WHAT DOES E-DISCOVERY HAVE TO DO WITH RECORDS RETENTION & COMPLIANCE PROGRAMS?

- Martin J. Jaron, Jr., Partner
- Suzanne Foster, Associate
HOLLAND & KNIGHT LLP
&
- Glenn Martin, Chief Internal Audit & Compliance Officer
EASTERN MAINE HEALTHCARE SYSTEMS

"The future ain't what it used to be."

Yogi Berra
E- Documents -
It’s not a paper world anymore.

• 93% of all information is now generated in electronic form
• 70% of these documents are never reduced to hard copy


Everyone knows “Where’s Waldo?”
Here’s a Much More Difficult Game: Where’s Waldo’s ESI?
So, where is Waldo’s ESI?

ESI ("electronically stored information"), the term used in the new Electronic Discovery Amendments to the Federal Rules of Civil Procedure, is everywhere and can include:

- Email – Outlook & Other Programs
- Word, Excel, Access, PowerPoint similar programs
- Company proprietary or customized programs (e.g., Oracle database; SQL Server database; SAP & other custom business applications; specialized accounting programs, etc.)
- Mainframe systems
- Network servers for email, documents, databases, other materials
- Desktop & laptop computer hard drives
- Home computer hard drives – common when employees work from home on non-company computers
- Third-party email providers (GMail, Yahoo, Hotmail, etc.)

Where else is Waldo’s ESI?

- Backup tapes and other storage media
- Abandoned servers and drives
- Voicemail systems
- Instant messaging systems
- Copier memory
- Fax machine memory
- Blackberries or PDA’s
- Cell-phones – for call times, phone locations, text messages
- Portable devices (memory sticks, flash drives, CF, SD, Mini-SD, CRDW, DVD, etc.)
- I-POD’s – and now I-Phones too
- GPS devices
- Many other sources – even viruses can carry data!
What About Waldo’s RAM?

• May 29, 2007 ruling from USDC in Los Angeles, California holding that transient RAM is now discoverable from TorrentSpy as potentially relevant to claims of copyright infringement and therefore must be preserved.

• Decision is on appeal, but if upheld this has implications for civil cases generally and would be a revolutionary change in preservation obligations and breathtaking increase in e-discovery costs.

*Columbia Pictures Industries v. Justin Bunnell, et al., Case No. CV-06-1093 FMC(JCx) (USDC-CD Cal.)*

Are Waldo’s electronic files discoverable?

• Waldo should not write anything he does not want to see on the front page of The Washington Post.

• In litigation today, smoking gun electronic documents are the key to unlock many cases.

• Every day brings new email disclosures, whistle blowing has now become electronic.

• Illusion of privacy: smaller screen, more privacy [computer, Blackberry, cell phone text message]

• Reality: none of it is private, everything is discoverable
Network Topology: Creating a Data Map

Backup Tapes: The Great Equalizer

Yes, now we have to know what’s on them.
“You Say You Want A Revolution. . .”

- Discovery in litigation has undergone a truly revolutionary change from paper to electronic files.
- Change was gradual, accelerating over past 10 years to become part of most litigations.
- FRCP E-Discovery amendments – Federal Rules have recognized and caught up to changes and states will likely soon follow.
- Not another Y2K. Can’t ignore it, can’t live in a paper world anymore.
- Profound and permanent change in the way litigation discovery is conducted.

The New Federal E-Discovery Rules
New E-Discovery Amendments to Federal Rules of Civil Procedure:

Copy of E-Discovery Amendments - attached in your materials

• **Effective date:** December 1, 2006

• **Rule 16(b),** allows court to establish rules for disclosure, privilege, methods of production and work product prior to commencement of electronic discovery

• **Rule 26(a),** adds “electronically stored information” (ESI) as own separate category of document subject to discovery

• **Rule 26(b)(2),** sets up two tier discovery for *accessible* and *inaccessible* data; provides procedures for cost shifting on inaccessible data

---

New E-Discovery Amendments to Federal Rules of Civil Procedure:

• **Rule 26(b)(5),** clarifies procedures when privileged ESI is inadvertently sent to requesting party to allow “clawback” of privileged information

• **Rule 26(f),** requires parties/attorneys to meet 21 days before Court scheduling conference to discuss discovery plan, including any issues relating to disclosure or discovery of ESI, including the form or forms of production – ADVANCE PREPARATION REQUIRED!!

• **Note on forms of Production:**
  1. Native format, with or without metadata
  2. Quasi-native (large databases)
  3. Quasi-paper (ESI converted to TIFF or PDF image files)
  4. Paper
New E-Discovery Amendments to Federal Rules of Civil Procedure:

- **Rule 33(d)**, includes ESI as part of the business records related to interrogatories to parties
- **Rule 34(b)**, establishes protocols for form of production, requesting party gets to choose form of production (including native files & metadata)
- **Rule 37(f)**, provides limited “safe harbor” when electronic evidence is lost or destroyed as a result of the routine, good-faith operation of an electronic information system
- **Rule 45**, document subpoenas to third-parties now include ESI as a document
- **Form 35**, requires discovery plan to include how ESI will be handled

Focus on Rule 37 – “Safe Harbor” Provision

**Rule 37** – Failure to Make Disclosure or Cooperate in Discovery; Sanctions

- provides limited protection against sanctions for a party’s inability to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system

**Beware** – The so-called “safe harbor” is illusory and not much of a safe harbor at all; a watered down version of the original proposal

**But** – if you have strong records management and compliance programs, you have an edge in showing “good faith” if documents are destroyed accidentally
"If you don't know where you are going, you might wind up somewhere else."

Yogi Berra

E-Discovery Process

Industry accepted flow chart describing the e-discovery process

Source: George Socha Consulting LLC
E-Discovery & Records Management

• A strong electronic data discovery readiness program ...
• Requires a strong records management program
• New Federal Rules highlight the value of established records management practices
• Litigation holds – always a part of a comprehensive records management program, and now much more important because of severe sanctions for failure to preserve e-documents and permitting spoliation of evidence

USDC-MD, Suggested Protocol For Discovery of ESI
- Introduction

• Note: the USDC-MD Protocols are included as an attachment in your materials – important and well worth time to review
• USDC-MD Protocols are the most detailed U.S. District Court guidelines for handling ESI under new Federal Rules
• Other courts are adopting similar guidelines (USDC, ND-Ohio)
• Some federal courts are simply relying upon the USDC-MD Protocols, recognizing their comprehensive and thoughtful structure
• State courts are not far behind - See Guidelines For State Trial Courts Regarding Discovery of Electronically Stored Information, Conference of Chief Justices, August, 2006 (attached)
USDC-MD, Suggested Protocol For Discovery of ESI
- Blueprint for ESI Records Retention Program

• The information called for in these guidelines is information that should now be gathered and maintained as part of company’s records retention, records management & compliance programs.

• Best practice: review your internal ESI records management and compliance programs to include the ESI information called for in the Protocols.

• Best practice: review the litigation hold component of your records management program to make sure it is comprehensive, includes the material identified in the Protocols, and has adequate implementation and follow-up procedures.

Holland & Knight

------------------------

USDC-MD, Suggested Protocol For Discovery of ESI
- Rule 26(f) Conference Preparation

• Conference of Parties is encouraged prior to Rule 26(f) Conference

• Topics to be discussed at conference of parties and 26(f) Conference include

• Identification of one or more IT personnel to act as ESI coordinator

• Become familiar with client’s current and past ESI, and identify person with knowledge to participate in Rule 26(f) Conference

Holland & Knight
USDC-MD, Suggested Protocol For Discovery of ESI - The Litigation Hold Description (Part I)

• Scope of the Litigation Hold
• Determination of categories of potentially discoverable information
• Discussion of issues in the case, including whether ESI is relevant
• Identification of “key persons”
• Relevant time period for litigation hold

USDC-MD, Suggested Protocol For Discovery of ESI - The Litigation Hold Description (Part II)

• Analysis of what ESI needs to be preserved (types of data, Meta-Data, deleted data, fragmented data)
• Paper documents that are exact duplicates of ESI
• Preservation of ESI that has been deleted but not purged
• Determine where ESI subject to Litigation Hold is maintained
• Distribution of the Litigation Hold
• Instruction to be included in the Litigation Hold notice
• Monitoring Compliance with the notice of Litigation Hold
Records Management & Compliance: The Keys To An Effective E-Discovery Program

- Thoughtful records management, records retention, and compliance programs are the foundation of a solid e-discovery program.
- Litigation Hold component of records management program is now more important than ever.
- You can achieve e-discovery readiness through records management & compliance.
- When? Too late after the litigation starts.
- How much? Much more expensive after the litigation starts.

Holland+Knight

MOTIVATION: A Cautionary Tale for Compliance Officers & Litigators

- Duty to preserve applies to litigation and investigations and audits
- Government audits and investigations can be parallel civil and criminal
- Potential sanctions more than just money and adverse inferences
- IMPORTANT: violations can lead to Obstruction of Justice and False Statements charges

Holland+Knight
MOTIVATION: A Cautionary Tale (Continued)

- Government Investigations:
  - Frequently begin with demand for production of records, including e-records
  - Include demand for preservation
  - Even inadvertent destruction viewed with suspicion
  - “Adverse Inferences” can lead to civil and criminal fraud cases

Failure to Locate and Preserve Data

- Phillip Morris sanctioned for spoliation and ordered to pay $2,750,000 plus costs
  - Despite a document preservation order, Phillip Morris continued to delete emails after 60 days (per their normal protocol) on a monthly system-wide basis for two years after the order was issued.
  - Phillip Morris waited for over four months after learning it had not suspended automatic deletion of emails before notifying the court and adversary, and continued automatic deletion for two months even after learning of problem
  - 11 key personnel, including an expert, were precluded from testifying at trial since they had not abided by the document preservation order.

**Zubulake v. UBS Warburg**

- The Zubulake V Court granted sanctions and costs to the plaintiff after determining that UBS Warburg had willfully deleted relevant emails despite a document preservation order to the contrary.

- The Court also noted that defense counsel was partly to blame for the document destruction because it had failed in its duty to locate the relevant information, to preserve the information and timely produce it.


**Don’t Forget to Look in the Closet**

- Morgan Stanley failed to locate 1,423 DLT backup tapes in a Brooklyn facility.

- Despite SEC regulation requiring two year email retention, Morgan Stanley overwrote emails and failed to notify and timely process hundreds of backup tapes, email attachments and emails.

- The court granted the plaintiff’s motion for an adverse inference instruction to the jury, noting that “[t]he conclusion is inescapable that [the defendant] sought to thwart discovery.”

- Morgan Stanley was penalized $1.45 billion due to adverse inference instruction.

E-Discovery: Defense of Process Is Critical

- An operating records management program makes defense of e-discovery process easier, and helps to show good faith and absence of bad faith if documents are accidentally destroyed.
- Important to document each step of the process.
- Show all steps taken were reasonable to preserve documents, including timing.
- Show why key employees are the appropriate and the only employees likely to have documents.
- Document conversations with IT and key employees because information from these sources are the basis for the reasonable steps taken.

New Rule 37(f) Safe Harbor

- Sanctions not imposed for the loss of records, if the loss resulted from:
  - The routine, good faith operation of
  - An electronic information system
- The key to this Safe Harbor (whatever its scope) is: **an operating records management system**
How Can A Records Management Program Make E-Discovery Easier?

• Records management means a comprehensive program for the retention, retrieval and management of records needed by the company; and

• Destruction of records not needed or used by the company.

• Records management reduces the volume of records that must be searched when litigation begins.

• Records management reduces the possibility that sanctions will be imposed for failure to preserve or for spoliation of evidence.

Who Has Control of Client’s Relevant Data?

• Rule 34 - must preserve all relevant documents in client’s “possession, custody or control.”

• This means if the party has actual possession, custody, or control, or the legal right to obtain the documents on demand.

• Depending on jurisdiction, this may also mean practical ability to obtain the documents from another, irrespective of legal entitlement to the documents.

• Parent (and even “grandparent”) corporations have sufficient ownership and control over wholly-owned subsidiary.

• Branch or subsidiary in another state/country are within a party’s control.
Records Management Programs In Context

- Control creation, volume and location of information
- Preserve critical business records
- Reduce storage costs
- Efficient access to information
- Increase productivity
- Protect corporate history and memory
- Reduce potential exposure to regulators and adverse litigants

ETHICS RULES AND E-DISCOVERY
Lawyers, Including In-House Counsel, Have An Ethical Duty To Preserve Electronic Evidence

The ethics rule relevant to the preservation of emails and other electronic data is ABA Model Rule 3.4 (and in Code States DR 7-102).

Rule 3.4 makes it unethical to unlawfully obstruct another party’s access to evidence or otherwise unlawfully alter, destroy, or conceal a document or other material that the lawyer knows or reasonably should know is relevant to a pending or reasonably foreseeable proceeding; nor may a lawyer counsel or assist another person to do any such act.

The Rule applies to evidentiary material generally and includes computerized information.

The comments to the Rule explain:

Documents and other items of evidence are often essential to establish a claim or defense. [T]he right of an opposing party . . . to obtain evidence through discovery or subpoena is an important procedural right. The exercise of that right can be frustrated if relevant material is altered, concealed, or destroyed. Applicable law in many jurisdictions makes it an offense to destroy material for the purpose of impairing its availability in a pending proceeding or one whose commencement can be foreseen. (Emphasis supplied.)
**Spoliation**

Spoliation is the destruction or material alteration of evidence in pending or reasonably foreseeable litigation. While violation of Rule 3.4, or spoliation, subjects a lawyer to discipline, it can also be the basis for courts taking corrective action through litigation sanctions.

Sanctions for spoliation have included:

1. The imposition of fines, costs and attorneys fees
2. Exclusion of evidence
3. An adverse inference instruction to the jury
   
   An adverse inference instruction can and often will end the case. Obviously, when a judge gives an instruction that the jury may infer that the party who destroyed emails did so out of the realization that the emails were unfavorable, the instruction is likely to devastate the case of the party believed to have destroyed the email.

4. Worst case: default judgment

**The Court will consider the following questions before giving an adverse inference instruction.**

1. Did the party who controlled the evidence have an obligation to preserve?
2. Was the act of destruction knowingly done?
3. Was the destroyed evidence relevant to the claims or defenses being advanced?
A Court’s finding of intent becomes important. Was the destruction the result of -

1. Bad faith
2. Gross negligence
3. Ordinary negligence

The more culpable the state of mind, the less proof needed to show the relevance of the destroyed documents.

In Re Sept. 11th Liability Insurance Cases

• Important recent decision issued June 20, 2007 in the SDNY imposing $1.25 Million in sanctions against Zurich & its two law firms, jointly & severally, under Rules 11 and 37 for destroying key policy documents related to insurance coverage. Electronic copies of documents were intentionally deleted. The court imposed $750,000 in sanctions under Rule 11, and another $500,000 for Rule 37 for failing to meet discovery obligations under Rule 26, stating that the Rule 37 violations compounded the Rule 11 violations.

In Re Sept. 11th Liability Insurance Cases, Opinion & Order Granting Sanctions For Discovery Abuses, 03 Civ. 322 (AKH) (USDC-SDNY)(June 20, 2007)
An Ounce of Prevention . . . .
1. Focus at the very outset on what evidence must be preserved and how – use written litigation hold letters.
2. Know the "trigger date" and make sure your client knows it too.
3. Identify the "key players."
4. Make sure the company and the individual key players in the matter understand their duties to preserve. Do not rely on in-house counsel to communicate these duties to other key players.
5. Make sure you talk to the people who created the e-documents and the client’s IT personnel so that you get the complete picture. Normally, neither group understands the other and this is a problem to be overcome in exercising litigation holds and making sure preservation obligations are met. This requires intense initial work, plus frequent follow-up.
6. Make sure your client is fully aware of how courts interpret the duty to preserve evidence.
7. Address how you are going to deal with privilege issues in the early stages of document review.

A/C Privilege and Waiver Issues
1. Privilege review of a large volume of electronic documents is difficult, time-consuming and expensive.
2. State law varies on what causes a waiver due to inadvertent disclosure. In some states, an inadvertent disclosure is a complete waiver of the privilege; in other states, the view is that so long as the client and/or the lawyer was diligent in efforts to prevent disclosure, no waiver occurs.
3. New Rule 26(f)(4) allows parties to negotiate concerning waiver of the privilege by inadvertent disclosure –
   - Sneak a peek
   - Claw back
4. Keep in mind third-party issues (e.g., the party who next litigates against the client). Third parties may not be bound by waiver agreements to which they were not parties.
Conclusion

“It is not the strongest of the species that survive, nor the most intelligent, but the ones most responsive to change.”

Charles Darwin