Best Practices
Information Acquisition
And Preservation

Presented by:
Woods Abbott & Eric Schwarz
January 17, 2008
Fordham Law School
Presentation Road Map

- Changing Environment
  - New Rules, New Benchmarks
- Strategic Planning: Before Litigation
  - Know Where The Information Is
  - What You Keep, What You Don’t
  - Common Pitfalls, Successful Strategies
  - Pre-Litigation Readiness
- When Litigation is “Reasonably Anticipated”
  - Triggering Mechanisms
  - Duty to Preserve – The Litigation Hold
  - Implementing the Hold
E-Discovery: Intersection Of Law And Technology
Changing Environment
ESI Preservation And The Amended Federal Rules

- Early and comprehensive consideration of ESI – Rule 26(f)
- Identifying and disclosing “inaccessible” data – Rule 26(b)(2)(B)
- Risks of waiving attorney client privilege or privacy rights and forfeiting confidentiality – Rule 26(b)(5)
  - Proposed Rule of Evidence 502
- Producing in the proper form (metadata) – Rule 34(b)
- The burden of tiered production without tiered preservation
- Limited safe harbor – Rule 37
New Expectations And Benchmarks

- Duty to preserve arises when litigation is “reasonably anticipated”
- Preservation efforts must be continuously monitored throughout litigation
- Both attorney and client share the duty
- Duty to preserve may extend to home computers and other personal devices, email accounts, information held by third parties
- Cost burden and cost shifting
- Preservation efforts must be defensible to the court and opposing parties
Strategic Planning:
Before Litigation
Privileged and Confidential Attorney Client and Attorney Work Product Privileges Apply

Records And E-Discovery Life Cycle

Records Life Cycle
- Create/Receive/Retrieve (Identify)
- Archival Preservation
- Distribute/Use (Classify)
- Retention & Disposition
- Storage & Maintenance

E-Discovery Life Cycle
- Risk Management
  - Identification
  - Collection
  - Review
  - Analysis

- Cost Containment
  - Processing
  - Production

= Meet and Confer
= Motion Practice
= E-Discovery Coordination Counsel

Records Life Cycle

E-Discovery Life Cycle

Archival Preservation
Distribute/Use (Classify)
Retention & Disposition
Storage & Maintenance

Identification
Collection
Review
Analysis

Processing
Production
## Industry Insights

<table>
<thead>
<tr>
<th>Common Pitfalls</th>
<th>Successful Strategies</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Technology</strong></td>
<td></td>
</tr>
<tr>
<td>Inadequate electronic information inventory</td>
<td>▪ Centralize electronic information repositories</td>
</tr>
<tr>
<td></td>
<td>▪ Identify data sources at risk of discovery</td>
</tr>
<tr>
<td><strong>People</strong></td>
<td></td>
</tr>
<tr>
<td>No central coordination of discovery requests</td>
<td>▪ Discovery Response Team comprised of IT, Business, and Legal</td>
</tr>
<tr>
<td></td>
<td>▪ Discovery Liaison</td>
</tr>
<tr>
<td><strong>Process</strong></td>
<td></td>
</tr>
<tr>
<td>Legal Holds preserve too much or too little</td>
<td>▪ Prioritize business lines with high discovery risk</td>
</tr>
<tr>
<td></td>
<td>▪ Develop data preservation plan</td>
</tr>
<tr>
<td></td>
<td>▪ Procedures to communicate and monitor success of preservation plan</td>
</tr>
</tbody>
</table>
### Planning The E-Discovery Life Cycle

#### Project Management/Quality Controls/Global Methodologies

<table>
<thead>
<tr>
<th>Strategies</th>
<th>Identify/Preserve</th>
<th>Collect</th>
<th>Process</th>
<th>Review</th>
<th>Produce</th>
</tr>
</thead>
<tbody>
<tr>
<td>➢ Define Policies, Protocols, Governance</td>
<td>➢ IT Interviews: Who, What, Where, How</td>
<td>➢ Define Defensible Collection Options</td>
<td>➢ Stage Data for Processing</td>
<td>➢ Establish Review Team</td>
<td>➢ Export Relevant Set</td>
</tr>
<tr>
<td>➢ Design Legal Hold Procedures</td>
<td>➢ Identify Preservation Requirements; Assess Current Protocols</td>
<td>➢ Document and Implement</td>
<td>➢ Perform File Analysis to Identify User Documents (vs. System Files, etc.)</td>
<td>➢ Identify Review Protocols and Objectives</td>
<td>➢ Create Custom Load Files Based on Criteria (native, TIFF or PDF)</td>
</tr>
<tr>
<td>➢ Map Categories of Content, Business Process, Legal Issues, Users, etc.</td>
<td>➢ Map Legal Hold Requirements to Systems; Define Preservation Options</td>
<td>➢ Document Chain of Custody</td>
<td>➢ Deduplicate; Data Filters</td>
<td>➢ Manage Workflow and Completion Status</td>
<td>➢ Perform Validation and QC checks</td>
</tr>
<tr>
<td>➢ Identify Supporting Technologies</td>
<td>➢ Document and Implement</td>
<td>➢ Load Data onto Analysis and/or Review Platform</td>
<td>➢ Escalate Documents based on Relevancy, Privilege</td>
<td>➢ Report on Results</td>
<td></td>
</tr>
</tbody>
</table>
When Litigation is “Reasonably Anticipated”
When Is Litigation Anticipated?

- Determination made whether circumstances give rise to a credible threat of litigation
- Procedure established for reporting potential threats of legal action to responsible decision maker
- Whether credible threat exists is based on established procedure consistently followed
- Whether threat is credible is based on prudent investigation and evaluation of relevant facts, circumstances, company’s experience
- Responsible, trained decision maker determines when litigation is reasonably anticipated based on known facts
- Evaluation process analyzed by courts and opposing parties based on consistent application of established process in good faith – no hindsight evaluation
What Is An Effective Legal Hold?

- Identify and preserve relevant information
- Appropriate scope
- Document and standardize activities
- Reasonable efforts towards compliance
- Consider disposition
- Counsel develops integrated legal strategy (merits and Legal Hold); provides advice and direction regarding Hold
- Technologist translates legal scope into technical requirements and protocols; designs and implements Legal Hold
Overview of Legal Hold Process

- In practical terms, preserving all potentially relevant ESI is not possible
- Scope should be reasonable and scope development is an iterative process
- Suspicion of malfeasance will significantly impact the preservation process
- Preliminary notice to custodians will use broad language to cover unknowns
- Preliminary notice to Corporate and Business Unit IT will instruct owners of high-value systems (e.g. email) to preserve/retain ESI
- Further investigation and understanding of potentially relevant systems/repositories will result in updated notices
A Basic Work Plan

- Understand the issues
- Identify affected business processes
- Identify custodians participating in affected business processes, typically limited to specific functions/roles
- Issue preservation notices to custodians with detailed instructions
- Identify systems that support affected business processes
- Do not cast too wide a net
- Issue preservation notices to business system owners with instructions regarding the method of preservation
- Trust but verify
Implementing the Work Plan

- An organized approach is critical
- Build a legal hold team
  - GCO, Information Security, Corporate and Business Unit IT, and Compliance
- In large legal holds, establish a Steering Board composed of stakeholders to provide vision, strategy and decision-making
- Decompose potentially relevant ESI into categories to improve manageability
## Identifying Relevant ESI

<table>
<thead>
<tr>
<th>Data Classifications</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Category 1:</strong> Corporate Email Servers, Archive and</td>
</tr>
<tr>
<td>Journaling Systems (email user data stored on servers)</td>
</tr>
<tr>
<td><strong>Category 2:</strong> Collaborative Systems (shared workspaces</td>
</tr>
<tr>
<td>on servers)</td>
</tr>
<tr>
<td><strong>Category 3:</strong> Corporate File Servers (personal and</td>
</tr>
<tr>
<td>shared user data stored on servers)</td>
</tr>
<tr>
<td><strong>Category 4:</strong> Individual Data and Documents Stored on</td>
</tr>
<tr>
<td>Personal/Local Systems</td>
</tr>
<tr>
<td><strong>Category 5:</strong> Business Application Data (data contained</td>
</tr>
<tr>
<td>in transactional databases, business applications or</td>
</tr>
<tr>
<td>other similar information sources)</td>
</tr>
<tr>
<td><strong>Category 6:</strong> Other: IM, Electronic Fax, Voicemail,</td>
</tr>
<tr>
<td>Network/Security Monitoring</td>
</tr>
</tbody>
</table>

| Unstructured, Usually Non-Cumulative                       |
| Structured, Usually Cumulative                             |
Forensic imaging creates a bit-for-bit copy of an evidence drive and stores it in a single file on a target drive.

Forensic analysis:
- Can be a very useful tool but has limitations.
- Data can be destroyed (evidence of data destruction may be detected).
- May not provide ‘all the answers’.

Risks:
- Damaged hard drives
- Wrong drive imaged
- Original data modified
- Incomplete image
- Misplaced drive
- Lost or overwritten image
- Chain of custody not maintained
- Inadequate documentation
Conclusions

- Manage ESI early
- Transparency not secrecy
- Plan and manage the project
- It’s about the process – no silver bullets