The Practical Application of Federal Rule of Civil Procedure 26(f)

Designed to provide both a general overview of Federal Rule of Civil Procedure 26(f) and planning considerations for the practical application of "Meet and Confer" requirements, "Considering Meet and Confer" contains notes, articles and references to help educate and support legal and information technology professionals as they consider "Meet and Confer".

Considering Meet and Confer

Developed by Orange Legal Technologies, Providers of the OneO® Discovery Platform.

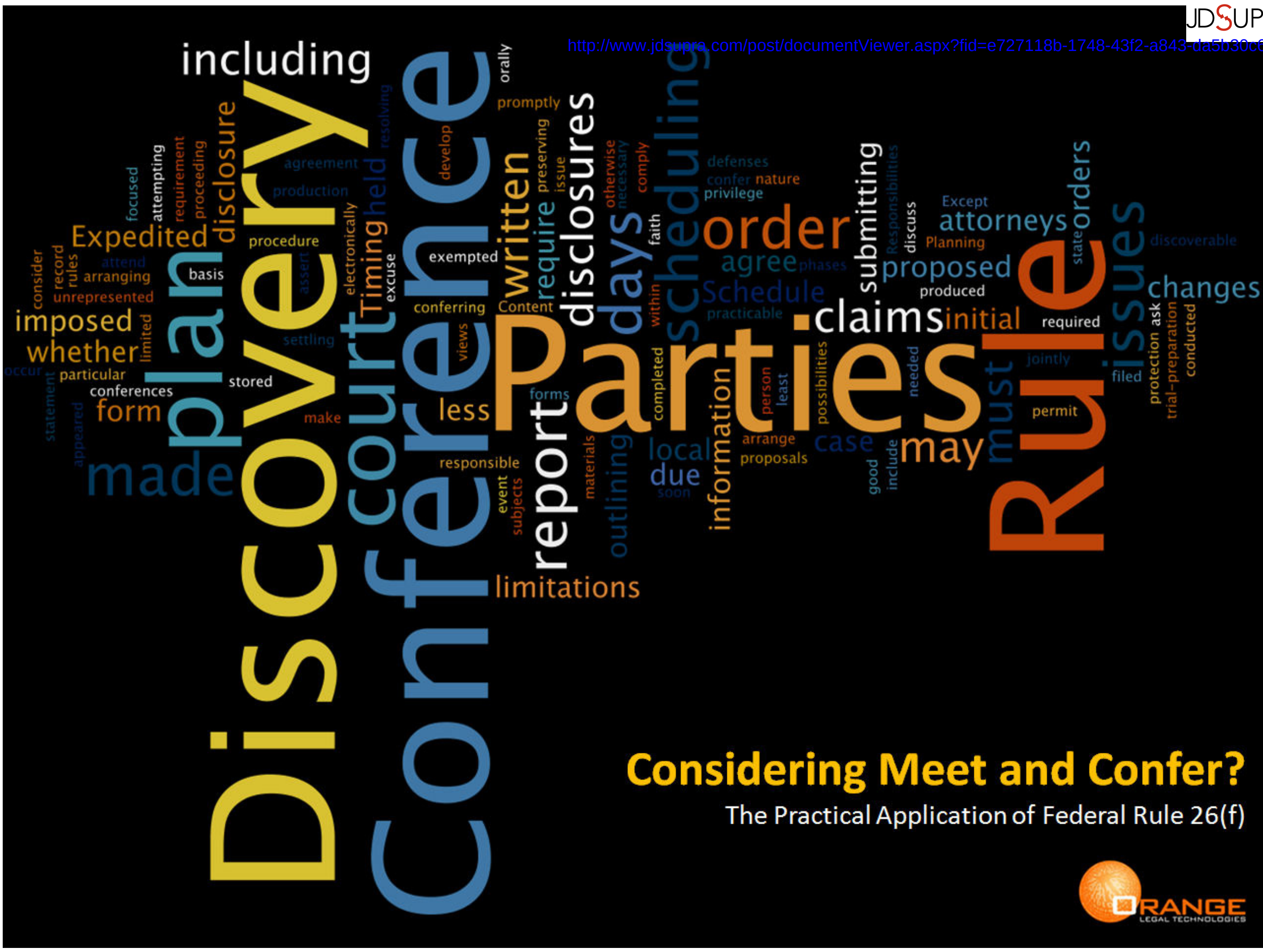


Table of Contents

Designed to provide both a general overview of Federal Rule 26(f) and planning considerations for the practical application of "Meet and Confer" requirements, this document contains notes, articles and references to help support and educate legal professionals as they consider "Meet and Confer".

Considering Meet and Confer

meet and confer n. a requirement of courts that before certain types of motions and/or petitions will be heard by the judge, the lawyers (and sometimes their clients) must "meet and confer" to try to resolve the matter or at least determine the points of conflict. This has the beneficial effect of resolving many matters, reducing the time for arguments, and making the lawyers and clients face up to the realities of their positions. On the other hand, it also can be a total waste of time for the parties and their attorneys.

Law.com

General Definition of Meet and Confer[1]

Definition: meet and confer n. a requirement of courts that before certain types of motions and/or petitions will be heard by the judge, the lawyers (and sometimes their clients) must "meet and confer" to try to resolve the matter or at least determine the points of conflict. This has the beneficial effect of resolving many matters, reducing the time for arguments, and making the lawyers and clients face up to the realities of their positions. On the other hand, it also can be a total waste of time for the parties and their attorneys.

Meet and Confer Characteristics

- Defining in Approach
- Collaborative in Nature
- Preparation Intensive
- Binding in Agreement

Key Points from General Definition

- Requirement
- Pre-Motion/Petition
- Meet to Determine and/Resolve Points of Conflict
- Objective of Accelerating Judicial Process

Meet and Confer and Electronic Discovery[2]

The meet-and-confer process is designed to allow both parties an opportunity to reach agreement on important issues about discovery early in the discovery process. The new federal rules, set to go into effect Dec. 1, 2006, require that 21 days before a Rule 16(b) scheduling conference, the parties are to meet and confer to discuss discovery. In this meeting, they must develop a plan for the preservation of data, documents and other evidence that may be important to discovery.

The meet and confer is evolving into a collaborative, rather than combative, approach to discovery in which both sides work together to limit the costs and headaches of electronic discovery. A thorough understanding of client systems can help facilitate this, as can an understanding of the challenges production of electronic data poses (including privilege waiver, form and/or format of data, accessing backed-up data and so forth).

It's often prudent to have a forensic expert or EDD consultant on hand to ascertain that any agreements are both feasible and appropriate. For example, specifying that "all deleted files" must be recovered for discovery may seem a straightforward order, but this sort of overly broad directive can lead to escalating EDD costs. It's better to have an expert available to guide the process and offer appropriate, cost-effective strategies and solutions.

Meet and Confer Drivers in Relation to eDiscovery

Federal Rules of Civil Procedure – Rule 16[3]

- Rule 16(b) - parties must "meet and confer" at least 21 days before the scheduling conference which, in turn, must occur within 120 days of filing a lawsuit.
- Rule 16(b) - scheduling order must include "provisions for disclosure or discovery of electronically stored information (ESI).

Federal Rule of Civil Procedure – Rule 26[4]

(Discussion from *Rule 26 and Other Amendment to the Federal Rules of Civil Procedured* used en total with permission of Iron Mountain)

- Rule 26(a) - explicitly defines ESI as discoverable.

The new Rule 26(a) explicitly defines ESI as a specific category of information to be disclosed. There is no longer any ambiguity about whether digital data constitutes a "document." Businesses now have a clear responsibility to produce eRecords. These amendments also permit the requesting party to request that ESI be produced in specific formats. The responding party can object to the request, but the parties must first meet and confer in an attempt to resolve the disagreement before a motion to compel can be filed. If need be, the court may order the form of production.

---

1 Law.com Dictionary - http://dictionary.law.com/default2.asp?selected=1235&bold=||||
2 Law.com Technology Roadmap - http://www.law.com/jsp/legaltechnology/roadmapArticle.jsp?id=1158014995208&hubpage=Preservation
3 eDiscovery 2.0 - http://www.clearwellsystems.com/e-discovery-blog/tag/rule-26/
4 Rule 26 and Other Amendments to the Federal Rules of Civil Procedure - http://www.ironmountain.com/resources/crm/Rule26_WP_Web.pdf

Companies therefore need to know exactly what formats their ESI is stored in, what metadata is associated with them, and what formats they can reasonably be converted into.

- Rule 26(f) - mandates early meet-and-confer sessions specifically to resolve eDiscovery issues.

Among the most important of the newly amended FRCP for businesses is Rule 26(f), which requires parties to meet within 120 days of the filing of litigation, and at least twenty-one days prior to the scheduling conference, specifically to discuss eDiscovery issues. The purpose of this Rule is to avoid loss of ESI and ensure its usability and timely production by resolving concerns up-front. During these sessions, parties must make every effort to reach agreement on logistical issues, including relevant repositories and classes of information, production formats, and matters of privilege. Companies must promptly identify all sources of ESI in their initial disclosures, meaning not only e-mail servers and backup tapes, but also deleted data, data on systems no longer in use, and data in remote or third-party locations. All of this data must be identified up-front if the data will be used in claims or defenses. A report must then be provided to the court, pursuant to a scheduling order.

Your ability to know and describe your system capabilities so your attorneys can negotiate reasonable time schedules and limits for production volume will be critical. Organizations that lack a comprehensive map of potentially relevant records will be at a major disadvantage from the outset, playing catch-up just when they should be doing serious analysis of the case. Conversely, businesses that can produce accurate inventories of electronic data repositories can save themselves millions of dollars in eDiscovery and settlement costs, and possibly even sway the outcome of the proceedings.

Rule 26(f) also demands that parties give early attention to data preservation. Providers risk claims of spoliation of evidence if litigation holds are not instituted quickly and efficiently since production requirements will be known up-front. On the other hand, the ability to agree during meet-and-confer sessions on what must be preserved versus what can be disposed of per standard retention policies can save companies money and protect against subsequent spoliation claims.

- Rule 26(b)(5) – addresses inadvertent production of privileged information during eDiscovery.

The greater the volume of ESI produced in a lawsuit, the greater the likelihood that privileged information, such as trade secrets or financial information, may be inadvertently produced. The traditional ability to inspect all data and filter out privileged information is simply not possible given the staggering quantity and variety of ESI that can be involved in large, complex litigations. For example, it is estimated that the average gigabyte of e-mail contains 100,000 printed pages of information, as compared to 3,000 pages for the average box of printed records. Hundreds of thousands of pages of ESI are now the norm in bigger cases.

Rule 26(b)(5) includes a new section covering the accidental production of privileged information. It permits organizations to retract ("clawback") privileged information following its discovery. Potential concerns regarding privilege are to be discussed during meet-and-confer sessions as part of the discovery plan. If information deemed privileged is produced, the producing party can notify the recipient of this assertion and the basis for it. The requesting party must return, sequester, or destroy the information promptly, and is barred from disclosing it until the claim is resolved. Further, if the recipient has already disclosed the privileged information prior to notification, it must take reasonable steps to retrieve it. In any event, the producing party must preserve the privileged information until the litigation is resolved. Recipients can naturally dispute claims of privilege by submitting the information to the court for a ruling. The producer must make responsible attempts to avoid such disclosures—sloppy production is not an excuse and may imply a waiver of privilege. Moreover, producers must assert claims of privilege within a "reasonable time," again requiring a handle on the data. Courts will weigh these factors in determining whether to waive or forfeit a claim of privilege.

- Rule 26(b)(2) - provides guidance regarding claims that ESI is unduly burdensome to produce.

In acknowledging that some information may be overwhelmingly difficult to retrieve (e.g., because the hardware/software required to restore it is obsolete, or the media it resides on is damaged), this rule specifies that a party need not produce ESI s it regards as "not reasonably accessible because of undue burden or cost." If, following meet-and-confer sessions, a claim of reasonable inaccessibility remains unresolved, the requesting party can introduce a motion to compel production to dispute the assertion. Likewise, the responding party can seek a protective order from the court barring production. In either case, however, the burden is on the responding party to prove that the information is not reasonably accessible. Further, if the requestor can demonstrate that there is just cause showing that the evidence should be produced, the court may then order its production. When might ESI be deemed reasonably inaccessible?

A range of factors will be involved, including:

- The burden or expenses of producing outweighs the likely benefit or relevance of the data.
- The request is unduly cumulative or duplicative.
- The quantity of data involved
- A party's inability to obtain the same or equivalent information from more accessible sources.
- The magnitude of the issues at stake in the litigation.
- The resources of the parties involved.

Federal Rule of Civil Procedure - Rule 34

- Rule 34(a) – addresses the scope of ESI to include information type and location.
- Rule 34 (b) – addresses and provides guidance concerning the production of ESI.

Key Points on Meet and Confer Drivers[5]

- FRCP developed in 1938. The U.S. Federal Rules of Civil Procedure (FRCP) define procedures for U.S.-based litigation. They date from 1938 but recently have been updated to deal with electronic documents. Email is by far the most important of such documents.
- FRCP currently comprised of 86 rules.
- FRCP Amendments on December 1, 2006 address ESI requirements.
- FRCP Rule 26(f) is the "center of gravity" for Meet and Confer. Rule 26(f)--the Meet and Confer rule--requires the parties in litigation to meet at an early stage to discuss the information they have and what they will share. Thus, when a subpoena arrives, organizations frequently must launch a highly disruptive emergency response project.

5 Ferris Research, http://www.ferris.com/?p=318586

Key Points in Relation to ESI - Form 35[1]

- Standardizes discovery agreements.
- Designed to avoid delays centered on discovery.
- Provides reminder/documentation of requirement to address ESI (Rule 26(f)).

Example Form 35. Report of Parties' Planning Meeting

[Caption and Names of Parties]

1. Pursuant to Fed. R. Civ. P. 26(f), a meeting was held on ____(date)____ at ____(place)____ and was attended by:

____(name)____ for plaintiff(s)

____(name)____ for defendant(s) ____(party name)____

2. Pre-Discovery Disclosures. The parties [have exchanged] [will exchange by ____(date)____] the information required by [Fed. R. Civ. P. 26(a)(1)] [local rule ____].

3. Discovery Plan. The parties jointly propose to the court the following discovery plan: [Use separate paragraphs or subparagraphs as necessary if parties disagree.]

Discovery will be needed on the following subjects: ____(brief description of subjects on which discovery will be needed).

All discovery commenced in time to be completed by ____(date)____. [Discovery on ____(issue for early discovery)____ to be completed by ____(date)____.)

Maximum of ____ interrogatories by each party to any other party. [Responses due ____ days after service.]

Maximum of ____ requests for admission by each party to any other party. [Responses due ____ days after service.]

Maximum of ____ depositions by plaintiff(s) and ____ by defendant(s).

Each deposition [other than of ________] limited to maximum of ____ hours unless extended by agreement of parties.

Reports from retained experts under Rule 26(a)(2) due: from plaintiff(s) by ____(date)____ from defendant(s) by ____(date)____.

Supplementations under Rule 26(e) due ____(time(s) or interval(s))____.

4. Other Items. [Use separate paragraphs or subparagraphs as necessary if parties disagree.]

The parties [request] [do not request] a conference with the court before entry of the scheduling order. The parties request a pretrial conference in __(month and year)__.

Plaintiff(s) should be allowed until ____(date)____ to join additional parties and until ____(date)____ to amend the pleadings.

Defendant(s) should be allowed until ____(date)____ to join additional parties and until ____(date)____ to amend the pleadings.

All potentially dispositive motions should be filed by ____(date)____.

Settlement [is likely] [is unlikely] [cannot be evaluated prior to ____(date)____] [may be enhanced by use of the following alternative dispute resolution procedure: ________________].

Final lists of witnesses and exhibits under Rule 26(a)(3) should be due from plaintiff(s) by ____(date)____ from defendant(s) by ____(date)____.

Parties should have ____ days after service of final lists of witnesses and exhibits to list objections under Rule 26(a)(3).

The case should be ready for trial by ____(date)____ [and at this time is expected to take approximately ____(length of time)____].

[Other matters.]

Date: ____________

1 Fios Case Law & Rules: Federal Rules of Civil Procedure - http://tinyurl.com/cyombw

Meet and Confer Planning Checklist[1]

(Content from *Prepare for an Effective Meet and Confer* by Linda Kish, Kroll Consultant - used en total with permission of Kroll Ontrack)

To help ensure that all potential topics that may addressed during the Meet and Confer Conference are considered during pre-conference planning, it is recommended that firms develop an internal planning checklist to guide them in their Meet and Confer planning. Key considerations for this checklist include:

1. Preservation Practices
2. Scope of Discovery
3. Accessibility
4. Production of Metadata
5. Costs & Burdens
6. Forms of Production
7. Privilege Issues & Waiver
8. Variations from FRCP Rules
9. Inventory of Opponent's IT Infrastructure
10. Other Info that may be Important to eDiscovery

Additional details on the questions associated with these considerations are as follows:

1. Preservation Practices

- What is being done to preserve ESI?
- Is a protective order necessary?

2. Scope of Discovery

- Will there be any deviations from the default initial disclosures specified in Rule 26(a)?
- What file types and time range is the opposing party seeking?
- Who are the main data custodians the opposing party is interested in?
- What will be the timing for exchanging discoverable ESI?

3. Accessibility

- What type of data is the opposing party interested in?
- (Backup tapes? Hard drives? Servers? Removable media? Deleted data?)
- How easy will it be to access this data?
- Will the use of an e-evidence expert be necessary?

4. Production of Metadata

What fields will be exchanged for the various file formats?

5. Costs & Burdens

Who will bear the costs associated with gathering, restoring, and producing the ESI?

6. Forms of Production

In what format or formats will parties produce the ESI be?

7. Privilege Issues & Waiver

How will parties handle inadvertently produced privileged documents?

8. Variations from FRCP Rules

Are there any local rules that apply in the jurisdiction?

---

1 Kroll Ontrack, Prepare for an Effective Meet and Confer (Linda Kish, Esq. Kroll) http://www.krollontrack.com

9. Inventory of opponent's IT Infrastructure

- Which operating systems and software packages were used to develop key data?
- Are those systems still in use?
- What are the opponent's document retention policies? Are they being enforced?

10. Other

Is there any other information that may be important to the e-discovery activity in the case?

Meet and Confer – Dictionary

Need Agreed Upon ESI "Vocabulary"

- To ensure a common understanding of ESI Terms.
- To serve as a reference point for clarification of ESI definition issues.
- To simplify and accelerate discussion during the 26(f) Meet and Confer Conference.

Potential References for ESI Terms

- American Document Management Glossary of Terms @ http://www.amdoc.com/glossary.php
- EDRM Glossary @ http://www.edrm.net/wiki/index.php/Glossary
- The Sedona Conference Glossary @ http://www.thesedonaconference.org/content/miscFiles/TSCGlossary_12_07.pdf


Experts
Estimation
Examination
Elements

Understanding ESI

While not specifically defined in the FRCP, electronically stored information, or ESI, is defined in the November 2006 issue of The Third Branch (Newsletter of the Federal Courts) simply as ”…all information in computers”.

Understanding Electronically Stored Information – The Elements of ESI[1]

What is Electronically Stored Information?

While not specifically defined in the FRCP, electronically stored information, or ESI, is defined in the November 2006 issue of The Third Branch (Newsletter of the Federal Courts) simply as "…all information in computers".

What is Information?

From a technology perspective, information is defined as the summarization of data. Technically, data are raw facts and figures that are processed into information, such as summaries and totals. But since information can also be the raw data for the next job or person, the two terms cannot be precisely defined, and both are used interchangeably.

What Is Data?

- Factual information, especially information organized for analysis or used to reason or make decisions.
- Computer Science. Numerical or other information represented in form suitable for processing by computer.

Data Scope (What is the scope of the data in question?)

- *Entity Scope* - Entities that may have had individuals involved in the creation, review, and/or response of data that may contain relevant information for the matter at hand.
- *Custodian Scope* - Individuals who may have been involved in the creation, review, and/or response of data that may contain relevant information for the matter at hand.
- *Data Steward Scope* - Individuals who have Information Technology management responsibilities for the entities and individuals determined to be relevant to the matter at hand and/or individuals who maintain access rights to the applications and equipment used by these entities and organizations.
- *Geographical Scope* - The geographical locales of the entities and individuals that may have been involved in the creation, review, and/or response of communications and/or documents relevant to the matter at hand as well as the locales of the equipment used to support creation, transmission, review, and storage of these communications and/or documents.
- *Time Frame Scope* - The period of time in which relevant information may have been created, reviewed, and/or responded to for the matter at hand.
- *Volume Scope* - The estimated volume of data that may contain relevant information for the matter at hand.

Data Structure (What is the structure of the data?)

- *Unstructured* - Unstructured data (or unstructured information) refers to masses of (usually) computerized information in which every bit of information does not have an assigned format and significance. Examples of "unstructured data" may include audio, video and unstructured text such as the body of an email or word processor document. Unstructured data represents approximately 85% of enterprise data.
- *Structured* - Structured data (or structured information) refers to masses of (usually) computerized information in which every bit of information has an assigned format and significance. Examples of "structured data" may include databases such as SQL or Access. Structured data represents approximately 15% of enterprise data.

Data Format (What is the format of the data?)

- *Still Image* - Images that convey their meaning in visual terms, e.g. pictorial images, photographs, posters, graphs, diagrams, documentary architectural drawings. Formats for such images may be bitmapped (sometimes called raster), vector, or some combination of the two. A bitmapped image is an array of dots (usually called pixels, from picture elements, when referring to screen display), the type of image produced by a digital camera or a scanner. Vector images are made up of scalable objects—lines, curves, and shapes—defined in mathematical terms, often with typographic insertions.
- *Sound* - Media-independent sound content that can be broken into two format sub-categories. The first sub-category consists of formats that represent recorded sound, often called waveform sound. Such formats are employed for applications like popular music recordings, recorded books, and digital oral histories. The second sub-category consists of formats that provide data to support dynamic construction of sound through combinations of software and hardware. Such software includes sequencers and trackers that use data that controls when individual sound elements should start and stop, attributes such as volume and pitch, and other effects that should be applied to the sound elements. The sound elements may be short sections of waveform sound (sometimes called samples or loops) or data elements that characterize a sound so that a synthesizer (which may be in software or

1 Orange Legal Technologies: http://orangelt.us/services/collection-services/

hardware) or sound generator (usually hardware) can produce the actual sound. The data are brought together when the file is played, i.e., the sounds are generated in a dynamic manner at runtime. This second sub-category is sometimes called structured audio.

- *Moving Image* - A variety of media-independent digital moving image formats and their implementations. Some formats, e.g., QuickTime and MPEG-4, allow for a very wide range of implementations compared to, say, MPEG-2, an encoding format whose possible implementations are relatively more constrained.
- *Textual* - Content works consisting primarily of text.
- *Web Archive* - Content in formats that might hold the results of a crawl of a Web site or set of Web sites, a dynamic action resulting from the use of a software package that calls up Web pages and captures them in the form disseminated to users.
- *Generic* - Content in widely acceptable generic formats to include but not limited to specifications for wrappers (e.g., RIFF and ISO_BMFF), bundling formats (e.g., METS and AES-31), and encodings (e.g., UTF-8 and IEEE 754 1985).

Data State (What is the state of the data?)

- *Active State* - Active Data is information residing on the hard drives or optical drives of computer systems, that is readily visible to the operating system and/or application software with which it was created and is immediately accessible to users without deletion, modification or reconstruction.
- *Static State* - Static Data (or Archival Data) is information that is not directly accessible to the user of a computer system but that the organization maintains for long-term storage and record keeping purposes.

Static data may be written to removable media such as a CD, magneto-optical media, tape or other electronic storage device, or may be maintained on system hard drives in compressed formats.

- *Residual State*: Residual Data (sometimes referred to as "Ambient Data") refers to data that is not active on a computer system. Residual data includes (1) data found on media free space; (2) data found in file slack space; and (3) data within files that has functionally been deleted in that it is not visible using the application with which the file was created, without use of undelete or special data recovery techniques.

Data Network (How does one "Connect" to the data?)

- *Non-Networked*: Data is not interconnected to a group of computers.
- *Personal Area Network (PAN)*: A personal area network (PAN) is a computer network used for communication among computer devices close to one person. Some examples of devices that may be used in a PAN are printers, fax machines, telephones, PDAs, or scanners. The reach of a PAN is typically within about 20-30 feet (approximately 4-6 Meters). PANs can be used for communication among the individual devices (intrapersonal communication), or for connecting to a higher level network and the Internet (an uplink).
- *Local Area Network (LAN)*: A network covering a small geographic area, like a home, office, or building. Current LANs are most likely to be based on Ethernet technology.
- *Campus Area Network (CAN)*: A network that connects two or more LANs but that is limited to a specific and contiguous geographical area such as a college campus, industrial complex, or a military base. A CAN, may be considered a type of MAN (metropolitan area network), but is generally limited to an area that is smaller than a typical MAN.
- *Metro Area Network (MAN)*: A Metropolitan Area Network is a network that connects two or more Local Area Networks or Campus Area Networks together but does not extend beyond the boundaries of the immediate town, city, or metropolitan area. Multiple routers, switches & hubs are connected to create a MAN.
- *Wide Area Network (WAN)*: A WAN is a data communications network that covers a relatively broad geographic area (i.e. one city to another and one country to another country) and that often uses transmission facilities provided by common carriers, such as telephone companies.
- *InterNetwork:* Two or more networks or network segments connected using devices that operate at layer 3 (the 'network' layer) of the OSI Basic Reference Model, such as a router. Any interconnection among or between public, private, commercial, industrial, or governmental networks may also be defined as an internetwork. In modern practice, the interconnected networks use the Internet Protocol. There are at least three variants of internetwork, depending on who administers and who participates in them:

Intranet: An intranet is a set of interconnected networks, using the Internet Protocol and uses IP-based tools such as web browsers, that are under the control of a single administrative entity. That administrative entity closes the intranet to the rest of the world, and allows only specific users. Most commonly, an intranet is the internal network of a company or other enterprise.

Extranet: An extranet is a network or internetwork that is limited in scope to a single organization or entity which also has limited connections to the networks of one or more other usually, but not necessarily, trusted organizations or entities (e.g. a company's customers may be given access to some part of its intranet creating in this way an extranet, while at the same time the customers may not be considered 'trusted' from a security standpoint). Technically, an extranet may also be categorized as a CAN, MAN, WAN, or other type of network, although, by definition, an extranet cannot consist of a single LAN; it must have at least one connection with an external network.

"The Internet": A specific internetwork , consisting of a worldwide interconnection of governmental, academic, public, and private networks based upon the Advanced Research Projects Agency Network (ARPANET) developed by ARPA of the U.S. Department of Defense – also home to the World Wide Web (WWW) and referred to as the 'Internet' with a capital 'I' to distinguish it from other generic internetworks.

Intranets and extranets may or may not have connections to the Internet. If connected to the Internet, the intranet or extranet is normally protected from being accessed from the Internet without proper authorization. The Internet itself is not considered to be a part of the intranet or extranet, although the Internet may serve as a portal for access to portions of an extranet.

Data Storage Network (How does one get to Active State data?)

- *Direct Attached Storage (DAS)*: Direct-attached storage (DAS) refers to a digital storage system directly attached to a server or workstation, without a storage network in between. It is a retronym, mainly used to differentiate non-networked storage from SAN and NAS.
- *Network-Attached Storage (NAS):* Network Attached Storage (NAS) is a file-level computer data storage connected to a computer network providing data access to heterogeneous network clients.
- *Storage Area Network (SAN):* A storage area network (SAN) is an architecture to attach remote computer storage devices (such as disk arrays, tape libraries and optical jukeboxes) to servers in such a way that, to the operating system, the devices appear as locally attached.

Data Storage Media (How does one maintain the Static State data?)

- *Semi Conductor Based Storage Media* (Memory Cards, USB Flash Drives, PDAs, Digital Audio Players, Digital Cameras, Mobile Phones, Copiers)
- *Magnetic Based Storage Media* (Floppy Disk, Hard Disk, Magnetic Tape)
- *Optical and Magneto Optical Storage Media* (CD, CD-ROM, DVD, BD-R, BL-RE, HD DVD, CD-R, DVD-R, DVD+R, CD-RW, DVD-RW, DVD+RW, DVD-RAM, UDO)

Data Volume (How much data will be acted upon?)

- *Uncompressed* - Data not having undergone a process of transformation from one representation to another, smaller representation from which the original, or a close approximation to it, can be recovered.
- *Compressed* - Data having undergone a process of transformation from one representation to another, smaller representation from which the original, or a close approximation to it, can be recovered.

Data Encryption (Is the data encrypted?)

- *Data Not-Encrypted* - Data not having undergone a procedure that renders the contents of a computer message or file unintelligible to anyone not authorized to read it. The data is encoded mathematically with a string of characters called a data encryption key.
- *Data Encrypted* - Data having undergone a procedure that renders the contents of a computer message or file unintelligible to anyone not authorized to read it. The data is encoded mathematically with a string of characters called a data encryption key.

Data Code Format (What capabilities will be needed to display information?)

- *Unicode Support* - Unicode Support provides a unique number for every character, no matter what the platform, no matter what the program, no matter what the language.
- *Non-Unicode Support* - Data Code Format does not provide a unique number for every character regardless of platform, program, or language.

Data Output (How will data reports and/or files be provided to requestor?)

- Custom Reports (Based On Task)
- Native Files
- TIFF Files
- PDF Files
- Load Files (Specifics Provided By Requestor)
- Custom Files (Specifics Provided By Requestor)

Data Storage Requirements (How will the data be stored after being acted upon?)

- *Hot* - Data is stored in an active state and is immediately accessible to end users.
- *Warm* - Data is stored in an active state not immediately accessible to end users.
- *Cold* - Data is stored in a static state.
- *Destruct* - Data is destroyed.

As one begins to understand these collections considerations, one can then begin to assign economic values (time/money) to the potential approaches to get the data and make it available for all parties involved in a specific matter. Ranging from extremely general and subjective on one end of the spectrum to very specific and objective on the other, this economic value can also serve as the basis for discussing from a position of understanding whether or not ESI is accessible or not-reasonably-accessible from a case-specific legal perspective.

ESI Technology Focus Framework

- *Creation* - enables the creation of ESI.
- *Connectivity* - infrastructure that connects communication and storage nodes of ESI.
- *Communication* - enables the dissemination of and collaboration on ESI.
- *Conduct (Management)* – enables functional area management of ESI.

Understanding Electronically Stored Information - Examination

What are the general categories of ESI in relation to ESI examination?

- Accessible*: "Information deemed 'accessible' is stored in a readily usable format." (Zubulake v. UBS Warburg)
- Unreasonably Accessible: Information not stored in a reasonable usable format.

What are the potential preservation and production implications of accessible/non-accessible ESI?

- Accessible - Need to preserve and to produce.
- Unreasonably Accessible - Need to preserve and understand requirements for production.

What electronic media may need to be examined for ESI*?

- Active, Online Data (Typically Accessible)
- Nearline Data (Typically Accessible)
- Offline Storage/Archives (Sometimes Accessible, Sometimes Unreasonably Accessible)
- Backup Tapes (Typically Unreasonably Accessible)
- Erased, Fragmented, or Damaged Data (Typically Unreasonably Accessible)

* Continuum of Accessibility is not defined in the FRCP as it may change over time.

Additional Reading: E-Discovery - The Long and the Short of "Accessibility". Duane Morris E-Discovery Alert, John Coughlin, April 2007, http://www.duanemorris.com/alerts/alert2475.html.

Understanding Electronically Stored Information - Expert

Why the need for determining Meet and Confer eDiscovery experts?

- Allows for the selection of a primary eDiscovery advisor for the responsible attorney of record.
- Allows for the selection of an eDiscovery liaison/facilitator for coordination and communication.
- Allows for the proactive selection and training of Rule 30(b)(6) experts.

Who might be selected as an eDiscovery expert/liaison?

- Attorney (In-House or Outside Counsel)
- Third Party Consultant
- Company/Organization Employee

What are the typical characteristics of an expert eDiscovery liaison?

- Technical familiarity with party's electronic systems and capabilities.
- Technical understanding of eDiscovery.
- Familiarity with and ability to establish "chain of custody" for all ESI.
- Prepared to participate in eDiscovery dispute resolutions and litigation.

Understanding Electronically Stored Information - Estimation

- **Pages in a MB/GB e-Discovery Calculator:** This free online calculator inputs Megabytes or Gigabytes of various file types (e.g., Outlook email PSTs, Word, Excel and other native files, PDFs, TIFFs, etc.) estimates equivalent pages and boxes. This calculator is useful for calculating e-Discovery document review costs and preparing litigation budgets. http://www.lexbe.com/hp/Pages-Megabyte-Gigabyte.aspx
- **eDiscovery Cost Calculator** – Mimosa Systems: Exchange-related discovery can be extremely costly to organizations when all factors and costs are considered. Exchange-related discovery costs include the cost to find, recover and review responsive emails from network storage, the Exchange database, backup tapes and custodian workstations and removable media. Also, the largest cost for most organizations is the legal review of responsive emails. http://www.mimosasystems.com/html/ediscovery_worksheet.htm
- **JurInnov Electronic Discovery Calculator** - This tool uses broad assumptions to determine data size and project cost and is only intended to illustrate review cost savings attributable to electronic discovery services. Every electronic discovery project is different. As such, actual data sizes and costs will vary based on project needs and circumstances. Calculations exclude travel time and expenses. http://www.jurinnov.com/electronic_discovery_calculator/
- **Backup Tape Liability Management Service -** This calculator can help determine the amount of potential savings in off-site storage of tape cartridges if you implemented RenewData's Backup Tape Liability Management Service. http://www.renewdata.com/backup-tape-liability-calc.php

Understanding Electronic Discovery Tasks

The discovery of electronic data will play an increasingly critical role in most business and commercial litigation cases, and will necessarily affect the way parties conduct litigation, particularly discovery. The increasing capacity by which data may be amassed and stored electronically has the ability to turn a seemingly simple discovery request into a litigation sideshow.

Aisha Shelton Adam

Understanding Electronic Discovery Tasks - Collection [1]

What is Collection? The collection of data can be simply defined as the acquisition of potentially relevant electronically stored information (ESI) in the conduct of electronic discovery.

Key Collection Considerations:

1. What is the scope of the data in question?
2. What is the structure of the data?
3. What is the format of the data?
4. What is the state of the data?
5. How does one "Connect" to the data?
6. How does one get to Active State data?
7. How does one maintain the Static State data?
8. How much data will be acted upon?
9. Is the data encrypted?
10. What capabilities will be needed to display information?
11. How will data reports and/or files be provided to requestor?
12. How will the data be stored after being acted upon?

Understanding Electronic Discovery Tasks - Analytics

What is Analytics? Analytics in the realm of electronic discovery is the leveraging of data through the use of a particular functional process to enable context-specific insight that is actionable. [2]

Why is Analytics important?

Case preparation by senior level attorneys is the part of the electronic discovery process that begins to translate relevant electronic information into organized and prioritized evidence to support a client's legal position. With the advent of advanced search technologies, these senior legal professionals have been able to improve their efficiency in organizing evidence as they build their respective cases.

However, as the proliferation of electronic communications continues, these same professionals need even more capability to rapidly and accurately evaluate large volumes of relevant information discovered during review. With the introduction of analytics into the electronic discovery process, senior level attorneys can now move beyond advanced search in their case preparation and can begin to organize, understand, and prioritize information and information patterns to make even quicker and more efficient case decisions. This early organization, understanding, and prioritization of information also helps decrease the size of data sets that are to be fully processed, reviewed, and produced, thus decreasing costs throughout downstream processes.

What are some of the key tasks in "analysis"?

- Locating of data to be analyzed.
- Indexing of located data.
- Searching of indexed data.

What are some of the key ways in which data can be located prior to analysis?

- Automated Network Discovery Of Devices/Repositories
- Online/Inline Accessibility To Workstations, Email Servers, File Servers, and Associated Archives
- Tape Restoration (Non-Native)

Key indexing features for analyzing data include such capabilities as indexing by:

- Data Clusters
- Discussion Threads

1 Orange Legal Technologies: http://orangelt.us/services/collection-services/
2 Gartner Research Definition of Analytics adjusted for eDiscovery.

- Communication Groups
- Topic Classifications
- File Receivers

Key search features for analyzing indexed data are rapidly increasing and include searching by:

- Boolean Operators
- Concepts
- Fuzzy Logic
- Macros
- Numeric Ranges
- Phrases
- Phonics
- Proximity (And Directed Proximity)
- Stemming
- Synonym Searching
- Thesaurus Searching
- Wildcards

Understanding Electronic Discovery Tasks - Processing[3]

What is "Processing"?

In the realm of electronic discovery, "Processing" is any operation or set of operations which is performed upon data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.[4]

Why is "Processing" important?

The principal objective of electronic discovery processing is to prepare relevant files for efficient and expedient review (in most instances by attorneys), production and subsequent use while ensuring that the techniques and processes used are both defensible with respect to clients' legal obligations and appropriately cost-effective and expedient in the context of the matter.

What are the major tasks that take place in electronic discovery processing?

While there are many ways to define, describe, and organize the tasks that take place in electronic discovery processing, for the purpose of this discussion we will focus on the following nine major tasks and how they inter-relate to accomplish electronic discovery processing:

- Chain of Custody Security and Tracking
- Data Staging
- Data Filtering
- Deduplication
- Metadata Extraction
- Full Text Extraction
- Exception Handling
- Data Conversion
- Load File Production

3 Orange Legal Technologies – Processing: http://orangelt.us/services/processing-services/
4 The Sedona Conference Glossary, December 2007.

Chain of Custody Security and Tracking

Defined by The Sedona Conference as "the documentation and testimony regarding the possession, movement, handling and location of evidence from the time it is obtained to the time it is presented in court; used to prove that evidence has not been altered or tampered with in any way; necessary both to assure admissibility and probative value", Chain of Custody is the part of electronic discovery processing that ensures the evidence is authentic.

By developing, documenting, and tracking the physical media that contains electronically stored information (ESI) throughout the entire electronic discovery process can help organizations ensure their evidence is viewed as authentic. Additionally, just as physical media containing electronic documents must be treated as evidence, the same rule holds true for each individual file.

Automation of technical chain of custody activities can help in the substantiation of an exact process files go through prior to admission in a case. The benefits of automation can be even greater when the case consists of millions of files and automation ensures each file goes through the exact same process.

Data Staging

Data Staging is the process by which original ESI files are copied, isolated, and stored in a forensically sound manner for future use.

This staging typically occurs in three phases:

1. Copying and storage of original ESI files on a closed and isolated network file server.
2. Storage of original media and ESI files in a forensically sound manner.
3. Storage of copied ESI files for use in further electronic discovery processing.

Data Filtering

Data Filtering consists of the process of identifying specific data for extraction based on specific parameters. Filtering can occur at many different levels to include:

- System File Filtering: This type of filtering is designed to exclude those files known as system files from the filtering results data set.
- Data Range Filtering: This type of filtering is designed to either include or exclude prescribed date and time ranges from the filtering results data set.
- Extension Filtering: This type of filtering is designed to either include or exclude specific files based on their extension and typically includes file type validation.
- Custodian Filtering: This type of filtering is designed to either include or exclude specific custodians from the filtering results data set.
- Key Word Filtering: This type of filtering is commonly referred to as "keyword search" and is designed to filter data by prescribed keywords and/or keyword driven concepts.

Deduplication

Deduplication is the process of identifying and segregating those files that are exact duplicates of one another. The goal is to provide a deliverable that contains one copy of each original document, while maintaining the information associated with each instance of that document within the collection.

Several ways duplicates can be identified are:

- A combination of metadata information can be compared to match files.
- An electronic fingerprint of each file can be taken and compared using a mathematical hashing algorithm such as MD5 Hash, SHA-1, or SHA-180.
- In some cases, a hashing algorithm is used in combination with metadata.

In addition to deduplication, the advent near-deduplication technologies allow for an even higher level of data deduplication as identify files that are materially similar are not bit-level duplicates. These near-deduplication technologies help identify and group/tag electronic files with "near duplicate" similarities, yet some differences in terms of content or metadata, or both. Examples include document versions, emails sent to multiple custodians, different parts of email chains, or similar proposals sent to several clients.

Metadata Extraction

Metadata are used to describe data or information. Metadata can describe just about anything you find on a computer, and the term is often used to refer to information about things that aren't on the computer.

- The National Information Standards Organization (NISO) defines metadata as "structured information that describes, explains, locates, or otherwise makes it easier to retrieve, use, or manage an information resource."
- The World Wide Web Consortium (W3C) defines metadata as "machine understandable information for the web".
- The Federal Geographic Data Committee (FGDC) defines metadata as describing, "the content, quality, condition, and other characteristics of data."
- The Sedona Conference (TSC) defines metadata as "Data typically stored electronically that describes characteristics of ESI, found in different places in different forms. Can be supplied by applications, users or the file system.

Metadata can describe how, when and by whom ESI was collected, created, accessed, modified and how it is formatted. Can be altered intentionally or inadvertently. Certain metadata can be extracted when native files are processed for litigation. Some metadata, such as file dates and sizes, can easily be seen by users; other metadata can be hidden or embedded and unavailable to computer users who are not technically adept. Metadata is generally not reproduced in full form when a document is printed to paper or electronic image.

Put simply, metadata is data about data. It provides a context for data, ideally machine-readable.

Metadata is extracted and archived as part of processing the source data so that it is available during review. Although metadata may not be used during processing, it is still critical that it be maintained for purposes of electronic discovery. If not, the integrity and authenticity of the data can be questioned.

Full Text Extraction

Full text extraction consists of the automated and/or non-automated processes of retrieving text from electronic text, hard copy, and/or sound files and presenting the data in a form suitable for further eDiscovery processing.

The extraction of data from electronic files commonly takes one of several paths:

- Electronic Text To Electronic Text Via Text Extraction Engines
- Electronic Images To Electronic Text Via OCR
- Hard Copy Images To Electronic Text Via OCR
- Audio Files To Electronic Text Via Sound Extraction Engines

These electronic files typically range from e-mail (and attachments), databases, text documents, spreadsheets, text messages, instant messages, to digital voice mail messages– all of which are considered electronically stored information (ESI) and are potentially discoverable under current Federal Rules of Civil Procedure.

Exception Handling

As in any process, there are times when standard processes are not effective in completing a task.

In electronic discovery processing, the extraction of full text is no exception to this fact.

With that fact in mind, most organizations have what is commonly referred to as an "exception handling" process that allows for further, non-standard text extraction tasks and also ensures the full documentation and reporting of files that cannot be successfully processed.

Data Conversion

After electronically stored information (ESI) has been processed from the "Chain of Custody" stage to the "Full Text Extraction" Stage, the ESI is usually converted into a normalized format that allows for the review of the information by legal professionals.

Typical ESI conversions are to formats that include:

- "Tagged Image File Format" or TIFF: An electronic copy of a document in the form of an image, and as such contains no embedded text, fonts, images, or graphics. TIFFs do not retain metadata from a source electronic document.
- "Portable Document Format" or PDF: Developed by Adobe Systems, Inc., 'PDF' is the de facto standard for the exchange of electronic documents. PDF preserves the fonts, images, graphics, and layout of any source document, regardless of how the original document was created. PDF files can be shared, viewed, and

printed with Acrobat, a viewer application available free from Adobe Systems. Documents can be converted to PDF using software products created by Adobe and others. Depending on how they are created, PDFs can also be searchable PDF, either by retaining text from the source document or by having a source image file converted by OCR. Depending on capture methodology, PDFs may retain some metadata.

Additionally, there are times when legal professionals chose not convert ESI into TIFF or PDF formats. In those situations they may chose ultimately review ESI in its original format – commonly referred to as a Native Format or Native File. Simply defined, a Native File is an electronic document produced as it was originally maintained and used.

Load File Production

In the last phase of electronic discovery processing, data is exported to a desired review tool format through the production of Load Files. Defined by The Sedona Conference as "a file that relates to a set of scanned images and indicates where individual pages belong together as documents", a load file may also contain data relevant to the individual documents, such as metadata and coding data. To ensure usability by reviewers, load files must be obtained and provided in prearranged formats to ensure transfer of accurate and usable images and data.

When the reviewer's opt to use TIFF or PDF formats, two load files are typically generated. The first load file contains a record entry for each document and its associated metadata as well as parent-child relationships. A second load file is also generated and it links all TIFFs or PDFs to each record in the first load file. These two load files are then delivered, along with all of the associated TIFF or PDF files, to the reviewers so that the files can be imported into a selected review application.

If the review involves native files, then the export process will generate a single load file that contains a record entry for every native file and all of its associated metadata. The load file also contains document relationships such as parent-child and a link to the native file itself. Next, the native files are gathered and built into a structure that is compatible with the load file generated so that when the native file link is selected during review, the proper native file appears.

Why is "Processing" important? Reprise

As stated earlier, the principal objective of electronic discovery processing is to prepare relevant files for efficient and expedient review (in most instances by attorneys), production and subsequent use. Through this overview of electronic discovery processing, the hope is that you will have enough information to ask the right questions and to evaluate the presented process tasks so as to ensure that the techniques and processes used in your specific electronic discovery matters are defensible with respect to clients' legal obligations as well as appropriately cost-effective/expedient in the context of the matter.

Understanding Electronic Discovery Tasks - Review[5]

What is "Review"?

In the realm of electronic discovery, "Review" can be defined as the culling process that produces a dataset of potentially responsive documents that are then examined and evaluated for a final selection of relevant and/or responsive documents and assertion of privilege, confidentiality, etc., as appropriate.

Additionally, "On-line Review" enables the culled dataset to be accessed via PC or other terminal device via a local network or remotely via the Internet. Often, the On-Line Review process is facilitated by specialized software that provides additional features and functions which may include: collaborative access of multiple reviewers, security, user logging, search and retrieval, document coding, redaction, and privilege logging.

Why is "Review" important?

The principal objective of review is to determine the relevancy and/or responsiveness of files for efficient and expedient production and subsequent use. This determination must be accomplished while ensuring that the techniques and processes used are both defensible with respect to clients' legal obligations and appropriate with respect to cost-effectiveness and expediency.

As the legal review of electronically stored information (ESI) remains the single most financially expensive portion of the electronic discovery process - in fact, depending on one's source of reference, the cost of review can comprise up to 80% of the total cost of eDiscovery – it is important to understand the major phases of document review, the key characteristics of document review tools, and the key features of document review tools in order to maximize results while controlling costs.

5 Orange Legal Technologies – Review: http://orangelt.us/services/review-services/

What are the two major phases of electronic discovery document review?

While there are many ways to define, describe, and organize the phases that take place in electronic discovery review, for the purpose of this discussion we will focus on the following two phases of review and how they interrelate:

- First Level Review
- Second Level Review

Document review in the context of litigation is done in two levels. The first level of document review is the discovery phase and first part in any litigation. This process is performed after receiving the legal "Request for production of documents". During this process the objective is to reduce the document set into a workable and responsive data set. Even though it is common for e-discovery best practices to have reduced a data set by almost 70%, there still may remain millions of documents to be reviewed. This is because the total quantity of documents has multiplied several times over the years.

In the second level of document review these workable documents are reviewed more seriously by seniors to ensure relevancy, authenticity, accessibility, and to prevent the inadvertent production of privileged documents.

First Level Review

The primary purpose of first level document review typically to review documents and determine whether or not they're "responsive" or "non-responsive" as they pertain to a specific legal case or issue. In essence, first level document review forms part of the discovery phase of litigation. It is performed prior to producing and after receiving documents pursuant to a legal "Request for Production of Documents." It's the initial review phase that helps narrow the document set to a responsive and workable data set for later, more senior review. Litigation aside, aspects of first level document review are also routinely performed in matters of regulatory compliance and corporate due diligence.

Second Level Review

Second Level Review, sometimes referred to as "Privilege Review", is one of the most critical and sensitive aspects of the document review process and usually involves the use of senior reviewers and/or review by the litigators actually involved in the matter under review.

In addition to ensuring a "second set of eyes" are involved in the evaluation of documents under review, second level reviewers are key in preventing the inadvertent production of privileged documents – productions that can result in waiver of privilege for the produced materials. If these protections are waived, any privileged documents disclosed may be deemed waived for all purposes, not only as it relates to the current matter but also as a basis for new civil filings. While the Federal Rules of Civil Procedure do provide some structure to resolve the dispute if a party inadvertently produces privileged material–and notifies the adversary–a much safer strategy is to make sure that privileged documents are not produced in the first place.

What are the key characteristics of viable document review tool (product or service)?

Implementation: Review tools should be able to be quickly set up and customized (via secure Internet connection) for immediate use by reviewers in multiple geographical locations.

Scalability: Review tools should allow the client to take full advantage of all available processing power regardless of the size of the data set being reviewed or the complexity of the review queries. The investment protection provided by scalable and centralized review architecture ensures that growing capacity requirements do not adversely affect review capability.

Centralization: Review tools should allow for time efficient for complex searches against large volumes of documents from centralized review architecture.

Security: Review tools should be secured and supported with forensically sound processes and protocols for both physical and digital security.

Usability: Review tools should be able to be easily accessed and intuitively used by multiple reviewers, from multiple locations, potentially on different review teams.

These primary characteristics of review tools serve as the basis for legal professionals to control electronic data, legal teams, and IT spending in the overall review process. In addition to these characteristics, viable review tools typically share a common set of features that are designed to support these characteristics. Examples of these features are provided in the following section.

What are some of the key capabilities of a viable document review tool (product and/or service)?

While there are many features that are necessary for time efficient and cost effective document review, the following features are ones that appear to be present in today's leading review tools:

- Intuitive to Use
- Built for Speed
- Robust Security
- Workflow Centric
- Robust Reporting
- Client Managed
- Strong Collaboration
- Allows Batch Foldering
- Provides Tag Rules
- Conflict Checking and Management
- Isolates Documents
- Native/Image Review and Redaction Capabilities
- Searching Capabilities
- Message Thread Conversation Grouping
- Parent/Child Association
- Duplicate Identification
- Comment Section
- Role Management
- Review Workflow Management
- Privilege Log Workflow Management
- Production Workflow Management
- Simplicity in Printing
- Allows Production

Intuitive to Use

The review tool should be designed for ease of use by everyone from the client administrator to the ultimate end user. Users should be able to quickly navigate through the tool minimizing the time and effort required to learn how to use the application.

Built for Speed

The review tool should be designed to handle large, fast-paced document reviews and any type of litigation or second request reviews.

Robust Security

The review tool should be secure so as to maintain privilege, protect trade secrets and comply with regulations. End user access should be restricted on a by feature, field, document, folder, or tag basis.

Workflow Centric

A workflow process and methodology should be used to coordinate people, documents and technology. The tool should also create an audit trail of activities and access, and enable management of the roles, responsibilities, tasks and processes for each type of user within a review.

Robust Reporting

Various and customizable reports should be able to be generated by the client for nearly every component of the review and production. For example, clients should be able to receive and review custom daily reports, permission reports, detailed project reports by client, case, or database, admini log reports, and forecasting reports.

Client Managed

The review tool should allow the client to perform most functions within the system, including creation of users, assignment of permissions, creation of tag and conflict rules, generation of productions and privilege logs, generation of various reports, management of reviewer assignments, and definition of batch foldering schemes.

Strong Collaboration

The review tool should provide a shared workspace environment that is accessible anytime, anywhere with an Internet connection. Collaboration support should include the ability to view documents simultaneously and through threaded comment discussions with a chat feature that can be locked down per user.

Allows Batch Foldering

The review tool should allow clients to automatically create folders based on fielded information. For example, a client should be able to folder by Custodian, by Date, by Custodian then by Date, by File Extension, or by original file path of an inbox or network stored files.

Provides Tag Rules

The review tool should be able to identify errors as they are made. This would allow consistent marking of documents across all reviewers, enabling more accurate and timely production sets.

Conflict Checking and Management

Conflict checking should be able to automatically generate reports on any tagging inconsistencies. The client should have predefined conflict rules built in and the ability to manually create conflict rules. This would support consistent marking of documents across all reviewers, thus allowing for more accurate and timely production sets.

Isolates Documents

Clients should be able to lock down, isolate and restrict access to specific documents so that when users log into the system, they will only see the documents they should have access to. This can reduce costs by limiting specialized reviewers to documents that require their specialty.

Native/Image Review and Redaction Capabilities

The review tool should provide native support for multiple formats and users should have a single point of access to their documents, regardless of format, from a single, easy-to-use interface. There should be no need to have the native application installed on the client PC, and redactions should be able to be applied to an image or the actual native document, which would eliminate the need for tiff-on-the-fly.

Searching Capabilities

The review tool should support simple and advanced queries, including Boolean or natural language searches. Other search options, such as word stemming, relevance, or fuzzy, should also be definable by the user with the ability to narrow the search to a specific folder or tag. This allows efficient culling, thus reducing time and expense of review. In addition, attorneys and paralegals can use the search to quickly see if the evidence would support a given legal theory.

Message Thread Conversation Grouping

In support of collaboration, the review application should support message threading, which connects messages that are direct responses to a specific topic or conversation.

Parent/Child Association

The review tool should quickly and easily display the association between emails and their attachments, also known as parent and child association. The feature should be available for both email files as well as scanned paper material.

Duplicate Identification

The review application should quickly and easily display all duplicates in the system on a document level. There should also be a feature enabling users to tag, comment, and redact the original and have all markings transfer to all duplicates. This prevents redundant and inconsistent redactions, which may destroy privilege.

Comment Section

The review application should provide an area where users can share comments and questions regarding specific documents. These comments should be stored as threaded discussions where users can respond to a comment to provide feedback.

These comments should be able to be shared as public or private, and the application should record the user who created the comment, and date/time of when the comment was created.

Role Management

The review application should define multiple roles within the application; for administration, users, expert witnesses, 1st and 2nd reviewers, and privilege reviewers. These roles should be designed to assist with easy categorization of users within a document review. These roles should not be restrictive, meaning that clients should be able to choose not to use them and be able to create custom privileges within the roles. This promotes flexibility in review and ease of setup, thus reducing costs.

Review Workflow Management

The review application should provide a simple interface to manage 1st and 2nd review teams, and allow them to work seamlessly in tandem. The application should assist the client with prioritizing and managing daily workflow tasks, distributing documents to reviewers for action, and generating pre-defined reports to understand the progress of the entire document review. Reviewers should be assigned to specific folders of documents, or be able to pull from the entire population of documents. The reviewers should receive the documents in batches.

The numbers of documents in the batches should be determined by the client and should be completely customizable. This allows review management teams to remain flexible, to add or remove reviewers as necessary, and monitor their progress.

Privilege Log Workflow Management

Clients should be able to easily manage one or more privilege logs in a centralized location with the application. This workspace would allow clients to manage and edit the privilege log, select the fields that need to be on the privilege log, and export the log to a desired delimited format. Furthermore, there should be ability to define privilege log rules and include privilege families so privileged information is not produced by mistake.

Production Workflow Management

Clients should be able to easily manage one or more productions in a centralized location with the application. There should be the ability to define production rules and run conflict checks to only produce what is intended to be produced. This workspace would allow clients to store the production specifications, and review the overall production summary. By doing this, litigation teams can efficiently allocate resources, even across multiple law firms.

Simplicity in Printing

Clients should be able to print reports in a variety of formats including Excel, Word, HTML, XML and several delimited formats and also print documents in PDF with custom headers and footers, watermarks and separator sheets containing fielded information from the database.

Allows for Production

Clients should be able to produce in any standard format with labels, watermarks and bates numbers and deliver the production over the Internet (secure FTP) or on CD, DVD or other magnetic media.

Why is "Review" Important? Reprise

As stated earlier, the principal objective of review is to determine the relevancy and/or responsiveness of files for efficient and expedient production and subsequent use. Through this high level overview of electronic discovery review, the hope is that you will have enough information to ask the right questions and to evaluate review phases, characteristics, and features, so as to ensure that the techniques and processes used in your specific electronic discovery review are effective, efficient, and defensible.

Understanding Electronic Discovery Tasks - Production[6]

What Is "Production"?

As defined by The Sedona Conference, "Production", in the context of electronic discovery, is "the process of delivering to another party, or making available for that party's review, documents and/or ESI deemed responsive to a discovery request". In even simpler terms, "Production" can be understood as the "delivery of data or information in response to an interrogatory, subpoena or discovery order or a similar legal process."

6 Orange Legal Technologies – Production: http://orangelt.us/services/production-services/

What Is One Of The Primary Drivers Of ESI Production?

One of the primary drivers of ESI production is the legal requirement presented in the Federal Rules of Civil Procedure (FRCP). Within the FRCP, Rule 34 (Production of Documents, Electronically Stored Information, and Things and Entry Upon Land for Inspection and Other Purposes) highlights the fact that electronically stored information (ESI) must be produced in forms that are reasonably usable. Requests for production may specify desired data formats for production. If no specification is made, parties must produce the ESI in the format in which it is ordinarily maintained, or in a reasonably usable form (ie, if ordinarily kept in a proprietary format.) Parties do not have to produce ESI in more than one format.

The full content of FRCP Rule 34 is provided below:

(a) Scope.

Any party may serve on any other party a request (1) to produce and permit the party making the request, or someone acting on the requestor's behalf, to inspect, copy, test, or sample any designated documents or electronically stored information — including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations stored in any medium from which information can be obtained — translated, if necessary, by the respondent into reasonably usable

form, or to inspect, copy, test, or sample any designated tangible things which constitute or contain matters within the scope of Rule 26(b) and which are in the possession, custody or control of the party upon whom the request is served; or (2) to permit entry upon designated land or other property in the possession or control of the party upon whom the request is served for the purpose of inspection and measuring, surveying, photographing, testing, or sampling the property or any designated object or operation thereon, within the scope of Rule 26(b).

(b) Procedure.

The request shall set forth, either by individual item or by category, the items to be inspected, and describe each with reasonable particularity. The request shall specify a reasonable time, place, and manner of making the inspection and performing the related acts. The request may specify the form or forms in which electronically stored information is to be produced. Without leave of court or written stipulation, a request may not be served before the time specified in Rule 26(d).

The party upon whom the request is served shall serve a written response within 30 days after the service of the request. A shorter or longer time may be directed by the court or, in the absence of such an order, agreed to in writing by the parties, subject to Rule 29. The response shall state, with respect to each item or category, that inspection and related activities will be permitted as requested, unless the request is objected to, including an objection to the requested form or forms for producing electronically stored information, stating the reasons for the objection. If objection is made to part of an item or category, the part shall be specified and inspection permitted of the remaining parts. If objection is made to the requested form or forms for producing electronically stored information — or if no form was specified in the request — the responding party must state the form or forms it intends to use. The party submitting the request may move for an order under Rule 37(a) with respect to any objection to or other failure to respond to the request or any part thereof, or any failure to permit inspection as requested.

Unless the parties otherwise agree, or the court otherwise orders:

(i) a party who produces documents for inspection shall produce them as they are kept in the usual course of business or shall organize and label them to correspond with the categories in the request;

(ii) if a request does not specify the form or forms for producing electronically stored information, a responding party must produce the information in a form or forms in which it is ordinarily maintained or in a form or forms that are reasonably usable; and

(iii) a party need not produce the same electronically stored information in more than one form.

What Are The Typical Production Formats?

In determining the appropriate forms of production in a case, requesting parties and counsel should consider: (a) the forms most likely to provide the information needed to establish the relevant facts of the case; (b) the need for metadata to organize and search the information produced; (c) whether the information sought is reasonably accessible in the forms requested; and (d) the requesting party's own ability to effectively manage and use the information in the forms requested. Once the requirements for the production, production formats can then be considered. Typically, ESI production formats are classified as native, near-native, near-paper and paper.

Native File Formats

Files produced in the format they were created and maintained are known as native production. In a native production, MS Word documents are produced as .doc files, MS Excel files are produced as .xls files, and Adobe files are produced as .pdf files, etc. Native format is often recommended for files that were not created for printing such as spreadsheets and small databases. For some file types the native format may be the only way to adequately produce the documents.

Near-Native Formats

Some files, including most e-mail, cannot be reviewed for production and/or produced without some form of conversion. Most e-mail files must be extracted and converted into individual files for document review and production. As a result, the original format is altered and they are no long in native format. There is no standard format for near-native file productions. Files are typically converted to a structured text format such as .html or xml. These formats do not require special software for viewing. Other common e-mail formats include .msg and .eml.

Near-Paper Formats

ESI can also be produced in a near paper format. Rendering an image is the process of converting ESI or scanning paper into a non-editable digital file. During this process a "picture" is taken of the file as it exists or would exist in paper format. Based on the print settings in the document, the printer or the computer, data can be altered or missing from the image. Expertise in the field of electronic discovery and image rendering tools are necessary to minimize this risk.

Paper Formats

A paper production is just what it sounds like: paper is produced as paper or ESI is printed to paper and the paper is produced. As with converting to image, printing documents to paper can result in missed or altered data. When producing ESI in paper, it is recommended to utilize someone with expertise in the field of e-discovery and image rendering tools to minimize this risk during the printing or image rendering process.

When Should Production Planning Begin?

Federal Rule of Civil Procedure 26(f) calls for an early discussion of form of production issues. Rule 34 sets forth a more detailed explanation of the ways in which parties should request and respond to requests seeking production or inspection of electronically stored information.

At the outset, parties seeking discovery should have sufficient technical knowledge of production options so that they can make an educated and reasonable request. These options should be discussed at the Rule 26(f) conference and included in any Rule 34(a) requests. Likewise, responding parties should be prepared to address form of production issues at the Rule 26(f) conference.

With respect to requests and responses, the revised Rule 34(b) provides that a request may specify the form or forms in which electronically stored information is to be produced. If objection is made to the requested form or forms for producing electronically stored information, or if no form was specified in the request, the responding party must state the form or forms it intends to use.

If a request does not specify the form or forms for producing electronically stored information, and absent agreement of the parties, a responding party must produce the information in a form or forms in which it is ordinarily maintained or in a form or forms that are reasonably usable unless otherwise ordered by the court. A party need not produce the same electronically stored information in more than one form. [v]

Understanding Meet and Confer Tasks

"As a general rule, the most successful man in life is the man who has the best information."

Benjamin Disraeli

Understanding Meet and Confer Tasks – Pre Meet and Confer

Article via ALI/ABA by Aisha Shelton Adam of Silver & Freedman, used with permission.

The Duty To Preserve Electronic Data In The Paperless Age - Preserving Electronic Documents

By now, it is common knowledge to lawyers and businesses alike that electronic data is discoverable. Courts have uniformly held that businesses may not erase relevant electronic data any more than they may shred relevant documents reduced to paper format. The substitution of the file room for the computer hard drive, however, has irrefutably altered the traditional means by which companies generate, record, and maintain information in ways that were not contemplated when traditional discovery rules were drafted. Millions of email messages, drafts, internal memoranda, correspondence, agreements, and other documents are created daily and stored electronically without copies ever being printed and saved. Not surprisingly, when a conflict or lawsuit arises, electronically stored data may be the only or most reliable evidence available to litigants to maintain or defend the case.

The discovery of electronic data will play an increasingly critical role in most business and commercial litigation cases, and will necessarily affect the way parties conduct litigation, particularly discovery. The increasing capacity by which data may be amassed and stored electronically has the ability to turn a seemingly simple discovery request into a litigation sideshow. As a result, electronic discovery has spawned a host of new legal issues which may arise during the discovery process.

For businesses that are often involved in litigation, especially large corporations, the discovery of electronically stored data presents new, and oftentimes expensive, challenges. Among the issues of concern are:

- When must a company take steps to maintain electronic documents?
- What documents must be retained?
- What steps should be taken to prevent the destruction of electronic data?
- Counsel's role in preserving evidence; and • The consequences for failing to preserve electronic evidence.

WHEN DOES A PARTY HAVE A DUTY TO MAINTAIN ELECTRONIC DOCUMENTS?

Absent actual or threatened litigation, an individual or company may destroy documents at any time or pursuant to an established document retention policy, if any. However, the duty to preserve attaches on notice that particular evidence is relevant to pending litigation or when the party should have known that the evidence may be relevant to future litigation. Zubulake v. UBS Warburg LLC, 220 F.R.D. 212 (S.D.N.Y. 2003). In considering whether the duty to preserve is triggered, the courts will review "the totality of the circumstances using either an objective or subjective test: did the party actually anticipate litigation, or would a reasonable person in the party's position anticipate litigation?" Trevino v. Ortega, 969 S.W.2d 950, 956 (Tex. 1990).

Anticipating Litigation

Litigation may be "reasonably anticipated" before a complaint is filed if a party is served with a demand letter, subpoena, or preservation letter requesting that certain electronic information be retained. The duty to retain electronic information relevant to future litigation may also arise by statute or may be triggered during an existing lawsuit. Turner v. Hudson Transit Lines, Inc., 142 F.R.D. 68, 72 (S.D.N.Y. 1991).

Additionally, the factual circumstances surrounding a certain event may also notify a party that future litigation may arise, thereby giving rise to the obligation to preserve evidence relevant to that lawsuit. Hirsch v. General Motors Corp., 628 A.2d 1108, 1122 (N.J. Super. Ct. Law Div. 1983).

For example, in Zubulake v. UBS Warburg LLC, et al., 220 F.R.D. 212 (S.D.N.Y. 2003) ("Zubulake IV"), plaintiff Zubulake filed a complaint with the Equal Employment Opportunity Commission ("EEOC") against her former employer UBS for gender discrimination. Plaintiff argued that the duty to preserve electronic evidence arose before she filed her complaint; the court agreed. Id. at 216. At the latest, the court concluded that the duty to preserve arose when Zubulake filed her complaint with the EEOC. Id. However, the court determined that the preservation duty attached even before the lawsuit was filed because "almost everyone associated with Zubulake recognized the possibility that she might sue." Id. at 216-217.

In reaching its decision, the court in Zubulake IV noted that key UBS employees, including plaintiff's supervisors and co-workers, circulated emails about plaintiff labeled "UBS Attorney Client Privilege" even though the emails were not directed toward any attorney and no attorney was copied on the email. Id. at 217. The court also noted that Zubulake's supervisor testified during deposition that he feared litigation was possible more than three months before the lawsuit was filed. Id. The Zubulake IV court was quick to caution that the "reasonable anticipation" of litigation consists of more than speculation by a few employees about the possibility of a future lawsuit.

Id. Future litigation must be "reasonably anticipated" by "key players," or persons who likely possess information which may be relevant to future or actual litigation. Id. In other words, mere gossip or speculation amongst co-workers is not enough.

THE SCOPE OF THE DUTY TO PRESERVE ELECTRONIC DATA

Once the obligation to preserve electronic data is triggered, it is imperative that the parties understand the scope of the data covered by the preservation obligation. In Zubulake IV, the court announced that a corporation need not "preserve every shred of paper, every e-mail or electronic document, and every backup tape" before or during actual or threatened litigation. Zubulake IV, 220 F.R.D. at 217. Indeed, such a blanket requirement would handicap or "cripple" large corporations that are often parties to lawsuits. Id.

At the same time, however, once a lawsuit is anticipated or has commenced, a party may not destroy evidence relevant to a claim or defense. Thus, although a party is under no duty to safeguard every document in its possession, it must preserve "what it knows, or reasonably should know is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery, [or] is the subjection of pending discovery sanction." Trevino, supra, 969 S.W.2d at 957.

The duty to preserve applies not only to data that existed before litigation commenced or was "reasonably anticipated," but to all data created any time thereafter. Zubulake IV, 220 F.R.D. at 218. Moreover, the duty to preserve evidence also includes the obligation to preserve backup tapes which may contain relevant documents which were deleted negligently, intentionally, or pursuant to a company's routine document retention policies. Id.

The court in Zubulake IV elaborated on a party's duty to preserve backup tapes, holding that the preservation obligation does "not apply to inaccessible backup tapes (e.g., those typically maintained solely for the purpose of disaster recovery), which may continue to be recycled on the schedule set forth in the company's policy." Id. Conversely, if a company's "backup tapes are accessible (i.e., actively used for information retrieval), then such tapes would likely be subject to the litigation hold." Id.

The court in Zubulake IV carved out an exception to these rules for situations in which a company is able to locate documents created by key players involved in litigation. The court expressly provided that "[i]f a company can identify where particular employee documents are stored on backup tapes, then the tapes storing the documents of 'key players' to the existing or threatened litigation should be preserved if the information contained on those tapes is not otherwise available. The exception applies to all backup tapes." Id.

PREVENTING THE DESTRUCTION OF ELECTRONIC DATA WHEN LITIGATION IS THREATENED OR IN ACTUAL LITIGATION

A company must take affirmative steps to ensure that it complies with its duty to preserve electronic data once the duty is triggered. Oftentimes, a company has a document retention policy that provides for automatic review, retention, and destruction of business records, emails, webpages and other documents. Although such policies promote efficiency by deleting unnecessary documents and files, these policies may directly conflict with the duty to maintain documents during anticipated or actual litigation. Because of this potential conflict, companies must act dutifully and quickly to safeguard relevant evidence.

In Zubulake IV, the court made clear that once the obligation to preserve electronic evidence is triggered, a party must suspend its routine document retention/destruction policy and put in a place a "litigation hold" to ensure the preservation of relevant documents and accessible backup tapes. Zubulake IV, 220 F.R.D. at 218. Failing to do so may have severe consequences. For example, in In re Prudential Insurance Company of America Sales Practices Litigation, 169 F.R.D. 598 (D. N.J. 1997), the defendant agreed to suspend its usual document retention policy, but failed to communicate the order in a manner in which "key players" were likely to read it.

Time, Risk and Cost in eDiscovery[1]

Time: The Need for Speed - The ability of legal professionals to quickly gain an understanding of potential evidence is of paramount importance if they want to seize the initiative in the conduct of litigation. In practical terms, the quicker a legal team can gain an understanding of available ESI, the quicker they can make early case assessments in relation to key questions to include:

- Does it appear that opposing counsel has an evidential basis for pursuing the case?
- What type of electronic discovery resources will be needed to conduct a complete document review?
- Based on FRCP 26(f)[2] , what are the timeline requirements for "Meet and Confer" preparation?
- Based on potential evidence and resource requirements, will it be more cost effective to settle or pursue?

By quickly being able to answer these questions, legal teams can gain the "litigation high ground" and ensure they are making informed client recommendations as early as possible in the litigation process – thus ensuring economy of effort without sacrificing the ability to achieve a desired outcome. Understanding of available ESI can also ensure counsel is prepared to proactively shape the direction of handling ESI during the federally mandated "Meet and Confer" process.

Traditional electronic discovery approaches typically can provide a legal team access to ESI in 2-3 weeks, however new approaches can provide access to ESI in as early as 2-3 days.

Risk: More than a Board Game - Litigation is inherently rife with risk, and the complexity of discovery of ESI only increases this risk based on the intricacies of digital data, the continually growing volume of data available, and evolving ESI related law. Managing this complexity requires an understanding of what is an acceptable risk in relation to the time available and the financial resources available. In determining acceptable risk, three of the key concerns of legal professionals are:

- Will the electronic discovery approach reduce the risk of missing potentially responsive documents?
- Will the electronic discovery technologies used minimize risks associated with the transfer of data between organizations and platforms?
- Will the electronic discovery effort be conducted in a legally defensible manner?

"The message to be taken from O'Keefe, Equity Analytics, and this opinion is that when parties decide to use a particular ESI search and retrieval methodology, they need to be aware of the literature describing the strengths and weaknesses of various methodologies." Judge Paul Grimm, District of Maryland Judge

In viewing traditional electronic discovery approaches and with these risk considerations in mind, it appears that time available and financial resources determine the level of acceptable risk. However, newer electronic discovery approaches can reduce the risk of missing potentially responsive documents, conduct the entire process in a legally defensible manner, and also do these things in the most time efficient and cost effective manners.

Cost: Show Me the Money - The economics of electronic discovery are such an important factor in litigation that, in some cases, they may drive counsel recommendations as much, if not more, than the actual evidentiary position of the client. Additionally, based on the current economic conditions worldwide, many law firms and corporations have been significantly impacted financially and while litigation related to the financial crisis may be on the rise, there is also a corresponding decrease in the number of discretionary litigation efforts due to cost constraints. [3] With this economic importance in mind, legal professionals not only want to but need to be able to conduct as thorough electronic discovery effort as possible at the lowest monetary cost possible. Key questions needing to be considered when evaluating the financial factor of electronic discovery may include:

- Based on time requirements and acceptable risk, what is the best electronic discovery approach congruent with firm and client financial resources and cost management objectives?
- Do we have the electronic discovery systems and expertise in place to conduct the electronic discovery tasks using the best electronic discovery approach congruent with client financial and cost management objectives?

Traditional electronic discovery approaches typically can cost anywhere between $40,000 to $130,000 – exclusive of attorney review costs – to conduct the necessary electronic discovery tasks on 100GB of ESI. However, new approaches can cut these costs significantly as they can perform the same tasks for less than $30,000.

1 Orange Legal Technologies: http://tinyurl.com/az6e84
2 Federal Rules of Civil Procedure, Rule 26(f), http://www.law.cornell.edu/rules/frcp/Rule26.htm
3 E-Discovery 2.0, Aaref Hilaly, January 8, 2008, http://snipr.com/9n1wz

Initiating Preservation

Trigger: Reasonable Anticipation of Litigation

Zubalake v. UBS Warburg LLC, 220 F.R.D. 212, 218 (S.D.N.Y. 2003) (Zubulake IV)

"Once a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a 'litigation hold' to ensure the preservation of relevant documents."

Tasks: Logical Task Considerations

1. Document Data/Time/Reason for Trigger Event
2. Temporarily Suspend Document Destruction Policies
3. Meet with Litigation Hold Planning Team to Establish Litigation Hold Strategy (Minimum of Potential Matter Lead (Legal), eDiscovery Team Lead, IT Team Lead, Records Management Team Lead).
4. Review Document Retention Plan and Procedures
5. Review Litigation Hold Procedures
6. Identify Potentially Relevant Custodians (By Name and By Role)
7. Identify Legal And Technology Leads for Specific Litigation Hold Effort
8. Prepare and Disseminate Litigation Hold Letters to Relevant Custodians (Name/Role) (Send Copy To Opposing Counsel if Opposing Counsel Activated "Trigger")
9. Adjust/Amend Document Destruction Policies as Appropriate
10. Follow Up with Potentially Relevant Custodians (Name/Role) to Confirm Understanding of Hold Letter

Scoping Data and Resources

Target: What data is to be preserved?

Zubulake IV, 220 F.R.D. at 217 - a party need not "preserve every shred of paper, every e-mail or electronic document, and every backup tape" before or during actual or threatened litigation.

Trevino, supra, 969 S.W.2d at 957 – a party must preserve "what it knows, or reasonably should know is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery, [or] is the subjection of pending discovery sanction."

Tasks: Logical Data Scoping and Resource Considerations

- Determine where the data to be preserved is located
- Determine the size of the accessible volume of data to be preserved
- Determine what resources may be needed to collect accessible data
- Determine the need for access to inaccessible data
- Estimate the potential resources that may be needed to collect inaccessible data
- Determine who might be able to serve as a potential expert – 30(b)(6) – witness.

Estimating Costs

Target: Understanding of Potential eDiscovery Costs in Terms of Time, Risk, and Money

Tasks: Logical eDiscovery Cost Planning Considerations

Time Considerations

- Does it appear that opposing counsel has an evidential basis for pursuing the case?
- What type of eDiscovery resources will be needed to conduct a complete document review?
- Based on FRCP 26(f) , what are the timeline requirements for "Meet and Confer" preparation?
- Based on potential evidence/resources, will it be more cost effective to settle or pursue?

Risk Considerations

- Will the electronic discovery approach reduce the risk of missing potentially responsive documents?

- Will the electronic discovery technologies used minimize risks associated with the transfer of data between organizations and platforms?
- Will the electronic discovery effort be conducted in a legally defensible manner?

Cost Considerations

- Based on time requirements and acceptable risk, what is the best electronic discovery approach congruent with firm and client financial resources and cost management objectives?
- Do we have the electronic discovery systems and expertise in place to conduct the electronic discovery tasks using the best electronic discovery approach congruent with client financial and cost management objectives?

Determining Plan/Proposal

Target: Develop a Recommended Discovery Plan for presentation to opposing counsel at the Meet and Confer Meeting.

Tasks: Logical Discovery Plan Preparation (Requirements and Time/Risk/Cost Estimates)

Timing Considerations

- Verify date/time of FRCP Rule 16(b) Scheduling Conference
- Coordinate with Opposing Counsel on date/time for Meet and Confer Conference (Required as soon as possible, NLT 21 days prior to Scheduling Conference (FRCP Rule 26 (f)(1)).

Plan/Proposal Considerations

- Determine best case Discovery Plan (What would you like to do?)
- Determine most objective Discovery Plan (What would you expect to do?)
- Determine worst case Discovery Plan (What are your limits of plan acceptance?)

Document Considerations

- Develop Form 35 "Drafts" for each Plan (Guidelines for Form 35 Completion/Negotiation)
- Prepare and Submit Disclosures as required by FRCP 26(a)

Understanding Meet and Confer Tasks – Meet and Confer Meeting

Preservation Considerations

- Define/Determine Data Scope
- Define Accessible and Unreasonably Accessible Data
- Define/Determine Handing of Unreasonably Accessible Data

Electronic Discovery Issues

- Determine Handling of Duplicates, Masters, and Attachments
- Determine Keyword Search Terms and Search Methodologies
- Determine Cost Shifting Approach

Production Considerations

- Determine Production Formats
- Determine Production Priorities
- Determine Approach for Special Markings (Privacy Act, Confidential/Data Secret, Bates Schema)

Privilege Considerations

- Determine Handling of Sensitive Data (Privacy Act, Confidential/Secret Data)
- Determine Need for Clawback Agreement
- Determine Need for Quick Peek Agreement

Understanding Meet and Confer Tasks – Post Meet and Confer Follow Up

Verify

- Litigation Hold Compliance (Update and Audit)
- Keyword Searches (Test)

Document

- Litigation Hold Efforts
- Complete Form 35
- Complete Proposed Scheduling Order (As Required By Court)

Report

- Submit Form 35 To Court (Typically within 14 Days of Meet and Confer Conference)
- Submit Proposed Scheduling Order (As Required By Court)

Example Scheduling Order: PROPOSED SCHEDULING ORDER – UTAH

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF UTAH ________________ DIVISION

Plaintiff, Plaintiff, v. *Defendant*, Defendant.	**SCHEDULING ORDER AND ORDER VACATING HEARING** Case No. *Case No.* District Judge *District Judge* Magistrate Judge *Magistrate Judge*

Pursuant to Fed.R. Civ P. 16(b), the Magistrate Judge[1] received the Attorneys' Planning Report filed by counsel. The following matters are scheduled. The times and deadlines set forth herein may not be modified without the approval of the Court and on a showing of good cause.

IT IS ORDERED that the Initial Pretrial Hearing set for *Hearing Date*, 20__, at *Hearing Time* ____:____ __. m. is VACATED.

****ALL TIMES 4:30 PM UNLESS INDICATED****

1.		**PRELIMINARY MATTERS**	**DATE**
		Nature of claims and any affirmative defenses:	
	a.	Was Rule 26(f)(1) Conference held?	*00/00/00*
	b.	Has Attorney Planning Meeting Form been submitted?	*00/00/00*
	c.	Was 26(a)(1) initial disclosure completed?	*00/00/00*
2.		**DISCOVERY LIMITATIONS**	**NUMBER**
	a.	Maximum Number of Depositions by Plaintiff(s)	*10 or #*
	b.	Maximum Number of Depositions by Defendant(s)	*10 or #*
	c.	Maximum Number of Hours for Each Deposition (unless extended by agreement of parties)	*7 or #*
	d.	Maximum Interrogatories by any Party to any Party	*25 or #*

Meet and Confer Tasks

e.	Maximum requests for admissions by any Party to any Party	#
f.	Maximum requests for production by any Party to any Party	#

3.	**AMENDMENT OF PLEADINGS/ADDING PARTIES[2]**	**DATE**
a.	Last Day to File Motion to Amend Pleadings	*00/00/00*
b.	Last Day to File Motion to Add Parties	*00/00/00*

4.	**RULE 26(a)(2) REPORTS FROM EXPERTS[3]**	**DATE**
a.	Plaintiff	*00/00/00*
b.	Defendant	*00/00/00*
c.	Counter reports	*00/00/00*

5.	**OTHER DEADLINES**	**DATE**
a.	Discovery to be completed by:	
	Fact discovery	*00/00/00*
	Expert discovery	*00/00/00*
b.	*(optional)* Final date for supplementation of disclosures and discovery under Rule 26 (e)	*00/00/00*
c.	Deadline for filing dispositive or potentially dispositive motions	*00/00/00*

6.	**SETTLEMENT/ALTERNATIVE DISPUTE RESOLUTION**		**DATE**
a.	Referral to Court-Annexed Mediation:	*Yes/No*	
b.	Referral to Court-Annexed Arbitration	*Yes/No*	
c.	Evaluate case for Settlement/ADR on		*00/00/00*
d.	Settlement probability:		

Specify # of days for Bench or Jury trial as appropriate.
Shaded areas will be completed by the court.

			TIME	DATE
7.	**TRIAL AND PREPARATION FOR TRIAL**			
a.	Rule 26(a)(3) Pretrial Disclosures[4]			
	Plaintiff			*00/00/00*
	Defendant			*00/00/00*
b.	Objections to Rule 26(a)(3) Disclosures (if different than 14 days provided in Rule)			*00/00/00*
c.	Special Attorney Conference[5] on or before			*00/00/00*
d.	Settlement Conference[6] on or before			*00/00/00*
e.	Final Pretrial Conference		___:___ _.m.	*00/00/00*
f.	Trial	Length		
	i. Bench Trial	*# days*	___:___ _.m.	*00/00/00*
	ii. Jury Trial	*# days*	___:___ _.m.	*00/00/00*

8. OTHER MATTERS

Counsel should contact chambers staff of the District Judge regarding Daubert and Markman motions to determine the desired process for filing and hearing of such motions. All such motions, including Motions in Limine should be filed well in advance of the Final Pre Trial. Unless otherwise directed by the court, any challenge to the qualifications of an expert or the reliability of expert testimony under Daubert must be raised by written motion before the final pre-trial conference.

Dated this ________ day of ____________________, 20__.

BY THE COURT:

____

U.S. Magistrate Judge

The Magistrate Judge completed Initial Pretrial Scheduling under DUCivR 16-1(b) and DUCivR 72-2(a)(5). The name of the Magistrate Judge who completed this order should NOT appear on the caption of future pleadings, unless the case is separately referred to that Magistrate Judge. A separate order may refer this case to a Magistrate Judge under DUCivR 72-2 (b) and 28 USC 636 (b)(1)(A) or DUCivR 72-2 (c) and 28 USC 636 (b)(1)(B). The name of any Magistrate Judge to whom the matter is referred under DUCivR 72-2 (b) or (c) should appear on the caption as required under DUCivR10-1(a).

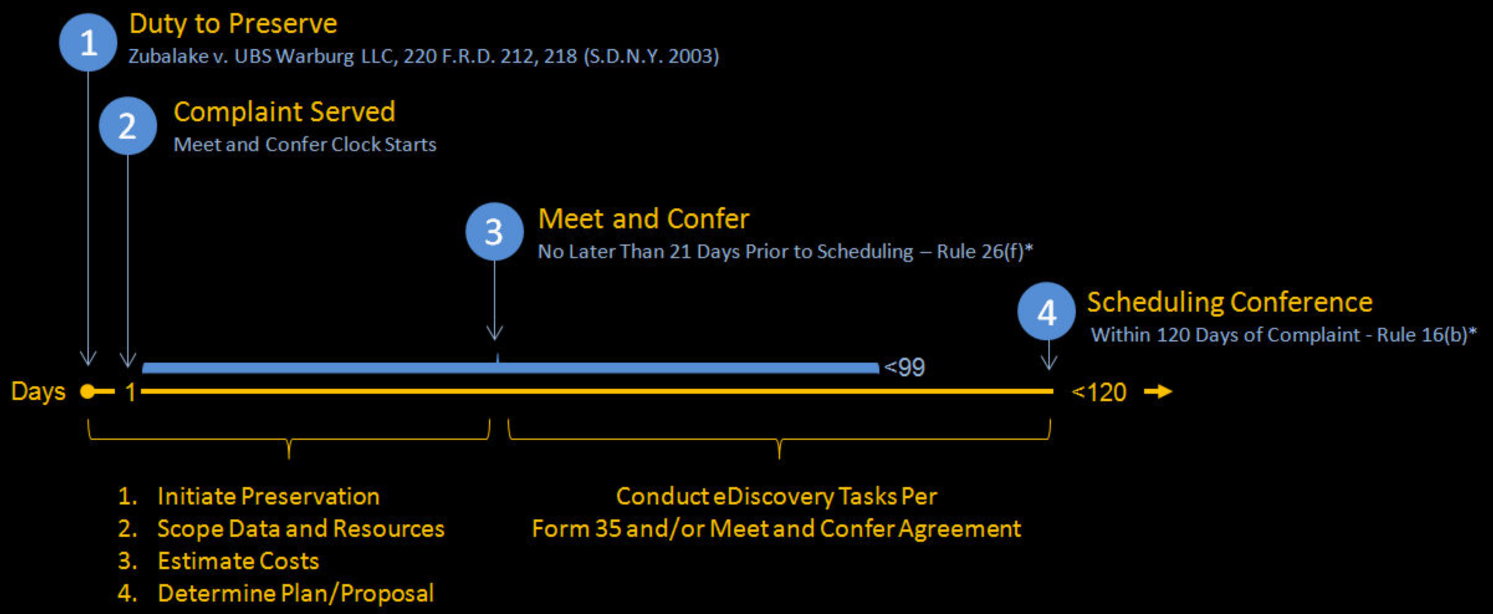
Counsel must still comply with the requirements of Fed. R. Civ. P. 15(a).

A party shall disclose the identity of each testifying expert and the subject of each such expert's testimony at least 60 days before the deadline for expert reports from that party. This disclosure shall be made even if the testifying expert is an employee from whom a report is not required.

Any demonstrative exhibits or animations must be disclosed and exchanged with the 26(a)(3) disclosures.

The Special Attorneys Conference does not involve the Court. Counsel will agree on voir dire questions, jury instructions, a pre-trial order and discuss the presentation of the case. Witnesses will be scheduled to avoid gaps and disruptions. Exhibits will be marked in a way that does not result in duplication of documents. Any special equipment or courtroom arrangement requirements will be included in the pre-trial order. The Settlement Conference does not involve the Court unless a separate order is entered. Counsel must ensure that a person or repre¬sentative with full settlement authority or otherwise authorized to make decisions regarding settlement is available in person or by telephone during the Settlement Conference.

The Sequence and Chronology of Meet and Confer



* Unless Otherwise Directed By The Court

Translating Understanding into Execution

"The goal is to transform data into information, and information into insight"

Carly Fiorina

Translating Understanding into Execution – Checklists for Meet and Confer Tasks

Example Checklists

- **Fios:** http://snurl.com/e7gns
- **ieDiscovery:** http://snurl.com/e7got
- **LexisNexis:** http://tinyurl.com/d77a4t (Litigation Readiness)
- **Merrill Corporation**: http://tinyurl.com/cjjdep
- **Pitney Bowes:** http://tinyurl.com/clebpj

Translating Understanding into Execution – Case Law Considerations

Toussie v. County of Suffolk, 2007. (E.D.N.Y. Dec. 21, 2007)[1]

Case Summary on County's "Foot Dragging" in Discovery and Failure to Implement Legal Hold Warrant Monetary Sanctions, but not Default Judgment or Adverse Inference Instruction, Posted On Electronic Discovery Law (www.ediscoverylaw.com) on January 3, 2007. Copyright © 2009, K&L Gates LLP.

In this case, plaintiffs alleged that their civil rights had been violated when the defendants denied them the opportunity to purchase real estate at auction. The email dispute was first brought to the court's attention in August 2006, when the plaintiffs moved to compel supplemental discovery responses from the County. Plaintiffs' counsel argued that the County had failed to perform a diligent search for responsive documents, evidenced by the fact that it had only produced two emails. During a conference with the court on the matter, counsel for the County suggested that since it was "more the exception than the rule," that employees were "communicating be email," a further search was unlikely to uncover additional emails. However, because it became clear that the County had failed to conduct a system wide search for responsive emails, the court directed the County to have its Information Technology Department search the County's servers for responsive emails.

In October 2006, plaintiffs moved for sanctions, contending that the County had willfully failed to comply with the court's order. In response, the County submitted an affidavit from its Director of Management Information Services, explaining that the County lacked the resources to perform the court-ordered search for additional emails. He estimated that the cost to restore the County's backed up data would be roughly $36,000, and that the process would take as much as 1,700 man hours.

Upon receipt of the County's response, the court held another conference, during which the court expressed its exasperation with the County's position by noting: "You can't just throw up your hands and say we don't store [e-mails] in an accessible form and then expect everybody to walk away." The court narrowed the scope of the email search to be conducted, and directed the County to prepare a search plan. The search plan was to include an estimate of the cost, manpower, and time needed to conduct a search for emails responsive to 35 search terms on the servers of five key County departments for a particular time period.

The County thereafter advised the court in a letter that, in order to perform the search, it would be necessary to restore 470 backup tapes, and that the new system required to conduct the search would cost approximately $934,000. The County estimated that the search would take 960 man hours to complete. The County also noted that it had explored the possibility of hiring an outside consultant to perform the search and learned that to do so would cost between $617,000 and $672,000.

Additional conferences with the court were held on the subject, and the County ultimately hired an outside vendor to perform the search. In the end, the vendor restored 417 backup tapes and yielded 2,403 pages of emails and attachments to those emails, of which approximately 200 were withheld on the basis of privilege, "a far cry from the two e-mails originally produced by the County."

1 Case Summary - K&L Gates: http://tinyurl.com/22jr98

Plaintiffs remained unsatisfied with the production, and argued that even after the restoration, the County's total production could not possibly represent the emails exchanged by dozens of people in the targeted departments. They noted, for example, that according to other documents produced, one of the key players should alone have had 1,200 emails in his inbox. Plaintiffs also argued that the destruction of emails was evident from the fact that the County was able to produce emails sent from one key player to another, but the email that should have been received was missing.

Plaintiffs argued that had the County implemented a litigation hold and discontinued its practice of overwriting tapes, more relevant emails would have been preserved. Consequently, plaintiffs requested that default judgment be entered against the defendants or, in the alternative, that an adverse instruction be given to the jury chosen to hear the case. The County denied any spoliation and claimed that it made enormous efforts, at a substantial monetary cost, to fulfill its obligations and that there was no destruction or untimely production of evidence.

Citing Zubulake v. UBS Warburg LLC, 229 F.R.D. 422 (S.D.N.Y. 2004), the court observed that plaintiffs needed to establish three elements in order to obtain spoliation sanctions: (1) that the party having control over the evidence had an obligation to preserve it at the time it was destroyed; (2) that the records were destroyed with a "culpable state of mind"; and (3) that the destroyed evidence was 'relevant' to the party's claim or defense such that a reasonable trier of fact could find that it would support that claim or defense.

The court found that the duty to preserve arose when the complaint was filed, and that the County was then under an obligation to preserve any "unique" and "relevant" evidence. "Simply stated, any documents prepared by or for County employees, employed in the four key departments, which involved the Toussie transactions, should have been preserved." The court concluded that the County had breached its duty to preserve in a number of respects. Among other things, it did nothing to alter its document retention policy to insure the availability of relevant discovery. Further, even after the County had received a document request, key personnel remained free to delete documents from the system because the County failed to put in place a litigation hold.

The court found that the second element had also been established, as the County's failure to implement a litigation hold amounted to gross negligence, and its failure to preserve all potentially relevant backup tapes was "merely negligent."

However, the court found that plaintiffs had not adequately established the relevance of the missing emails:

There is no question that the County's early foot dragging delayed this litigation and that the County failed to implement a litigation hold. This conduct, however, does not rise to the egregious level seen in cases where relevance is determined as a matter of law. The courts analysis, thus, turns to the extrinsic evidence offered by the plaintiffs to show that the destroyed e-mails would have been favorable to their case.

The court evaluated six emails plaintiffs had attached to their briefing, and found that, if anything, the emails were more helpful to the defense. The court concluded:

While the evidence is clear that at least 9% of the back up tapes were destroyed and the plaintiffs may be correct that e-mails have been deleted by users, there is no reason to believe that any of those e-mails would have provided any additional support of plaintiffs' claims. Accordingly, the plaintiffs have not sufficiently demonstrated that the destroyed/lost emails were favorable or relevant and the motion for a default judgment or an adverse inference instruction is denied.

The court went on to award plaintiffs their costs associated with the email dispute:

Although the plaintiffs have not provided sufficient evidence of relevance to warrant an adverse inference instruction, the County was initially recalcitrant in meeting its discovery obligations. The County's lack of diligence is evidenced by the fact that the County first took the position that it would not uncover more than the two e-mails initially produced. In addition, counsel for the County first became aware that its back up tapes were damaged by a 2004 flood six months into these proceedings. There is no question that until the February 2007 hearing, the plaintiffs were required to expend resources in litigation in order to obtain the e-mails that have now been produced, and thus, those costs are compensable. Accordingly, the County shall also reimburse the plaintiffs for the costs associated with their appearance at the hearings dated November 21st and December 4th, as well as the preparation of their January 4, 2007 application. The plaintiffs shall submit an affidavit to the court setting forth those costs by January 11, 2008.

O'Bar v. Lowe's Home Centers, Inc., 2007. (W.D. N.C. May 2, 2007)[2]

Case Summary on Court Detailed Guidelines for Discovery of ESI, Adapting "Suggested Protocol" of the District of Maryland Posted On Electronic Discovery Law (www.ediscoverylaw.com) on May 9, 2007. Copyright © 2007, K&L Gates LLP.

This is a putative class action in which the plaintiffs allege they were discriminated against because they were not minorities or females. Finding that plaintiffs were entitled to limited precertification discovery, the court ordered the parties, pursuant to Rule 26(f), to jointly prepare and submit to the court a specific and detailed precertification discovery plan. Based upon the previous disputes between the parties, the court stated it anticipated issues arising as to the discovery of data through various types of computer programs maintained by defendant. Thus, in order to assist the parties in conducting discovery of electronically stored information ("ESI"), the court set out detailed guidelines that would govern the parties. The guidelines were adapted from the "Suggested Protocol for Discovery of Electronically Stored Information" set forth by the United States District Court for the District of Maryland.

The court encouraged the parties to discuss the following subjects, in preparing the precertification discovery plan:

A. The anticipated scope of requests for, and objections to, production of ESI, as well as the form of production of ESI and, specifically, but without limitation, whether production will be of the Native File, Static Image, or other searchable or non-searchable formats;

B. Whether Meta-Data is requested for some or all ESI and, if so, the volume and costs of producing and reviewing said ESI;

C. Preservation of ESI during the pendency of the lawsuit;

D. Post-production assertion, and preservation or waiver of, the attorney-client privilege, work product doctrine, and/or other privileges in light of "clawback," "quick peek," or testing or sampling procedures, and submission of a proposed order;

E. Identification of ESI that is or is not reasonably accessible without undue burden or cost;

F. Methods of identifying pages or segments of ESI produced in discovery;

G. The method and manner of redacting information from ESI if only part of the ESI is discoverable;

H. The nature of information systems used by the party or person or entity served with a subpoena requesting ESI;

I. Specific facts related to the costs and burdens of preservation, retrieval, and use of ESI;

J. Cost sharing for the preservation, retrieval and/or production of ESI, including any discovery database, differentiating between ESI that is reasonably accessible and ESI that is not reasonably accessible;

K. Search methodologies for retrieving or reviewing ESI;

L. Preliminary depositions of information systems personnel, and limits on the scope of such depositions;

M. The need for two-tier or staged discovery of ESI, considering whether ESI initially can be produced in a manner that is more cost-effective, while reserving the right to request or to oppose additional more comprehensive production in a latter stage or stages;

N. The need for any protective orders or confidentiality orders, in conformance with the Local Rules and substantive principles governing such orders;

O. Any request for sampling or testing of ESI; the parameters of such requests; the time, manner, scope, and place limitations that will voluntarily or by Court order be placed on such processes; the persons to be involved; and the dispute resolution mechanism, if any, agreed-upon by the parties; and

P. Any agreement concerning retention of an agreed-upon Court expert, retained at the cost of the parties, to assist in the resolution of technical issues presented by ESI.

2 Case Summary - K&L Gates: http://tinyurl.com/33vlm7

Translating Understanding into Execution – Additional Reading

Books

- Discovery of Electronically Stored Information – Surveying the Legal Landscape - Ronald J. Hedges/BNA Books
- The Discovery Revolution – E-Discovery Amendments to the Federal Rules of Civil Procedure - George L. Paul and Bruce H. Nearon/ABA Publishing
- Electronic Discovery and Digital Evidence: Cases and Materials - Shira Scheindlin, Daniel Capra and The Sedona Conference/West Publishing
- A Process of Illumination – The Practical Guide to Electronic Discovery - Mary Mack, Esq./Fios
- E-Discovery: Current Trends and Cases - Ralph C. Losey/ABA Publishing

Articles/Papers

- The Duty To Preserve Electronic Data In The Paperless Age - Preserving Electronic Documents - Aisha Shelton Adam /The Practical Litigator - http://tinyurl.com/dxn7ed
- E-Discovery - The Long and the Short of "Accessibility" - John Coughlin/Duane Morris E-Discovery Alert - http://tinyurl.com/dmtl7a
- Prepare for an Effective Meet and Confer - Linda Kish/DataBased Advisor - http://tinyurl.com/d6creu -
- 2009 Meet & Confer Toolkit - i.e.Discovery Professional Tool- http://www.iediscovery.com/offer/Default.aspx
- One Hundred Days of Discovery - Preparing for the 26(f) Meet & Confer Scheduling Conference - Pitney Bowes White Paper - http://tinyurl.com/clebpj

ORANGE LEGAL TECHNOLOGIES

About Orange Legal Technologies

Orange Legal Technologies delivers one source litigation, audit, and investigation support services with a focus on the electronic discovery tasks of analytics, processing, and review. The One OneO® Discovery Platform provides law firm and corporate legal professionals with an integrated, web-accessible, forensically sound electronic discovery platform that enables online analytics, processing, and review of data from the security of a hosted centralized repository. To learn more, contact us at info@orangelt.com or via the web at OrangeLT.com.

About the OneO® Discovery Platform

The OneO® Discovery Platform, provides law firm and corporate legal professionals with an integrated, web-accessible, forensically sound electronic discovery platform that enables online analytics, processing, and review of data from the security of a hosted centralized repository. The OneO® Discovery Platform can quantifiably save users 1/2 the time, 1/2 the cost, while lowering the risks associated with traditional electronic discovery approaches.

Orange Legal Technologies
251 South Floral Street
Salt Lake City, Utah 84111
OrangeLT.com | info@orangelt.com