Chapter Eight

Mastering E-Discovery

This chapter discusses the software programs and technical and organizational problems and solutions available for handling e-discovery and offers best practices for new lawyers.

Chapter Overview

- By the end of this chapter, you should be familiar with
- e-discovery compliance issues
- electronic information storage, retrieval, and methods of production
- the technical and organizational problems and solutions available for handling e-discovery
- e-discovery retrieval and organization
- the rules on e-discovery that you must comply with

First, let's take a step-by-step look at the major e-discovery steps involved in litigation:

Step 1: Spoliation Matters.

A litigation hold preventing the recycling, discarding, or deleting of electronically stored media and information is established when litigation is reasonably anticipated, but must be no later than when the client has notice of pending litigation. This is an important step in preserving information so that it is available for discovery, as many businesses and individuals routinely recycle their backup media and delete material in the ordinary course of business. You must inform your clients to establish a litigation hold at the earliest possible opportunity to avoid claims of spoliation of evidence.

Step 2: Discovery Sources.

Your litigation team must determine likely sources of discoverable information, both from a standpoint of key people and of repositories for such information. An organizational chart and schematic for stored information helps to pinpoint likely targets for e-discovery and traditional hard-copy material. These issues are

discussed both with the client—who will need to conduct searches responsive to the adversary's requests—and with opposing counsel, to narrow areas of dispute, speed discovery, and reduce costs.

Step 3: Initial Disclosures.

Federal courts require the parties to make initial disclosures before formal discovery can be undertaken. Some state courts require the same. As part of the initial disclosures in accordance with Rule 26(f), the parties establish a plan for dealing with e-discovery issues, including the discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. On a motion to compel discovery or for a protective order, the parties should be prepared to address how reasonably accessible the information is based on both undue burden and cost. The discovery plan must state the parties' views and proposals on any issues about disclosure or discovery of electronically stored information, including the form or forms of production and any limitations on discovery.

Step 4: E-Discovery Plans.

The court may issue discovery orders regarding the plan or require a formal discovery conference or pretrial conference under Rule 16, which will set out timelines, the scope of discovery including e-discovery, and software and expense issues concerning e-discovery.

Step 5: E-Discovery Searches.

Your litigation team drafts discovery requests, including interrogatories and requests for production of documents, targeting the identity and holders of key electronic and other information that falls within the scope of discoverable information. After your team drafts appropriate discovery requests and ensures that hard-copy and soft-copy information is carefully examined, then those discovery requests are served on the opposing party and information storage entities. At this point, a Keeper of the Records deposition is scheduled to ensure that all possible sources of discoverable information have been reached and a thorough search has been made.

Step 6: Discovery Compliance and Privilege.

Your litigation team reviews responses from the client and opponents to ensure compliance with the discovery requests, assertion of privilege claims, creation of a privilege log, and any objections to the requests. A party produces a privilege log when objecting to a discovery request based on privilege or work product. The privilege log briefly describes each document that is protected by a claim of privilege

or other protection while being careful to preserve the privileged contents. The person asserting the privilege generally provides the following information in the privilege log for each document: the author or authors, the recipient or recipients, its date or dates, its length, the nature of the document or its intended purpose, and the basis for the objection. The privilege log is served on all other parties, who may then object to any asserted claims of privilege. The procedure for production of a privilege log and contesting its claims are more often found in case law than in the rules of civil procedure. Also, objections to discovery requests are made for a variety of reasons: the requested information exceeds the scope of permissible discovery; the time period that the request covers is too broad; the cost of search and retrieval of e-discovery information is too expensive and therefore should be borne by the requesting party; and the information is available on stored media that is simply too expensive or inaccessible to retrieve.

Step 7: Discovery Compliance Conferencing.

Good practice demands—and many local rules require—that discovery issues be discussed by counsel before presenting them to the court for resolution. Whether it is e-discovery or traditional discovery issues, this "meet and confer" practice helps narrow the area of dispute and may help reduce the cost of final compliance. Some courts also require the parties to formally meet in person and confer before filing Rule 37 motions.

Step 8: Seeking Sanctions.

Under Rule 37, the litigation team prepares and presents motions to the court to resolve outstanding e-discovery and other discovery compliance issues.

TECHNICAL AND ORGANIZATIONAL PROBLEMS AND SOLUTIONS FOR HANDLING E-DISCOVERY

In this electronic age, discovery—and specifically the discovery of electronically stored information (ESI)—is a tripartite problem involving information storage, data retrieval, and methods of production. Each part of the puzzle has its own problems and pitfalls, and the new lawyer must be knowledgeable about where data is stored, how it is retrieved, and how it can be produced in a cost-effective manner. The new advocate who gains this technological expertise becomes a valued member of the trial team. Keeping abreast of technological developments and emerging media trends is vital in this age of intensive electronic discovery.

It is also vital that while handling ESI, you ensure that attorney-client privilege is not lost through inadvertent disclosure of protected information. A reasonable effort to maintain privilege must be undertaken during production of ESI. It is

likely under FRE 502 that the court will find that the attorney-client privilege has not been lost even though documents may have been inadvertently disclosed, if the holder of the privilege has taken reasonable precautions to prevent disclosure and took reasonably prompt measures to rectify the release of the privileged information once aware of the disclosure.

Identifying all of the repositories of likely sources of information is a crucial step in undertaking the search for ESI. Repositories of electronically stored information include computers, file servers or other network interfaces, backup media, disks, tapes, CD/DVDs, flash drives, PDAs, cell phones, or other storage media. A thorough list of these storage media must be made—both for information you will be asked to produce and for information you are seeking from the opponent. It may be best to engage an IT expert, if your budget is sufficiently large, to ensure that crucial repositories are not overlooked.

Once you and your IT expert have established the likely repositories of information, it will be necessary to prepare your discovery requests and ensure that they are sufficiently encompassing to sweep in the necessary information to prove the case. Sampling is often used in searching repositories for ESI. It is used to test databases for the existence and amount of relevant information. Sampling helps finalize decisions about which repositories of data are likely to yield discoverable information and the likely effectiveness of such searches or other data extraction procedures.

In searching for ESI, your team must adopt a search methodology that will identify potentially relevant electronic documents reliably and efficiently. This task requires subject matter and technological and legal expertise, and it needs to be undertaken in close cooperation with your office IT specialist.

Keyword searches search for a term exactly as the search term specifies, so a keyword search will not pick up documents containing abbreviations or common misspellings. To locate such information, you'll need to perform additional keyword searches or fuzzy searches. Fuzzy searches are searches conducted for misspelled terms and concepts and are helpful in returning results when the original text has been corrupted through an optical character recognition error common in scanned documents. Boolean searches search for terms appearing in a specified relation to one another, usually with connectors like "and," "or," and "but not." Courts often accept as appropriate either or both search methodologies. Other search methodologies gaining in use are content-based searches, which identify and organize concepts into clusters, or concept-based searches. Clustering is a statistical analysis of ESI, which identifies relationships among documents that have similar content and clusters the identified information together. A concept search broadens a keyword-based search to include synonyms or related concepts.

Once information is found in the storage media, the method of production becomes the paramount issue. If there is only a little information in a readily available program, it can be loaded onto a flash drive, CD, or DVD at relatively little cost and provided to the opponent. That, however, is not often the case. While the cost of the search in work hours can be an expensive endeavor, the cost of retrieval on backup or stored media can be even more expensive, especially in a case involving voluminous information. If the information requires an expensive or hard-to-locate application in order to retrieve or view the information, then the cost of e-discovery increases. The court can order the sharing of expenses associated with e-discovery.

There are also software applications and ESI providers that help ease the burden of e-discovery. A good e-discovery program automates the discovery of information, thereby making large batches of electronic databases, documents, and e-mails easily accessible for search and review by attorneys. The software accelerates document processing, allowing users to gain immediate review of the facts; conduct e-discovery searches; group documents together by discussion threads and concepts; and receive comprehensive case management support. The following are some examples of programs and ESI support providers used by law firms and attorneys:

- Software programs like Kazeon, CommVault, Guidance, and i365 cover all of the stages of e-discovery and emphasize e-discovery and document management.
- Others, such as Assentor, Attenex, Autonomy, CaseLogistix, Cataphora, Stratify, and Zantaz, include advanced concept searching and analytics to streamline the review process.
- HardCopy Pro Plus is an application for data discovery, used in conjunction with retrieval systems to make large batches of electronic documents and e-mails easily accessible for searching and review.
- iLumin Software Services Assentor Discovery 2.0 is a tool for rapidly searching and producing e-mail messages. Assentor Discovery provides the ability to harvest archived information and manage and produce that information or preserve it for protection by the attorney-client privilege.
- Stratify Legal Discovery service is a full service ESI and e-discovery processing service; it culls the data universe and statistically analyzes terms and phrases, both within and across documents in responding to or reviewing responses to discovery requests.
- Williams Lea, Inc., is a national company that provides e-discovery services, reprographics, imaging, and digital processing services to law firms and attorneys.

- DiscoverReady LLC is a national provider of discovery management and document review services to Fortune 500 corporate legal departments.
- Fios is an electronic discovery services provider that manages every aspect of discovery response enabling collection, processing, review, and delivery of relevant documents in a predictable and legally defensible manner. Supported by Fios, DiscoveryResources.org is an online resource for law firms and litigation support professionals seeking current information about electronic discovery.
- Kroll Ontrack provides corporations, law firms, and government agencies with technology and consulting services for large-scale paper and electronic discovery, computer forensics, and litigation readiness and response projects.
- eClaris is an e-discovery consulting firm that assists law firms and corporations with classifying, processing, and reviewing their electronically stored data.

Concerned with the rising costs associated with e-discovery because of the serious burden it places on the judicial system, the Sedona Conference launched a national drive to promote open and forthright information sharing, training, and the development of practical tools to facilitate cooperative, collaborative, transparent discovery. The Sedona Conference is a good source of information on the latest trends in e-discovery. It is developing and distributing practical "toolkits" to train and support lawyers, judges, paralegals, and others in techniques of discovery cooperation, collaboration, and transparency. It is creating a clearinghouse of practical resources, including form agreements, case management orders, and discovery protocols.

Two particularly useful sources of information for "best practices" regarding the methodologies of searching are The *Sedona Conference's Best Practices Commentary on the Use of Search and Information Retrieval Methods in E-Discovery*[1] and the federal government's Text Retrieval Conference (TREC) Legal Track[2] initiative. The Legal Track at the Text Retrieval Conference assesses how effective the comparative search methodologies are at retrieving information. The TREC Legal Track was held for the first time in 2006 and is in the process of establishing objective benchmark criteria for comparing search technologies.

1. Available at http://www.thesedonaconference.org/content/miscFiles/Best_Practices_Retrieval_Methods___revised_cover_and_preface.pdf.
2. Available at http://trec.nist.gov/.

ESI TERMINOLOGY FOR THE NEW LAWYER

There are some fundamental terms that you must know when dealing with ESI:

- **Attachments.** These are electronic files appended to e-mails.
- **Backup.** Backup is the copied file that results from the activity of copying files or databases to preserve access to the information in case files are lost or corrupted due to operator error, equipment failure, or other problems. Most businesses and individuals create backups routinely. Backups are a source of locating discoverable information even when an attempt has been made to destroy the information.
- **Computer forensics specialist.** This is a computer investigation and analysis expert who searches for concealed or "lost" information that may be recovered from the computer. Computer forensic specialists use many methods to capture computer system data and recover deleted, encrypted, or damaged file information.
- **Computer network.** This is a series of computers connected to a server or host computer that stores files for access by other computers on the network.
- **Data filtering.** Data filtering is the process of identifying and extracting data based on specified limitations such as keywords, file types, dates, or names.
- **Deleted files.** File are deleted from an operating system for various reasons, but even deleted files can sometimes be recovered and restored to the computer.
- **E-mail thread or e-mail string.** This refers to e-mails linked together by e-mail responses and forwards.
- **E-discovery.** This is the search, retrieval, collection, review, and production of electronically stored information (ESI) in discovery. This includes all "soft copy" information, as opposed to paper copies, which are traditionally called "hard copy" material.
- **Electronically stored information (ESI).** These are files or other data that are stored on computers, file servers, disks, tapes, or other electronic devices or media.
- **File server.** A file server is a host computer that stores files for access by other computers on a network of computers.

- **Fuzzy search**. Fuzzy searches are searches conducted for misspelled terms and concepts. Fuzzy searches are helpful in returning results when the original text has been corrupted through an optical character recognition (OCR) error, which is common in scanned documents.
- **Harvesting**. Harvesting is the practice of retrieving electronic data from computers and other storage media.
- **IT specialist**. This Information Technology professional provides technical and consultative expertise in the support and coordination of computer hardware, software, information, technology services, and activities.
- **Legal hold**. A legal hold is a notice or communication from counsel that suspends the normal document retention policy, such as the deletion of old files and the disposition or processing of records like backup tape recycling.
- **Metadata**. Metadata is information about the characteristics, origins, or usage of an electronic file embedded in the file. This information is not visible when viewing a printed or on-screen rendition of the document. Metadata is either application metadata, which is information not visible on the printed page but embedded in the document file; or system metadata, meaning data stored externally on the computer file system.
- **Native file format**. These are electronic documents produced as originally maintained and used in the application.
- **Optical character recognition (OCR)**. This is the process of scanning images and electronically converting them into editable text.
- **Outlook**. Outlook is Microsoft's personal information management (PIM) program, which includes e-mail, task management, and calendar.
- **Portable document format (PDF)**. This format preserves the fonts, images, graphics, and layout of the source document in an electronic format. PDF files are viewed and printed with Acrobat, a viewer application available from Adobe Systems.
- **Privilege log**. A party produces a privilege log when objecting to a discovery request based on privilege or work product. The privilege log briefly describes each document that is protected by a claim of privilege or other protection while being careful to preserve the privileged contents.

- **PST file format.** File format used by the personal information management (PIM) program of Outlook, which includes e-mail, archived e-mails, task management ticklers, and a calendar.
- **Sampling.** Sampling is the process of testing a database for the existence or frequency of relevant information.
- **Spoliation of evidence.** Spoliation concerns the destruction, loss, or alteration of data or documents that could be evidence in litigation. Some jurisdictions have a separate cause of action for spoliation of evidence in addition to other remedies the litigants may invoke.
- **TIFF or TIF.** TIFF stands for Tagged Image File Format. This is an electronic copy of a document in the form of an image. TIFFs do not retain metadata from a source electronic document.[3]

DISCOVERY RULES FOR ELECTRONICALLY STORED INFORMATION

The Federal Rules of Civil Procedure recognize that much information is stored electronically, and the rules regulate the maintenance and discovery of ESI. This means that attorneys and clients must be thoroughly familiar with the obligation to retain and retrieve information created, stored, or in any way associated with a computer, whether presently involved in litigation or not. You must also know how to obtain ESI in the hands of your opponent. The advocate and client must also ensure that the company's e-mail and document retention policies do not conflict with the obligations of companies to preserve information. Obligations to protect electronic information reach beyond the rules of civil procedure and extend to counsel as evidenced by the indictment of a lawyer in Connecticut for violating the Sarbanes-Oxley Act, 18 U.S.C. § 1519, relating to the destruction, mutilation, or concealment of records for his role in dismantling his client's laptop. The attorney ultimately pleaded guilty to misprision of a felony.[4]

The modern Federal Rules of Civil Procedure for electronic discovery change little the discovery practices that most lawyers have engaged in for years. While there are additional obligations on counsel to educate clients and preserve information, and concomitantly additional expense, modern practice rules merely reflect how our business and social culture have changed because of the desktop computer. For many years now, the "smoking gun" in any case was more often found on an opponent's hard drive than in yesterday's hard-copy format. Business organizations have a near universal reliance on electronic records and good discovery practices

3. Lexbe, e-Discovery & Metadata Definitions, http://www.lexbe.com/hp/define-e-Discovery-meta-data.htm.
4. United States v. Russell, Docket No. 3:07-CR-00031, 2007 WL 4961124 (D.C. Conn. 2007).

recognize that practice. The Federal Rules of Civil Procedure simply reflect our growing reliance on ESI.

Lawyers must issue sufficiently encompassing requests for all relevant documents in both hard-copy and electronic "soft copy" requests. It is important to note that information received and produced in discovery may need to be put in a useable format with the applicable programs. Under the Rules of Civil Procedure and case law, the production of ESI is a cooperative endeavor, which may include the sharing of resources and costs.

CHECKLIST 8.1: YOUR ROLE COMPLYING WITH RULES REGARDING E-DISCOVERY

As a new attorney, you must ensure that you and the client

- Give early attention to issues relating to electronic discovery, including the form of production, preservation of information and problems reviewing electronic information for privilege.
- Make a diligent search for ESI while recognizing that the cost of searching for inaccessible electronic information may need to be addressed by the court.
- Are careful not to disclose privileged information that is stored electronically while recognizing that information inadvertently disclosed may retain protection if the privilege is asserted reasonably after the inadvertent disclosure.
- Work on an agreement regarding the form of production of electronic information or present the issue promptly to a judge for determination.
- Avoid court-imposed sanctions for the deliberate loss of electronic information. If you can show that the routine operations of computer systems, such as the automatic purging of stale e-mails caused the loss, then you may avoid potential sanctions.

The major rule requirements regarding the discovery of ESI are found in the requirements of Rules 16(b) and 26(f), pertaining to counsel's obligation to meet and confer; Rule 26(b)(2), regarding the duty of disclosure; Rule 26(b)(5), relating to privilege claims; Rule 34, concerning the different forms of production; and Rule 37, and its safe harbor provisions; as well as sanctions, for the loss of certain ESI.

Many district courts have local rules addressing electronic discovery; therefore, it is especially important to review these rules as you undertake discovery. Some courts

have fashioned sample discovery plans that you should review and get guidance as to how you would like to proceed. Many of these sample discovery plans include provisions for electronic information disclosures. These discovery plans often require the *parties to provide a brief description of their proposals regarding the disclosure or discovery of electronically stored information, identify any disputes regarding the same, and include a proposed order.*

FIGURE 8.1: SAMPLE DISCOVERY PLAN

The United States District Court for the District of New Hampshire offers the following sample discovery plan on its Web site:[5]

UNITED STATES DISTRICT COURT
DISTRICT OF NEW HAMPSHIRE

Plaintiff(s)	)	
v.	)	Civil No. Case #
	)	Judge Initials _____
Defendant(s)	)	

DISCOVERY PLAN

FED. R. CIV. P. 26(F)

DATE/PLACE OF CONFERENCE:

COUNSEL PRESENT/REPRESENTING:

CASE SUMMARY

THEORY OF LIABILITY:

THEORY OF DEFENSE:

DAMAGES:

DEMAND:

due date [need not be filed with the court]

5. Available at http://www.nhd.uscourts.gov/ru/form-samplediscoveryplan.asp.

OFFER:

due date [need not be filed with the court]

JURISDICTIONAL QUESTIONS:

QUESTIONS OF LAW:

TYPE OF TRIAL:

jury or bench

DISCOVERY

TRACK ASSIGNMENT:

EXPEDITED—6 MONTHS
STANDARD—12 MONTHS
COMPLEX—24 MONTHS

DISCOVERY NEEDED:

Give brief description of subjects on which discovery will be needed.

MANDATORY DISCLOSURES (FED. R. CIV. P. 26(A)(1))

Advise the court whether the parties have stipulated to a different method of disclosure than is required by Fed. R. Civ. P. 26(a)(1) or have agreed not to require any Rule 26(a)(1) disclosures.

ELECTRONIC INFORMATION DISCLOSURES (FED. R. CIV. P. 26(F))

The parties should provide (a) a brief description of their proposals regarding the disclosure or discovery of electronically stored information (and/or attach a proposed order) and/or (b) identify any disputes regarding the same.

STIPULATION REGARDING CLAIMS OF PRIVILEGE/PROTECTION OF TRIAL PREPARATION MATERIALS (FED. R. CIV. P. 26(F))

The parties should provide a brief description of the provisions of any proposed order governing claims of privilege or of protection as trial preparation material after production (and/or attach a proposed order).

COMPLETION OF DISCOVERY:

(1) Date all discovery complete [approximately 60 days prior to trial date according to Track] (2) If there are issues for early discovery, date for completion of discovery on those issues.

INTERROGATORIES:

A maximum of *(number)* [presumptive limit 25] interrogatories by each party to any other party. Responses due 30 days after service unless otherwise agreed to pursuant to Fed. R. Civ. P. 29.

REQUESTS FOR ADMISSION:

A maximum of *(number)* requests for admission by each party to any other party. Responses due 30 days after service unless otherwise agreed to pursuant to Fed. R. Civ. P. 29.

DEPOSITIONS:

A maximum of *(number)* [presumptive limit 10] depositions by plaintiff(s) and *(number)* [presumptive limit 10] by defendant(s).

Each deposition (other than of /name\) limited to a maximum of *(number)* [Presumptive Limit 7] hours unless extended by agreement of the parties.

DATES OF DISCLOSURE OF EXPERTS AND EXPERTS' WRITTEN REPORTS AND SUPPLEMENTATIOS:

Plaintiff:
due date

Defendant:
due date

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

Advise the court whether the parties have stipulated to a different form of expert report than that specified in Fed. R. Civ. P. 26(a)(2).

CHALLENGES TO EXPERT TESTIMONY:

due date: [no later than 45 days prior to trial]

OTHER ITEMS

JOINDER OF ADDITIONAL PARTIES:

Plaintiff:
due date

Defendant:
due date

THIRD-PARTY ACTIONS:

due date

AMENDMENT OF PLEADINGS:

Plaintiff:
due date

Defendant:
due date

DISPOSITIVE MOTIONS:

To Dismiss:
due date [no later than 90 days after preliminary pretrial]

For Summary Judgment:
due date [no later than 120 days prior to trial date according to Track]

SETTLEMENT POSSIBILITIES:

1. is likely
2. is unlikely
3. cannot be evaluated prior to (date)
4. may be enhanced by ADR:
   a. Request to the court
   b. Outside source

JOINT STATEMENT RE MEDIATION:

The parties shall indicate a date by which mediation, if any, will occur.

WITNESSES AND EXHIBITS:

[No dates necessary; due dates—10 days before final pretrial conference but not less than 30 days before trial for lists (included in final pretrial statements) and 14 days after service of final pretrial statement for objections—set by clerk's notice of trial assignment.]

TRIAL ESTIMATE:

number of days

TRIAL DATE:

The parties shall set out an agreed trial date–adhering to time periods as mandated by the chosen track assignment—using a preset jury selection day as provided on the court's Web site (www.nhd.uscourts.gov). If the parties cannot agree on a date, they shall set out their respective proposed dates.

PRELIMINARY PRETRIAL CONFERENCE:

The parties [request] [do not request] a preliminary pretrial conference with the court before entry of the scheduling order. [NOTE: The parties should plan to attend the preliminary pretrial conference as scheduled unless otherwise notified by the court.]

OTHER MATTERS:

The parties should list here their positions on any other matters which should be brought to the court's attention including other orders that should be entered under Fed. R. Civ. P. 26(c) or 16(b) and (c).

The state courts, through the Conference of Chief Justices, have also been proactive in dealing with e-discovery issues. The Conference of Chief Justices has adopted guidelines similar to the practices in federal court for state courts to use in considering issues related to e-discovery. Those guidelines can be obtained from the National Center for State Courts' Web site, which is www.ncsconline.org.

Finally, the lawyer and client must work closely to deal with issues relating to the search, maintenance, and retrieval of ESI to avoid costly sanctions and adverse

judgments that are likely to occur for failing to follow proper protocol for ESI. Both Rule 37 and civil actions for spoliation of evidence are used to compensate for the loss of important evidence. In *Zubulake v. UBS Warburg LLC*[6], the landmark case for e-discovery production and cost-sharing criteria, a former employee was ultimately awarded a $29 million verdict on her discrimination claim. After many disputes regarding the production of ESI, at trial the court gave a jury instruction on spoliation, directing jurors to presume that certain e-mails that the defendant never produced would have contained information detrimental to the defendant. Also, in *U.S. v. Philip Morris,*[7] the court imposed nearly $3 *million* in sanctions against Philip Morris for e-discovery violations. As an additional sanction, the court also precluded Phillip Morris from calling certain witnesses in its defense. District court actions for spoliation of evidence claims exist in many states, including California, Pennsylvania, and New Jersey.[8]

In conclusion, attorneys must counsel clients carefully on compliance issues regarding the storage and retrieval of ESI. Attorneys must also become thoroughly familiar with the business and ESI practices of their clients. Attorneys must be knowledgeable about information systems and emerging media trends so that information can be disclosed and effectively organized and retrieved. Attorneys and clients must work together to practice preventive law. In good faith, attorneys must help clients develop standard procedures for retaining and purging information and recycling media that are consistent with sound business practices, develop systems to segregate privileged and confidential information, and develop a comprehensive plan to educate the client's employees on responsibilities for use and storage of electronic information.

KEY TERMS	
attachments	discovery compliance and privilege
backup	discovery sources
compliance conferencing	e-discovery
computer forensics specialist	e-discovery plans
computer network	e-discovery retrieval
data filtering	e-discovery searches
deleted files	

6. Zubulake v. UBS Warburg, LLC, 229 F.R.D. 422 (S.D.N.Y. 2004).
7. U.S. v. Philip Morris, 327 F. Supp. 2d 21 (D.D.C. 2004).
8. 19 COA 2d 249 (2008).

KEY TERMS	
electronically stored information (ESI)	native file format
e-mail string	optical character recognition
file server	Outlook
fuzzy searches	portable document format
harvesting	privilege log
initial disclosures	PST file format
IT specialist	sampling
key concept searches	sanctions
key term searches	search methodology
legal hold	Spoliation of Evidence
metadata	TIFF

DISCUSSION QUESTIONS

1. What are some of the key terms, programs, software, and technological advances dealing with ESI that new lawyers must be familiar with?
2. What are some of the key tasks that they new lawyer must undertake in ESI matters?
3. What are some best practices that new lawyers should employ when dealing with ESI?
4. What are some key tips to keep in mind regarding compliance with the rules on e-discovery?

ELECTRONIC DISCOVERY DRIVEN AMENDMENTS TO THE FEDERAL RULES OF CIVIL PROCEDURE- EFFECTIVE DECEMBER 1, 2006

Rule 16(b)(5) & (6):

- Enables the court to provide in the scheduling order for the disclosure and discovery of electronically stored information and parties' agreements for claims of privilege or of protection as trial-preparation material after production.

Rule 26(a):

- Obligates parties to include descriptions of electronically stored information in their initial disclosures.

Rule 26(b)(2):

- Codifies a balancing test for the production of electronic discovery where a party claims the information is not reasonably accessible.

- Court will consider the undue burden or cost to the producing party, the likely benefit of the information sought and whether good cause exists for its production.

Rule 26(b)(5)(B):

- Establishes a system for parties to preserve privilege in instances where discovery material, electronic or otherwise, is inadvertently produced.

- The party notified of the inadvertent disclosure must promptly return, sequester or destroy the specified information and may not use it until the privilege claim is resolved.

Rule 26(f)(3) & (4):

- Obligates parties to discuss issues relating to disclosure or discovery of electronic information at the discovery planning meeting as well as procedure for claims of privilege or of protection as trial-preparation material.

Rule 33(d):

- Incorporates electronic documents into rule permitting parties to make available records for inspection and copying where the burden of ascertaining the answer to an interrogatory is substantially the same for the party serving the interrogatory as for the party served.

Rule 34:

- Authorizes parties to engage in electronic discovery and to request production of electronic data in a particular format, subject to objection by the producing party.

- Unless otherwise requested or ordered, parties must produce information in the form in which it is ordinarily maintained or that is reasonably usable.

Rule 37:

- Establishes narrow safe harbor from discovery sanctions for parties that that fail to produce electronic information which has been destroyed as a result of the routine, good faith operation of their information systems.

- Courts' finding of "good faith" requires showing that parties took steps to implement effective and appropriate litigation holds to preserve the relevant data.

Rule 45(a)(1)(C) & (2)(C), (c)(2)(A) & (B), and (d)(1)(B)-(D) & (2)(b):

- Enables parties to obtain electronic information from third parties by use of subpoena and establishes the same rules and standards of discovery for electronic information as set forth in Rules 33 and 34.

ELECTRONIC DISCOVERY AND RECORD'S RETENTION CHECKLIST

THE SEVERE CONSEQUENCES OF THE FAILURE TO PRESERVE ELECTRONIC EVIDENCE

- In Re Prudential Insurance Company of America Sales Practices, 169 F.R.D. 598 (D. N.J. 1997).
The court ordered various sanctions against Prudential including the payment of a $1 million fine to punish Prudential for the loss of evidence resulting from its "haphazard and uncoordinated" approach to document retention. The court sanctioned Prudential for failing to institute a comprehensive document preservation plan and distribute it to all employees, and failing to advise employees of all the potential sanctions for not complying with the court's document preservation order.

- USA v. Philip Morris USA, Civil Action No. 99-2496 (D. D.C. July 21, 2004).
The Court ordered the defendant to pay a monetary ...alty of $2.75 million because it continued to delete ...ils as part of its routine document destruction policy for two years after the court ordered the retention of documents pertaining to the litigation. Company executives failed to routinely print and preserve relevant emails, as required. The court found that the company acted with "reckless disregard and gross indifference" warranting severe monetary sanctions. The court further sanctioned the defendant by precluding one of the defendant's key witnesses from testifying at trial.

- Leon v. IDX Sys. Corp., 2006 WL 2684512 (9th Cir. Sept. 20, 2006)
The court dismissed a wrongful termination claim and fined the plaintiff $65,000. A computer forensics expert determined that the plaintiff deleted files from his employer-issued laptop in violation of the employer's attorney's request that he preserve all data on his laptop.

- Metropolitan Opera Ass'n, Inc. v. Local 100, Hotel Employees and Restaurant Employees International Union, et al., 212 F.R.D. 178 (S.D. N.Y. 2003)
The court entered a default judgment against the defendant because it failed to conduct a reasonable investigation into whether there were electronic documents responsive to discovery requests, failed to prevent the destruction of documents, failed to instruct proper personnel as to the requirements of ...ument collection, and allowed computers to be replaced immediately before an on-site inspection.

	ASAP/Pre-Litigation	Litigation Contemplated	During Litigation	Post-Litigation
Operations				
Familiarize yourself with operations, including information systems	√			
Determine types of information maintained	√			
Determine how information is stored	√			
Determine how information can be retrieved	√			
Consider costs of retrieval	√	√		
Research cost of past restoration attempts	√			
Document Retention				
Develop document retention policy	√			
Ensure that document retention policy includes electronic information	√	√	√	√
Implement document retention policy	√			√
Monitor document retention policy and ensure compliance	√	√	√	√
Educate employees regarding document retention policy, the purpose of the policy and the important of complying with the policy	√	√	√	√
Develop plan for suspension of document retention policy	√			
Information Systems - Operations				
Familiarize yourself with operations, including information systems	√			
Develop formalized backup protocol for information systems, including all electronic information	√			
Implement backup protocol for information systems	√			√
Monitor backup protocol and ensure compliance	√	√	√	√
Develop plan for suspension of backup protocol, including for suspension of backup take recycling	√			
Information Systems - Personnel				
Designate key personnel, including information systems personnel, for maintaining information regarding electronic information	√			
Designate key personnel for maintaining information regarding document retention policy	√			
Designate key personnel, including information systems personnel, for maintaining information regarding backup protocol	√			
Educate information services contact regarding types of information ordinarily requested during discovery process	√	√	√	√
Designate and prepare information systems personnel contact to act as 30(b)(6) deposition witness, if necessary	√	√		
Educate information services personnel regarding document retention policy, backup protocol and procedures for suspending each	√	√	√	√
Request that information services maintain inventory of systems and software, including obsolete and/or no longer used systems and software	√	√	√	√
Request that information services document all installations, changes, modifications, upgrades and patches of all hardware and software	√	√	√	√
Request that information services maintain inventory of stored information	√	√	√	√
Request that information services establish systems to simplify and organize identification, retrieval and production of electronic information	√			
Working with Legal Counsel				
Inform legal counsel whenever litigation is contemplated or anticipated		√		
Immediately inform legal counsel whenever notice of litigation is received		√		
Review and distribute litigation preservation and/or litigation hold correspondence		√		
Monitor compliance with litigation preservation and/or litigation hold requests		√	√	√
Implement suspension of document retention policy		√		
Monitor suspension of document retention policy		√	√	√
Implement suspension of back up protocol		√		
Monitor suspension of back up protocol		√	√	√