can determine whether the date and time on a computer system has been manipulated.

Embedded data
Similar to metadata, embedded data is typically not visible. For example, some data processing documents (such as *Microsoft Word* or *WordPerfect*) track changes to documents. While embedded data is more subject to manipulation than metadata, it is useful in determining document validity.

Native files *****
Files in their original state, including metadata and embedded data.

Preservation *****
The protection of data already created (similar to *Retention*).

Retention *****
The ongoing protection of data yet to be or being produced (similar to *Preservation*).

Litigation hold *****
The concept that a company involved, or potentially involved, in litigation has the obligation to preserve data that may later be deemed relevant to that litigation. Courts have ruled that a party may be subject to sanctions for failing to initiate a litigation hold early enough, even prior to the filing of a lawsuit.

Spoliation *****
Spoliation is a general legal term that refers to evidence that has not been properly preserved for use by another in pending or future litigation. In E-Discovery, this may include files that are not in their original state or files that have been lost or destroyed. Spoliation may be caused by the innocent opening of a file, or intentional attempts to delete or alter the file. Sanctions for spoliation can be severe.

Post-production spoliation motions
A party who allows spoliation may be sanctioned by the court. Sanctions may range from loss of the right to present certain evidence to dismissal of the case, depending on the seriousness of the spoliation. Remedies sought in such motions may include:

- *Default judgment*
- *Dismissal*
- *Fines*
- *Award of attorneys' fees*
- *Contempt citation*
- *Disqualification of counsel*
- *Adverse inference instruction*
- *Exclusion of evidence*

Adverse inference instruction
This dreaded measure is used in extreme cases where a party has allowed evidence to be subject to spoliation. Basically, a jury is told that evidence that should have been available has been altered or destroyed, and the jury may infer that the destruction was an attempt to hide damaging information.

Confidentiality agreement *****
An agreement between parties that certain information shall not be shared or discussed with anyone else. A confidentiality agreement is critical when dealing with experts or outside entities during the process.

Non-waiver agreements
A non-waiver agreement during the E-Discovery process usually refers to information exposed during the examination of data that would under any other circumstance be privileged, such as medical information or communications between a party and his or her attorney. The agreement states that any inadvertent disclosure of privileged information must be excluded from litigation, and that the *existence* of such data, that would constitute exposed privileged information, is disclosed to the all parties.

Two-Tiered E-Discovery plan *****
In order to limit the high cost of E-Discovery, courts have been receptive to alternate solutions to full-blown data extraction. One such solution is the Two-Tiered E-Discovery plan.

In such a case, the responding party first discloses files and information from active data (data that is readily accessible to the user). If the requesting party is not satisfied with those results, or if spoliation or fraud is suspected, that party may request a second, more intrusive response that would include extensive data extraction (including metadata, fragmented data, and embedded data). Typically, the court would need to be convinced that the initial (active data) response was not sufficient, and that the second tier would result in additional relevant data.

Legacy data *****
Data on older forms of media storage, such as tape drives.

Fragmented data *****
Information that is spread across a hard drive. Fragmented data may be reassembled and recovered by an expert in some cases. An example of fragmented data is a deleted document. Even though the document is no longer visible on the hard drive, the bits that made-up the document probably still reside on the drive. Those bits are now simply marked by the computer's operating system as being able to be overwritten. But until the hard drive is filled up, those bits retain the information that make up the document. An expert may be able to reassemble those bits to reconstruct the document.

Active Data *****
Files currently on the hard drive that are accessible through standard means.

Latent (or Ambient) Data *****
Deleted files and other data still on the hard drive, but not readily accessible, such as metadata, temporary files, printer spool files, and other digitally dispersed data. This data is likely to require an expert to recover.

Archival Data
Data kept on media other than the original drive. One problem with archival data is that it usually does not include latent data, which may be critical in determining authenticity. This is also why just copying files from a hard drive is not always sufficient for E-Discovery purposes.

Hard drive image *****
An image of a hard drive preserves the metadata and embedded data. It is an exact replica, bit by bit, of the original hard drive. Instead of simply copying the files that reside on the hard drive, an image duplicates every aspect of the hard drive. Obtaining a hard drive image must be done carefully and every step documented so as to ensure the accuracy of the evidence and to preserve the "chain of custody."

Electronic Discovery Expert
An electronic discovery expert searches through the extracted media for relevant documents, files, or other data.

Forensic Computer Technologist *****
A forensic computer technologist is the expert who extracts data.

Sampling *****
Sometimes there is a dispute over the need for E-Discovery. The responding party may claim that the request constitutes an undue burden of massive production. This is where sampling comes in. A forensic expert takes a sample, a fraction, of the data requested. If relevant information is discovered, the party will most likely have to produce. If no relevant information is found in the sample, the requesting party will have a very difficult time convincing the court that more data is needed. (FYI: Sampling is provided for in F.R.C.P. Rule 34(a)).

Cost-shifting

Courts have ruled that the party producing the documents generally bears the burden of cost. In order to shift the cost to the requesting party, a court must be convinced that doing so is justified. *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309 (S.D.N.Y. 2003) has established a 7-part test for cost-shifting. Those considerations include:

1. *Is the request specifically tailored to discover relevant information?*
2. *Is the information available from other sources?*
3. *How does cost of production compare to the amount in controversy?*
4. *What are the relative positions of the parties in terms of resources?*
5. *Who is best able to control costs and has an incentive to do so?*
6. *Are the issues in discovery key to the issues at stake in the litigation?*
7. *What are the relative benefits to the parties of obtaining the data?*

*The Sedona Conference **

There is no single source for answering E-Discovery issues, but several groups are attempting to establsih standards that could be adopted by state and federal courts. The *Sedona Conference* is an annual conference that deals with current legal issues, including such topics as E-Discovery. Many publications and courts, cite *Sedona* as an influence in developing E-Discovery procedures.

THE FOUNDATIONS OF E-DISCOVERY

A few foundational points regarding E-Discovery:

What is encompassed by the term "E-Discovery?"

Today, the majority of document creation, communication, and administration involves electronic or computer-related processes. Since the goal of discovery is to allow parties to exchange relevant information, it is natural that part of that exchange would evolve to include electronic sources. This is E-Discovery. The problem is that we as a society have not considered the fact that information inputted to a computer is potentially discoverable in litigation. When information is requested from an electronic source, extracting what is relevant and discoverable from what is irrelevant or privileged is complicated, time consuming, and often expensive. As E-Discovery becomes more mainstream, courts and law firms will devise methods and procedures to make the process fair and, hopefully, less expensive.

When E-Discovery is warranted and when it is not

Currently most cases involving E-Discovery are larger lawsuits or complicated criminal cases with issues that at some point involve information on computers. A lawsuit involving a simple car accident would not typically involve E-Discovery (unless an on-board computer monitoring system existed). An insurance fraud lawsuit involving the same car accident might involve E-Discovery if there was reason to believe that computers, cell phones or other electronic sources held information relevant to the alleged fraud.

What kind of expert will the firm need?

It depends on what the firm is looking for. If the firm does not anticipate the need to determine whether files or drives were modified, deleted, or improperly copied, an E-Discovery vendor may be enough. But if there is the need to determine whether spoliation has taken place, a highly qualified *forensic computer expert* will probably be required.

Privacy issues

If E-Discovery is part of litigation, a party may ask for more than simply a set of documents (such as emails or files) found on the other party's computer. The requesting party may ask to view the original (also called "native") files. This means that the party wants to obtain a copy of the computer hard drive (or other digital media, such as discs or back-up drives). The problem is that most of the information on that drive typically has nothing to do with the lawsuit. The extraneous information may even be private and/or confidential. Procedures are taking shape to help ensure that this material, and material protected by any potential privilege, is not at risk.

THE THREE STAGES OF E-DISCOVERY

There are three stages to the E-Discovery process. They are:

1. *The Pre-Litigation Stage*
2. *The Requesting Stage*
3. *The Responding Stage*

1. THE PRE-LITIGATION STAGE: ANTICIPATING E-DISCOVERY

This stage is often the most neglected point of the E-Discovery process. E-Discovery is a relatively new process, and the focus has been placed on demand of material and compliance. The problem is that by the time electronic data is requested, it is sometimes too late due to intentional or unintentional destruction of data. Courts, however, are in many cases holding litigants liable for the loss of relevant data and sanctioning those litigants, even if the data was destroyed prior to litigation. The key to avoiding such an outcome is for a firm to be aware of key concepts, have a "litigation hold" policy in effect, and communicate that plan to a client when it appears that litigation is even a slight possibility. The concept of "anticipation of litigation" is incredibly important.

How a law firm needs to be prepared

A law firm should have a set of protocols in place for any potential litigation involving electronically stored data. These protocols should include helping clients establish data retention policies, how and when to communicate E-Discovery guidelines to the client, guidelines for when a litigation hold should be recommended to the client (and possibly for the law firm itself), and who will be responsible for educating the client as to data retention during a litigation hold.

Create a "Tech Team"
To be most effective, a law firm should consider creating a "Tech Team," or "E-Discovery Response Team." This team would consist of at least one lawyer, one paralegal and one legal secretary. This team would work together to educate clients about E-Discovery, help clients to develop data retention policies and coordinate E-Discovery demands and responses in coordination with the attorney of record in the case. The team would not create the requests or respond directly but would be able to help attorneys in the firm avoid pitfalls and hire competent professionals depending on the complexity of the case. Having a Tech Team in place prevents the need for every attorney and paralegal in the firm to become expert in the mechanics of the E-Discovery process.

Help the client create email and document retention policies
Every client of a law firm, especially business clients, should be provided with at least general guidelines for electronic document creation, email, and data storage. These guidelines should be provided whether or not litigation is seen as a possibility. Some examples of typical retention policies would include:

- *Limit employees to using the firm email system for only work-related communication.*
- *Require all work-related email to be created using the company's email system (no web-based email, such as Hotmail, Gmail or AOL).*
- *Provide written guidelines, including potential punishment for violation of policies.*
- *Retain all email and documents for a specified period (usually 60 or 90 days).*
- *Once a file or other data is no longer needed and is past the retention period, get rid of it as a part of the normal process of records management. Keeping old files simply because there is room for them on original or back-up media will make it much more difficult, and expensive, to sort through the data later.*
- *Ensure the policy complies with state and federal regulations and, if applicable, industry standards.*
- *Enforce the policy that is adopted. Failure to enforce a policy may be worse than not having a policy.*

What constitutes "anticipation of litigation?"
Anticipation of litigation means that a business or individual under normal circumstances would have reason to believe that another business or individual may be interested in suing. There is no set of criteria to follow, but one standard would be if a party has discussed a matter with an attorney, or if an individual has threatened to seek legal redress.

E-DISCOVERY TIP

Interrogatories can sometimes be useful in determining the extent of discoverable information that is contained on computers. An interrogatory can also be used to identify a responding party's computer network specialist and any records-retention policy that may be in effect.

When does a litigation hold come into effect?
A litigation hold is usually triggered when both of the following take place:

- ☐ *A legitimate anticipation of litigation*
- ☐ *A reasonable basis to believe that electronically stored documents or communication (data) could be requested during the discovery stage of that potential litigation*

How to accomplish a litigation hold for the client
A client should be informed, in writing the following should take place immediately:

- Data should be retained, including:
  - ☐ All data on hard drives
  - ☐ All data on back-up drives
  - ☐ All data on servers
  - ☐ All data on tape back-ups
  - ☐ All data on portable media, such as "thumb drives," "flash drives," external hard drives, CD ROMs, DVDs or DVD ROMs, floppy disks, and any other device capable of holding data

- A more comprehensive list of potential media may be found below under the *Requesting Stage*.

- Depending on the size of the firm, and the litigation involved, such data retention may be limited to individuals in the firm relevant to the litigation. The list of individuals, however, should be quite broad. Include even those who possibly had documents or communication relevant to litigation.

- Retained data may be date specific (such as going back to September of 2018), but the date criteria should be broad to ensure retention of all relevant data.

- The data retention should be ongoing and include documents and communication created "from this date forward, until otherwise informed."

The firm should be prepared to provide the client with information and references related to experts in electronic data retention and computer forensics.

2. THE REQUESTING STAGE: BROAD RETENTION – NARROW DISCOVERY

How to initiate an E-Discovery request
E-Discovery is typically a part of a *Request for Production*. It is advisable to require broad retention but request specific discovery. For example:

> *Request Number 1*
> Plaintiff requests the right to inspect any and all electronically stored or recorded **email communication** between Defendant and Plaintiff from September 2018 to present and demands that all potentially relevant data be retained until conclusion of this litigation. Please refer to Exhibit A for a list of media to be included in this request.
>
> *Request Number 2*
> Plaintiff requests the right to inspect any and all **electronically stored or recorded maps or image files** relevant to this litigation from September 2018 to present and demands that all potentially relevant data be retained until conclusion of this litigation.

The above requests are broad in terms of requiring retention of data (data to be retained), but specific as to the discovery documents sought (emails, and "maps or image files").

What "media" should be included in the request?
The requesting party is usually not aware of the kind of computer and document retention systems the responding party possesses. Thus, a broad brush is usually required. Media potentially subject to E-Discovery could include:

- ☐ Servers
- ☐ Mainframes
- ☐ Network file systems
- ☐ Workstations
- ☐ Laptop computers
- ☐ Smart phones and cell phones
- ☐ Personal home computers
- ☐ Private branch exchange (PBX)
- ☐ Voice mail
- ☐ Digital printers or copiers
- ☐ Cell phones
- ☐ Tablets, such as iPads
- ☐ SIM cards
- ☐ Monthly system-wide backups
- ☐ Weekly system-wide backups
- ☐ Incremental system-wide backups
- ☐ Unscheduled backups
- ☐ Personal backups
- ☐ CD-ROMs
- ☐ DVDs and DVD ROMs
- ☐ Floppy diskettes
- ☐ Zip disks
- ☐ Tape archives
- ☐ Removable hard drives
- ☐ Thumb Drives or Flash Drives
- ☐ USB Memory Sticks
- ☐ Digital camera media
- ☐ Online servers (Cloud servers)

You may also refer to the *Media Evaluation Exhibit Checklist* below for specific guidance regarding procedures for securing electronic data.

Locating a service to search the data
Your firm may already have experts in mind, but if your firm is new to E-Discovery, a search on the Internet may be the quickest way to find a firm with experience. A more reliable source may be to check attorney newsletters and Bar Association magazines for advertisements. In any case, be sure to ask for and check references.

3. **THE RESPONDING STAGE:** MAKING TIME STAND STILL

Clear communication between the law firm and client
An attorney, sometimes with the assistance of a paralegal, must communicate the seriousness of the E-Discovery process. The steps recommended to initiate a litigation hold are helpful, but nothing replaces clear and direct communication. It is critical that if instruction is provided orally (by phone or in person), those instructions must be included in a follow-up letter. Help protect your firm by documenting the instructions you and your attorney have provided to the client. A court may become extremely agitated if an attorney failed to provide proper guidance to the client.

Initiate a Litigation Hold, if not already in place
Once a request for E-Discovery is made, a litigation hold should go into effect. But what steps, exactly, should be taken? See the *Litigation Hold Checklist* later in this chapter for a suggested set of recommended procedures.

Searching within the data
Strategies for searching within data will depend on whether the amount of data is limited or extensive. In small cases, an attorney or paralegal may be able to review the extracted data themselves, or (as is becoming common) a team of paralegals can review the information and input relevant data into a data management system such as *Concordance* or *Summation*. If the amount of information is more substantial, an E-Discovery vendor may be more cost effective in the long term. In such a case, the vendor must be provided with guidelines for the information being sought, such as emails between specific individuals or on a specific topic, documents related to specific subject matters, etc. The vendor, often using proprietary software, searches within the data and extracts all relevant "hits." This information is then provided to the firm for analysis.

SOME FINAL E-DISCOVERY CONSIDERATIONS

Online document review
In cases involving large amounts of data for review and multiple plaintiffs or multiple defendants, the parties may choose to post discovery documents online for review. Of course, the documents would not retain all metadata and embedded data, but if that is not a concern, online review is a cost-effective, efficient means of document analysis.

Trade Secrets, personal information, and other protected data
A paralegal who assists a client in responding to E-Discovery must be sensitive to private information. In most cases, personal information and trade secrets are not within the scope of E-Discovery and should not be provided to the requesting party. If there is a dispute about whether such information is relevant, the court will most likely view the document in private (called "*in camera*") and determine whether some or all of the information is relevant and should thus be disclosed.

The high cost of E-Discovery
Even though costs are decreasing somewhat with more competition from vendors, the price of E-Discovery is alarming. Even the smallest of cases can cost five to ten thousand dollars, not including the law firm's time. The largest cases can cost more than a million dollars. Courts, therefore, must sometimes be convinced that E-Discovery is a necessary burden.

A devil's bargain?
Not all attorneys are comfortable with the technology involved in E-Discovery, or they are concerned about the high cost to the client. As a result, some attorneys enter into an informal agreement that goes something like this: "I won't ask for E-Discovery if you won't ask for E-Discovery." Be aware that such an agreement is not only unethical behavior; it could possibly expose an attorney agreeing to such an arrangement to a malpractice claim. (Could some of that electronically stored information have been of value to the client?)

AUTHORITIES SHAPING E-DISCOVERY

1. *Zubulake v. UBS Warburg LLC,* 217 F.R.D. 309 (S.D.N.Y. 2003)
   May be the landmark case on E-Discovery. Sets standards for aspects of E-Discovery, such as obligations to preserve electronic data and cost-shifting.

2. *Peskoff v. Faber*, 2006 WL 1933483 (D.D.C. 2006)
   The court requires email production (not reported in F. Supp.).

3. *Williams v. Sprint/United Mgmt. Co*., 2006 WL 1867478 (D. Kan. 2006)
   A case establishing the need to include metadata in evidence production.

4. *Treppel v. Biovail Corp*., 233 F.R.D. 363 (S.D.N.Y. 2006)
   In this defamation case, the plaintiff moved to compel the defendant to take three actions based on electronically stored information:

   a. Preserve any paper and electronic data that could be considered discoverable

   b. Disclose in detail their document and data management policies by way of a list of questions provided by the plaintiff

   c. Produce all of the accessible and responsive data from the plaintiff's earlier request for production

5. *Rule 37 Federal Rules of Civil Procedure: Failure to make disclosure or cooperate in discovery*. Requires the preservation of electronically stored data. Also provides protection for the good-faith loss of electronically stored information, and for sanctions if parties are negligent in data retention.

USEFUL CHECKLISTS FOR E-DISCOVERY

Checklists are a great tool for e-discovery. The following pages include these checklists:

1. *General Company Retention Policies (prior to litigation)*
2. *Preservation Duty in Anticipation of Litigation*
3. *The Preservation Plan*
4. *Early Recognition of Electronic Discovery Issues*
5. *Making Electronic Discovery Requests*
6. *Responding to Electronic Discovery Requests*
7. *Litigation Hold for Responding Party*
8. *Media Evaluation Exhibit*
9. *Analysis of Electronically Stored Information*

1. *Checklist: General Company Retention Policies (prior to litigation)*

- ☐ Create reasonable document storage retention policy that allows for ongoing legitimate business activity.
- ☐ Develop company-wide policies for home computer use.
- ☐ Establish policies concerning retirement of old computer systems and programs, ensuring ability to access and read old computer data (often called "legacy" data).
- ☐ Maintain written company policies regarding access to employees' computer systems and email and notify employees of their limited expectation of privacy.

---

2. *Checklist: Preservation Duty in Anticipation of Litigation*

- ☐ Learn client's computer environment and information available on client's computers to determine what to preserve, what to disclose, and what to withhold from disclosing.
- ☐ Implement preservation plan upon anticipation or awareness of potential litigation.
- ☐ Client must be advised of duty to preserve relevant evidence.
- ☐ Advise client to advise employees of duty to preserve relevant evidence, including, in written notice to employees, details of litigation, scope of information to be preserved, and consequences of failure to preserve.
- ☐ Assist client in developing retention plan.

---

3. *Checklist: The Preservation Plan*

- ☐ Determine what electronically stored information is relevant to the claim or to the defense for any party in litigation.
- ☐ Implement backup procedures for storage devices.
- ☐ Disable auto delete and enable auto archive features of computer systems and applications.
- ☐ Make mirror-image copies of local hard drives. If possible, never erase a hard drive.
- ☐ Preserve "legacy" or outdated hardware and especially software to enable reading of older data.
- ☐ Provide written notice to employees of preservation obligations regarding potentially discoverable information.
- ☐ Monitor/record employee compliance with preservation procedures.
- ☐ Make an agreement on preservation procedures a part of initial opposing party communication.
- ☐ In some circumstances, a court order may be necessary.

---

4. *Checklist: Early Recognition of Electronic Discovery Issues*

- ☐ Identify relevance and sources of potential electronically stored information in possession of the client or opposing party early in litigation.
- ☐ Consider hiring a computer technician to collect, preserve, and analyze ESI (Electronically Stored Information).
- ☐ Confer with opposing counsel to avoid spoliation and establish initial expectations of electronic discovery.

- ☐ Establish a paper trail of preservation by sending a preservation letter, outlining types of evidence claimed to be relevant to claims and defenses, and demanding preservation of electronically stored evidence.

- ☐ Disclose electronically stored information that disclosing party may use to support its claims or defenses as part of disclosure obligations.

- ☐ If appropriate to the circumstances, request that the court order expedited discovery to prevent destruction of relevant evidence.

- ☐ If computer equipment necessary for ongoing business operations has been seized, consider obtaining a court order for release of that equipment once data has been obtained.

---

5. *Checklist: Making Electronic Discovery Requests*

- ☐ Consider different forms of discoverable electronic information, including hard drives, databases, other storage media, emails, software, and residual-deleted data, as well as home computers, laptops, and mobile handheld devices in which relevant information may be available.

- ☐ Determine whether creation of special program to retrieve electronic data is necessary.

- ☐ Consider formal discovery requests pertaining to opposing party's computer environment, systems, and processes, including party's record retention and destruction policies, if information was not provided in initial disclosure.

- ☐ Consider formal discovery requests for electronically stored information relied on by opponent's expert as basis of opinion.

- ☐ Determine whether on-site computer inspection is appropriate.

- ☐ Focus discovery requests by seeking relevant information from:

    - *Individual files*
    - *Individual hard drives*
    - *Computer database accessed by individual users*

☐ Determine desired format of items to be produced, which may include:

- *Electronic copies only (specifying preferred storage medium)*
- *Paper copies only*
- *Electronic and paper copies*

---

6. *Checklist: Responding to Electronic Discovery Requests*

☐ When objecting, determine whether objection is based on:

- *Relevancy*
- *Undue expense or burden*
- *Privilege such as attorney-client communications*
- *Attorney work product*
- *Assertion that request seeks cumulative or duplicative materials*
- *Assertion that alternative, more convenient, means to obtain information is available*

☐ Review electronically stored information being disclosed by your client very carefully to prevent inadvertent disclosure of privileged information.

☐ Draft confidentiality agreement with opposition, or in the alternative seek court order, to maintain privileged status of documents inadvertently disclosed.

---

7. *Checklist: Litigation Hold for Responding Party*
This checklist is designed to be used once a party has been served with *Requests for Production* that include E-Discovery requests or a demand for a litigation hold.

☐ Have a Tech Team in place.

☐ If your client is initiating E-Discovery, the Tech Team should have templates of letters to be completed and then sent to the opposing party regarding the preservation of evidence. The letter (sent to the attorney, actually) must identify the individuals involved, issues relevant to the litigation, and a statement that failure to comply may result in sanctions.

- ☐ Workstations that are relevant to the litigation should be unplugged and stored safely. One solution is to replicate the hard drive using software (such as *Norton Ghost*) and install that replica on a new workstation computer. But lock up the original. That original hard drive becomes the secured media. The replicated drive is for use by the responding party.

- ☐ Do not defragment a drive, delete data, or add new programs. Doing so will overwrite existing data and metadata.

- ☐ Warn the client that even looking at the files on a computer/hard drive can be damaging. Replicate the drives, then look at the replicas. Do not search for and review evidence now. Instead, *preserve it*.

- ☐ Get a sense of the back-up system used by the client. Meet with the client's IT team to determine how best to maintain the data already on the back-up, and to prevent regularly scheduled data destruction. Impress on the client, and the client's IT team, the importance of retention.

- ☐ Consider taking back-up storage media out of the loop to preserve data that may exist on those devices.

- ☐ Consider other sources of data, such as iPhones, iPads or tablets, voice mail systems, laptop computers, and back-up drives or external media. Depending on the matter being litigated, these may need to be a part of the hold.

- ☐ The litigation hold may mean altering the client's data retention policy.

- ☐ The Tech Team should have templates of letters to be sent to key individuals (from managers to partners to secretaries) who may have relevant data to the litigation. These letters need to spell out what is required of them in terms of protecting data and the often-dire consequences of not doing so. The result of spoliation may be heavy fines, sanctions on the use of evidence or testimony, cost shifting or an "adverse inference" instruction to the jury.

8. *Checklist: Media Evaluation Exhibit*
Following is an example of an exhibit to attach to discovery requests, outlining procedures for securing electronic data stored on media devices. (Note that this checklist is also useful for responding parties if no such list is provided by opposing counsel.)

Exhibit A
Requested of media devices included in attached *Request for Production*:

a. Responding party shall record each device with a unique identifying number.
b. The responding party shall "write protect" each media device.
c. The responding party shall forensically duplicate each media device to create a true mirror image (note this does not mean copying or "Ghosting"). The requesting party requests documentation of any such forensic procedure.
d. The responding party shall mathematically verify and validate that the mirror image is identical to the original by using hashing algorithms (MD5, SHA1, SHA2).
e. The responding party shall scan media devices for viruses and spyware-documenting the results.
f. The responding party shall produce directory structure for devices.
g. The responding party shall analyze media; extract relevant data.
h. The responding party is responsible for securing each media device, both original and replica, so that such devices may be available to resolve any disputes or inconsistencies in resulting data.

---

9. *Checklist: Analysis of Electronically Stored Information*

☐ Check for duplicate information, especially regarding emails, and compare to determine if information has been altered.

☐ Utilize software designed for "data searching," in consultation with computer technician, to search visible and hidden files on a hard drive/storage media.

☐ Search for potentially helpful embedded information or metadata, (which may also help with verifying authenticity and spoliation issues) such as:
- Identity of file's author; date of file's creation, modification, or deletion
- Blind copies of email, as well as names on distribution lists
- Hidden formulas in excel documents and spreadsheets

☐ Search for deleted files that still may be available in the computer's free space.