



Record Retention: Stay Ahead of the eDiscovery Storm

Stephanie A. "Tess" Blair
Morgan, Lewis & Bockius LLP



Introduction

The Perfect Storm

An eDiscovery Perfect Storm is on the Horizon . . .

- Billions of emails sent daily in U.S.
 - 93% of information produced each year is stored in digital form
 - 2.3 billion emails are sent each day
 - 12.3 million networks are installed currently in the U.S.
- Cost
 - eDiscovery industry predicted to reach \$2.8 billion by 2007
- Litigation Risk
 - Casual mode of communication
 - Spoliation



When the eDiscovery Perfect Storm Hits . . .

- The *Zubulake* saga:
 - failure to preserve backup tapes
 - failure to produce email
 - adverse inference instruction
 - \$29M verdict (\$20M in punitives)
- Morgan Stanley
 - failure to preserve and produce from backup tapes
 - burden of proof shifted
 - counsel sanctioned and fired
 - \$1.4 BILLION verdict



Record Retention as a Defensive Weapon

- When failure to produce records in litigation is result of comprehensive and consistently enforced record retention program, program becomes a defense to claims of spoliation
 - *United States v. Arthur Andersen*, 125 S. Ct. 2129 (2005)
 - *Park v. City of Chicago*, 297 F.3d 606 (7th Cir. 2002)
 - *Lewy v. Remington Arms Co., Inc.*, 836 F.2d 1104 (8th Cir. 1988)
 - *Cf. Testa v. Wal-Mart Stores, Inc.*, 144 F.3d 173 (1st Cir. 1998)

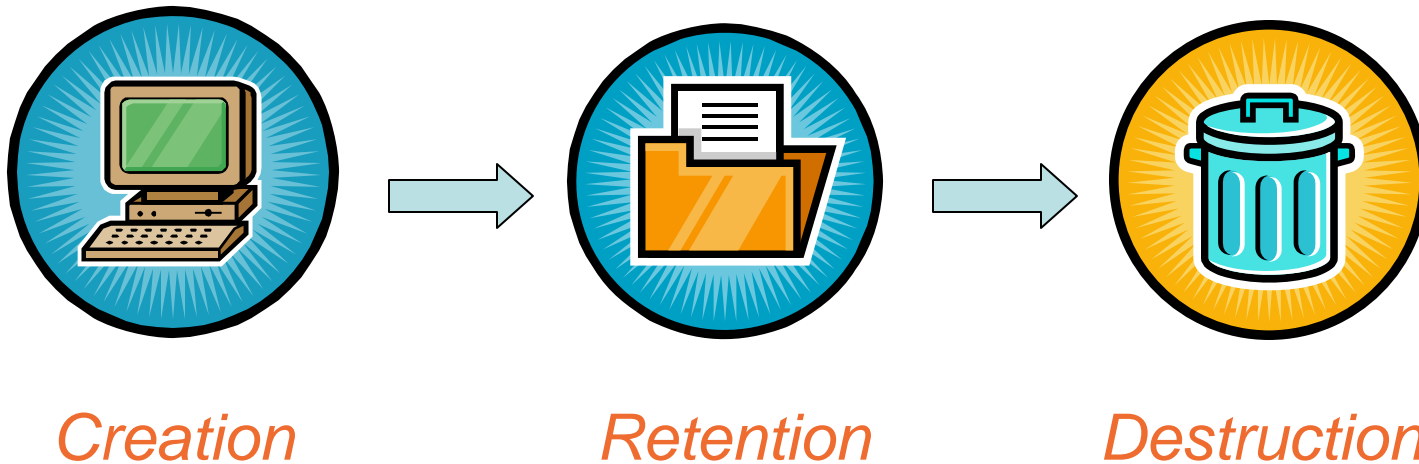




Proactive Record Management

A Holistic Approach

Lifecycle of a Record



Risks at every stage



Creation

- Smoking Guns
- Privilege Waiver
- Duplicates

Retention

- Storage
- Organization
- Management

Destruction

- Statutory and Regulatory Obligations
- Legal Hold
- Corporate Assets



Proactive Record Management



Record Creation





Creation

- Employee Training is Key
- Training program should include:
 - Litigation Primer
 - Best Practices
 - Record Retention Program Implementation





Creation

- Litigation Primer
- Employees should know:
 - Litigants are generally entitled to all non-privileged potentially relevant records of the other party
 - Records include email and other electronically stored information
 - Organizations are obligated to produce records within the company's "possession, custody or control"
 - Such records include all records received, created or stored by employees including personal communications from corporate computers and corporate communications from personal computers





Creation

- Best Practices Training Highlights:
 - Be scrupulously accurate
 - Create documents that memorialize resolution of issues rather than debate or argue points
 - Always include context for communication
 - Limit preparation of critical evaluations to employees with responsibility for the function being evaluated
 - Avoid editorial comment, rhetoric, conjecture, speculation, gratuitous characterizations
 - Do not distribute documents indiscriminantly
 - Treat email as you would treat any other medium of business communication
 - Do not use email for privileged or confidential communications





Creation

- Record Retention Program Implementation
- Employees should know:
 - Importance of program
 - Distinction between “business records” and “records of transitory value”
 - How to store and discard business records in accordance with program
 - Consequences of failure to properly retain records
 - Sarbanes-Oxley Act of 2002
 - Title 18 Obstruction of Justice
 - Civil Penalties including adverse inference



Proactive Record Management



Record Retention





Retention

- Policy should be designed to meet business needs and legal obligations
- Policy should be comprehensive, yet simple
 - Must address both electronic data and paper
 - Clearly state rationale for policy
 - Include retention/destruction schedules
 - Include an exception for litigation hold





Retention

- Best Practices
 - Designate a gatekeeper
 - Inventory “Business Records”
 - Identify record groups
 - Tax
 - HR
 - Finance
 - Insurance Policies
 - etc.





Retention

- Best Practices
 - Research laws and regulations applicable to each group
 - Develop retention/destruction schedules for each group
 - Describe retention method





Retention

- Caution:
 - Do not use format to determine retention period
 - ie. Delete all email after 45 days
 - A policy ignored is worse than no policy at all
 - Develop a mechanism for auditing and compliance



Proactive Record Management



Record Destruction





Destruction

- Documents must be destroyed “in the ordinary course of business” to be legally defensible
- One time destruction should be avoided
- *Destruction must be suspended for anticipated or pending litigation or investigation*





Destruction

- Destruction Methods should minimize risk of:
 - Loss of confidential/trade secret information
 - HIPAA violations
 - Identity Theft





Destruction

- Hard Copy:
 - Sensitive business and HR records should be destroyed by professionals
 - Destruction should be certified
 - Day to day destruction of business records should be done with shredders
- Electronic Records:
 - Recycling and reformatting is preferred method for tapes and drives
 - But it is virtually impossible to guarantee destruction



Proactive Record Management



Litigation Hold





Litigation Hold

- Design your “litigation hold” with the following questions in mind:
 - Whose documents must be retained?
 - Who are the key players?
 - Which business units, locations, departments have information relevant to the claims or defenses of any party?
 - What time period is implicated by the hold?
 - Documents extant at the time the obligation is triggered
 - Newly created materials





Litigation Hold

- Design your “litigation hold” with the following questions in mind:
 - What kind of information is likely to be implicated?
 - Hard-copy documents?
 - Computerized or other digital data?
 - Voice, video data?
 - Is this data accessible?





Litigation Hold

- Key Components of a Litigation Hold:
 - Subject
 - Directive regarding preservation of potential discovery materials and electronic data
 - Description of Scope
 - Define potentially relevant information
 - Explain breadth of definition
 - Caution re: underinclusive v. overinclusive
 - Definition of “Document”
 - Expansive meaning includes hard-copy paper, electronic data, email and attachments, databases, drafts, notes, calendars, etc.





Litigation Hold

- Key Components of a Litigation Hold:
 - Distribution list:
 - all “key players”
 - others with potentially relevant records
 - Sender – someone with “corporate heft”
 - GC or in-house counsel
 - Company’s compliance officer
 - Other
 - Identify who the employees can call for help





Litigation Hold

- Key Components of a Litigation Hold:
 - Specific Instructions to Halt routine destruction of each document type as appropriate: paper, email, text files, databases, etc.
 - Instructions highly contingent on:
 - Sophistication of client's IT infrastructure
 - Client's IT resources
 - volume of implicated data
 - amount at stake in litigation
 - likelihood of discovery dispute
 - agreement of parties





Record Retention: Stay Ahead of the eDiscovery Storm

Stephanie A. “Tess” Blair
Morgan, Lewis & Bockius LLP