MINT LEGAL
SOLUTIONS LLC

E-Discovery 101

Defined

Discovery- the process of identifying, preserving, collecting, reviewing, analyzing and producing information during civil and criminal legal actions. The goal of discovery is to obtain information that will be useful in developing relevant information for pre-trial motions and for the trial itself. Information sought during discovery can include documents, testimony and other information that may be deemed necessary by a court, although not all discovery is court-imposed.

E-Discovery- the extension of the discovery process to information that is stored electronically, including email, instant messages, word processing files, spreadsheets, social networking content, and any other electronic information that may be stored on desktops, laptops, file servers, mainframes, smartphones, employees' home computers or on a variety of other platforms.

Other Uses

Organizations can also use e-discovery tools outside the context of just civil litigation. These uses include, but are not limited to, helping to manage and avoid employee misbehavior and legal actions; helping an organization to comply with its regulatory obligations; preserving intellectual property, knowledge and other data; storage management; and avoiding embarrassing data loss or leaks.

Why is it important?

- Electronic content is growing by leaps and bounds.
- This means higher costs: storage, processing, reviewing.
- These costs are pushed on to the litigants.
- Types of data is also changing- i.e. social media sites, texts, etc.

The EDRM

- Electronic Discovery Reference Model
- Collaboration between various organizations to create guidelines and best practices in an unregulated field
- Covers 8 sections to manage e-discovery efforts:
  - Identification
  - Preservation
  - Collection
  - Processing
  - Review
  - Analysis
  - Production
  - Presentation

EDRM- Identification

Understand the "inventory" of ESI that might be relevant in a particular legal action and that might have to be presented during discovery. At this point in the process, discovery demands, disclosure obligations and other pertinent claims and demands are reviewed and considered. The goal at this stage of the process is to understand the universe of information that might be required in order to respond to appropriate ediscovery requests and then determine the subset of information that will be relevant for further processing.

EDRM- Preservation

This is a critical step that ensures that ESI is protected from spoliation and modification, such as through the imposition and enforcement of a legal hold on all relevant ESI. If spoliation does occur, the consequences can be expensive. And lately there have been a boatload of cases on the need for preservation … and the resulting sanctions for “bad” preservation.

EDRM- Collection

During this phase, all relevant ESI is collected from the various sources that contain it, including messaging archives, backup tapes, file servers, desktops, laptops, employees' home computers, smartphones and other sources.

EDRM- Processing

At this point, collected data should be de-duplicated in order to reduce the amount of data that must be processed during subsequent phases of the discovery process. Collected data should also be prioritized into a) that content that will likely be relevant later in the process and b) content that will likely not be relevant. At this point, decision makers may want to convert ESI into a form that will permit the most efficient and thorough review of its contents.

EDRM- Review

Where the contract attorneys come in. The review phase includes redacting ESI as appropriate, evaluating the content for its relevance, determining if specific items are subject to attorney-client privilege, etc.

EDRM- Analysis

This phase involves a variety of activities, including determining exactly what the ESI means in the context of the legal action at hand, developing summaries of relevant information, determining the key issues on which to focus, etc.

EDRM- Production

The production of data involves delivering the relevant ESI to any parties or systems that will need it. It also includes the activities focused on delivering ESI in the appropriate form(s), including DVDs, CD-ROMs, paper, etc.

EDRM- Presentation

The presentation of ESI is a key consideration at various points of the e-discovery process – as information is reviewed, analyzed, produced, etc. The specific forms of presentation for ESI will vary widely depending on the content; how, where and by whom the content will be presented; and other factors.

FRCP

Federal Rules of Civil Procedure govern the court procedures for managing discovery, including e-discovery.

- 2006 Amendments - primarily focused on the changes in how discovery is performed on ESI and intended to provide courts and litigants needed guidance on how to meet the new challenges.
- 2015 amendments- primarily focused on streamlining discovery and reducing the risk of sanctions (imposes new liabilities/responsibilities on counsel and clients)

ESI- Characteristics

- ESI- Electronically stored information
- ESI is normally stored in much greater volume than are hard copy documents.
- ESI is dynamic, in many cases modified simply by turning a computer on and off.
- ESI can be incomprehensible when separated from the systems that created it.
- ESI contains non-apparent information, or metadata, that describes the context of the information and provides other useful and important information.

FRE Correlation

The Federal Rules of Evidence (FRE), determine how evidence is presented during trial in the US federal courts. It is important to note that for purposes of presenting evidence, a printed or otherwise human-readable version of electronic evidence is considered to be an original and can be presented at trial according to FRE Rule 1001(3).

Authentication is a very important part of the e-discovery process because its goal is to prove that a document is what its presenter claims it to be – a true and verifiable representation of an electronic document. Authentication for electronic content is even more critical than for paper-based documents, since electronic documents are more easily altered. Therefore, in order to prove the authenticity of a particular electronic document, such as an email, those submitting this evidence must provide affidavits or otherwise demonstrate that an original document was not modified after the fact.

Data Outside US

- Numerous challenges in collecting data that is not located/originated in the US
- Many countries have far more stringent standards for privacy
- A party seeking to process personal data for litigation must take numerous steps to protect personal information

Conclusion

- Due to the growing volume of data there is an emphasis on maximizing efficiency/reducing costs
- Data preservation/collection must be carefully structured and documented in order to prevent sanctions
- Numerous issues arise with cross-border discovery- should employ local counsel