



## Boston Executive Briefing Series

### Corporate Records: What to Keep and What to Toss

April 4, 2007  
Boston, MA

Presented by:  
Mark F. Foley  
Michael J. Tuteur



©2007 Foley & Lardner LLP • Attorney Advertising • Prior results do not guarantee a similar outcome • Models used are not clients but may be representative of clients • 321 N. Clark Street, Suite 2800, Chicago, IL 60610 • 312.832.4500 • The information reported should not be construed as legal advice, nor utilized to resolve legal problems.



## Need for a Policy

- Ubiquitous Digital Records Makes Data Policy Essential
  - Litigation Nightmares – *Morgan Stanley*
  - Cost Shifting - *Zubulake*
  - Legal Malpractice - Judge Preska, author of *Met. Opera*
  - Ethical Violations?

©2007 Foley & Lardner LLP



## Need for a Policy

- “Philosophies” of Data Retention
  - “I can’t throw it out; someday it may help us!”
  - “Storage is cheap, and time is money. Let’s deal with this when we have to.”
  - *U.S. v. Microsoft* - 3 million e-mails, and Bill Gates can’t recall any of them!
  - No “right” answer; but policy-based destruction is preferred

©2007 Foley & Lardner LLP



## Principles of Good DRP

- Collect and Keep Only What You Truly Need
  - What information do you collect?
    - Types of data
    - Types of data subjects
  - Where does it come from?
    - Provided
    - Captured
    - Purchased
    - Created
    - Domestic v International
  - Why do you collect it?
  - Why do you keep it?

©2007 Foley & Lardner LLP



## Principles of Good DRP

- If you don't have it, you:
  - Can't misuse it
  - Don't need to store and protect it
  - Don't need to send out change notices
  - Don't need to find and produce it
  - Don't need to destroy it

©2007 Foley & Lardner LLP

**FOLEY**  
FOLEY & LARDNER LLP

## Principles of a Good DRP

- Compliance with Law
  - Maintain records that demonstrate compliance with substantive law
  - Retain records concerning company's legal obligations for the period of time the obligation remains; but no longer
  - Keep records for as long as statute of limitations; but no longer

©2007 Foley & Lardner LLP

**FOLEY**  
FOLEY & LARDNER LLP

## Principles of a Good DRP

- Destroy Data Pursuant to Set Policy
  - Destruction should occur on a regular basis
  - Destruction should be based on business reasons
    - Real business needs come first
    - Cost
    - Administrative efficiency
    - Disaster recovery

©2007 Foley & Lardner LLP



## Principles of a Good DRP

- Destruction Stops Immediately Once a Claim is “Likely”
  - Failing negotiations
  - Government inquiry
  - Demand Letter, Notice of Claim, or Cease & Desist
  - Service of Process
  - Voluntary cooperation with Government

©2007 Foley & Lardner LLP



## Principles of a Good DRP

- Maintain Privacy and Security During Retention and Disposal
  - Confidentiality
  - Integrity
  - Accessibility

©2007 Foley & Lardner LLP



## Establishing a DRP

- Firm-Wide Records and Data Audit
  - DRP Team from all departments
  - Include GC, HR, IT, Accounting, Compliance
  - In large firm, consider retention of DRP counsel and consultants

©2007 Foley & Lardner LLP



## Establishing a **DRP**

- Assess Company Systems for Data Creation & Retention
  - Inventory all hardware, including PCs, voicemail, fax, email, PDAs, servers, etc.
  - Remember home computers, faxes, etc.
  - Consider deep and dead storage, including off-site storage
  - Consider variety of media, including paper, magnetic, optical, film, fiche, etc.

*more . . .*



©2007 Foley & Lardner LLP

## Establishing a **DRP**

- Assess Company Systems for Data Creation & Retention
  - SMS/text messaging; IM; company blogs; company and personal storage websites
  - Don't forget third-parties who may be creating, receiving, processing, or retaining your data



©2007 Foley & Lardner LLP

## Establishing a **DRP**

- Determine Legal Requirements and Compliance Issues
  - Audit all legal obligations and requirements applicable to Firm's business
    - HR obligations are often largest number,
    - In certain industries (e.g. securities, pharmaceuticals, environmental, etc.) other regulations may outnumber
  - Calculate applicable statutes of limitation

*more . . .*



©2007 Foley & Lardner LLP

## Establishing a **DRP**

- Determine Legal Requirements and Compliance Issues - more
  - Remember that US may not be only governing law – e.g., consider EU
    - Data that is valuable to a data subject may not be destroyed without her consent
    - Data retention policies must be disclosed
    - Data may only be collected for the purpose originally identified and disclosed.



©2007 Foley & Lardner LLP

## Establishing a **DRP**

- Develop Centralized Records Inventory System
  - Create uniform file system for all departments?
  - Dewey Decimal System
  - How to handle dynamic data: databases, spreadsheets, etc.?
- Know where your records are!

©2007 Foley & Lardner LLP



## Establishing a **DRP**

- Consider Separate Email & Voicemail Policies
  - Email is often most dangerous, most highly prized in litigation
  - Searching and recovery of email often extraordinarily costly.
  - Voicemail is even worse
  - Huge volumes of undeleted email often choke system resources
  - Quick, automatic deletion to be preferred (but check legal/regulatory obligations)

©2007 Foley & Lardner LLP





## Establishing a **DRP**

- Draft Workable Policies That Conform with Business Needs
  - DRP Team drafts policies and time-frames consistent with good DRP principles
    - Buy-in from all departments
  - Circulate time-frames -- and be prepared for shouting!
  - See examples in materials
  - Incorporate policies into business processes

©2007 Foley & Lardner LLP



## Establishing a **DRP**

- Establish Procedure for Immediate Suspension of DRP When Litigation is Threatened
  - Centralize claim receipt procedure: HR, GC or Compliance Dept.
  - Pre-drafted memos and emails to stop destruction (see handout)
  - Work closely with IT on procedure for stopping destruction of back-up tapes, email servers, etc.
  - Establish testing procedure
  - Include procedure for restarting DRP after claim is resolved

©2007 Foley & Lardner LLP



## What Not To Do...



©2007 Foley & Lardner LLP

**FOLEY**  
FOLEY & LARDNER LLP

## Enforce, Enforce, Enforce!

- Enforcement (the “hard part”)
  - Both management and in house counsel must be vigilant
  - ACCA hosted seminars (e.g. Best Practices Forum for Enforced Records Management)
  - Various vendors (Computer Forensics Consultants; Accutrac; Documentum; EMC2; File Net; File Surf; Manage; ARMS Records Management)

©2007 Foley & Lardner LLP

**FOLEY**  
FOLEY & LARDNER LLP

## **Enforce, Enforce, Enforce!**

- Name DRP Representative Within Each Business Unit
  - Invest DRP Rep with Executive's authority
  - Teach from the Top: Apply DRP to Executive Office
  - Invest in Training

©2007 Foley & Lardner LLP



## **Enforce, Enforce, Enforce!**

- Audit Compliance with DRP from Inception
  - Use DRP Team to Assist with Audit
  - Consider Retaining Consultants if Necessary
  - Test Systems for Stopping, Restarting DRP
  - Test security

©2007 Foley & Lardner LLP



## Enforce, Enforce, Enforce!

- Effectiveness of Policy is Key
  - Ineffective Policy may be Worse than No Policy
    - *Murphy Oil v. Fluor Daniel*: Failure to follow email destruction policy leads to order of production of backup tape; “if Fluor had followed this policy, the email issue would be moot.”
    - *Zubulake*: Parties are now “on notice”; cost-shifting will not take place if policy is not followed
    - Spoliation – the new buzzword!

©2007 Foley & Lardner LLP



## Practical Tips

- Involve IT at Every Level
  - IT often believes in saving data; needs to learn about losing it as well
  - IT should help devise ways to automate proper retention, retrieval, and disposal.

©2007 Foley & Lardner LLP





## Practical Tips

- Establish clear accountability at all levels
  - Incorporate compliance into business plans
  - Incorporate compliance into individual performance and compensation reviews
  - Reward/penalize managers for business unit performance on completion, compliance and results
  - Assess discovery costs to business units

©2007 Foley & Lardner LLP



## Practical Tips

- Train
  - Educate staff on perils of e-communication
  - Educate staff on how to manage their e-communication
  - Educate staff on what to do with records when claims arise
  - Eliminate local data retention to fullest possible extent.

©2007 Foley & Lardner LLP





## Practical Tips

- Prevent email bloat
  - Segregate personal and business email
  - Delete all email promptly unless saved in a specific folder
  - Encourage Total Workday Control over email

©2007 Foley & Lardner LLP



## Practical Tips

- Identify privileged documents when generated or received
  - Set up automated tags for e-documents
  - Color-code paper documents

©2007 Foley & Lardner LLP





## Practical Tips

- Keep disaster recovery and document retention distinct
  - Backup tapes are for disaster recovery, not data preservation or retrieval
  - Recycle backup media as often as practical to eliminate them as costly discovery mechanisms
  - Be able to retrieve stored data that does not involve sequential backups
  - Plan for data retrieval and disposal from legacy systems when they are replaced

©2007 Foley & Lardner LLP



## New Federal Rules

- Changes in FRCP Have Affected Data Retention Issues
- New Federal Rules Became Effective December 1, 2006
- State rules are changing; guidelines have been promulgated (see handout) and new laws are being enacted

©2007 Foley & Lardner LLP



## New Federal Rules

- Electronic data are different from paper
  - Dynamic vs. static system
  - Huge volumes of documents
  - Much information is stored in forms that are not “documents”
  - Serious risk of privilege waiver
  - Burden of searching legacy/backup systems

©2007 Foley & Lardner LLP

**FOLEY**  
FOLEY & LARDNER LLP

## New Federal Rules

- Rule 26(b) and (f)
  - Early conference to address electronic discovery, including privilege issues
  - Early preservation orders are disfavored
  - New “two-tier” discovery process for electronic information
    - Identify and produce reasonably accessible electronic documents and information
    - Identify sources of information that are not reasonably accessible, but “a party need not provide discovery of electronically stored information from sources that ... [are] not reasonably accessible because of undue burden or cost.” (Rule 26(b)(2))
    - Codification of *Zubulake*'s 7 factors

©2007 Foley & Lardner LLP

**FOLEY**  
FOLEY & LARDNER LLP





## New Federal Rules

- Rule 26(b)(5)(B) – New Approach to Assertion of Privilege
  - No automatic waiver
  - Establishes procedure for late assertion of privilege
  - Recognition that much privileged information may be hidden and cannot be searched in advance

©2007 Foley & Lardner LLP



## New Federal Rules

- Rule 37(f) – Limitation on sanctions
  - Recognition of dynamic nature of electronic information
  - “Good faith” standard
  - “[C]ourt may not impose sanctions ... [if] information [is] lost as a result of the routine, good faith operation of an electronic information system.”

©2007 Foley & Lardner LLP



## New Federal Rules

- Practical consequences
  - Work with active and to-be-acquired systems; legacy systems can wait
  - Litigation holds still essential, but fewer sanctions for inadvertent destruction
  - Huge, upfront searching costs may be reduced – maybe.
  - But federal only for now; and worst sanctions have come in state cases.
  - Use counsel who are facile not just with the rules, but with the technology.

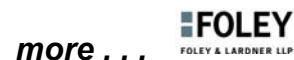
©2007 Foley & Lardner LLP



## Practical Tips - Litigation

- Be Prepared for Litigation
  - Have a Plan
    - Know who will be involved in responding to systems assessments and responses to requests for electronically stored information
    - Have an up-to-date system architecture and inventory
    - Have considered and tested hold procedures

©2007 Foley & Lardner LLP



## Practical Tips - Litigation

### – When litigation is threatened:

- Circulate memos and emails regarding data preservation
- Establish a privileged point of contact for questions
- Make sure all destruction processes are stopped, or evaluated for their applicability to potentially material data by legally savvy personnel
- Send letter to opposing party (through outside counsel) demanding preservation of evidence
- Confer with e-discovery counsel to map the architecture, policies, and processes involved with your electronically stored and manually stored data and create a plan for retrieval, review, and production of relevant data

©2007 Foley & Lardner LLP



## When Litigation Comes

### – Seek agreement with other side regarding:

- Scope of discovery
- Preservation and management of e-evidence
- Sampling of records
- Forms of production (e.g., print out, native format, etc.)
- Cost sharing.
- Initial disclosures and depositions regarding data and systems architecture, software, retention policies, and retrieval capabilities

©2007 Foley & Lardner LLP





## Conclusion

# A Data Retention Policy is No Longer a Matter of Choice

©2007 Foley & Lardner LLP



## Boston Executive Briefing Series

### Corporate Records: What to Keep and What to Toss

April 4, 2007  
Boston, MA



Presented by:  
Mark F. Foley

[mfoley@foley.com](mailto:mfoley@foley.com)  
(414) 297-5514

Michael J. Tuteur

[mtuteur@foley.com](mailto:mtuteur@foley.com)  
(617) 342-4016

©2007 Foley & Lardner LLP • Attorney Advertising • Prior results do not guarantee a similar outcome • Models used are not clients but may be representative of clients • 321 N. Clark Street, Suite 2800, Chicago, IL 60610 • 312.832.4500 • The information reported should not be construed as legal advice, nor utilized to resolve legal problems.