



Ready or Not, Here They Come: The Amended Federal Rules and What They Mean for eDiscovery

October 30, 2006

We will begin the webcast at 2:00 p.m. Eastern
For the Audio Portion, Please Call 888.391.0236
Call 866.229.3239 option 1 for WebEx Tech Support

Morgan Lewis Legal Logistics Presenters



Stephanie A. "Tess" Blair, Esq.
Partner and Director
Morgan Lewis Legal Logistics
215.963.5161
sblair@morganlewis.com



Robert B. "Barry" Wiggins, Esq.
Assistant Director
Morgan Lewis Legal Logistics
202.739.5040
rwiggins@morganlewis.com



Scott A. Milner, Esq.
Assistant Director
Morgan Lewis Legal Logistics
215.963.5016
smilner@morganlewis.com

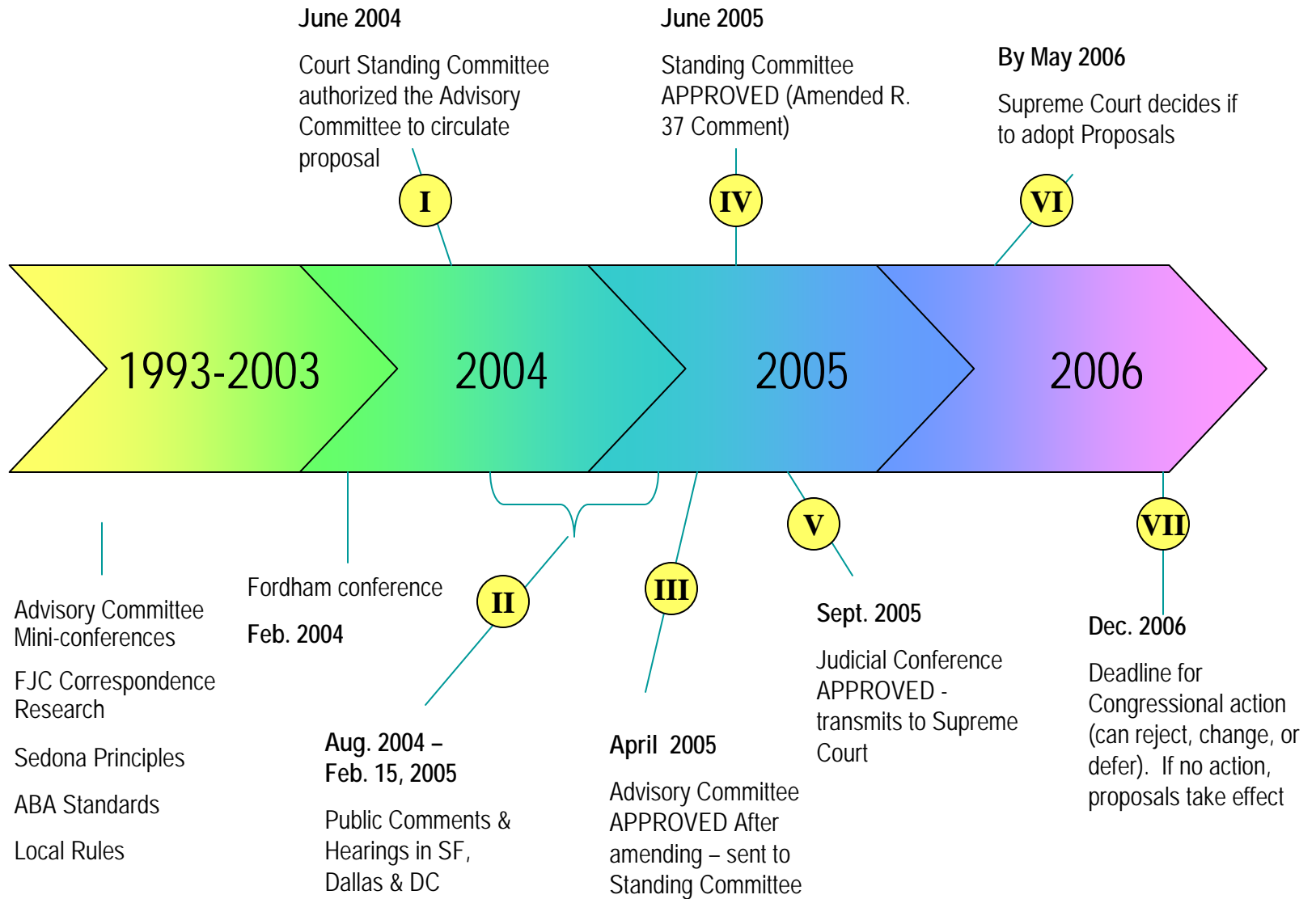


Denise E. Backhouse, Esq.
Assistant Director
Morgan Lewis Legal Logistics
212.309.6364
dbackhouse@morganlewis.com



The Future is Now!

www.uscourts.gov/rules/index.html



The Proposed Amendments to the Federal Rules

Overview

- “Electronically stored information” (ESI)
- Early attention by parties to eDiscovery issues
- Forms of electronic production
- Discovery of ESI “not reasonably accessible”
- Inadvertent production and waiver of privilege
- “Safe Harbor” – Limit on sanctions for loss of electronic information in routine, good-faith programs





Electronically Stored Information

“Documents” Under Current Rule 34

Rule 34. Production of Documents and Things and Entry Upon Land for Inspection and Other Purposes

- (a) **Scope.** Any party may serve on any other party a request (1) to produce and permit the party making the request, or someone acting on the requestor's behalf, to inspect and copy, **any designated documents** (including writings, drawings, graphs, charts, photographs, phonorecords, and **other data compilations** from which information can be obtained, translated, if necessary, by the respondent through detection devices into reasonably usable form), or to inspect and copy, test, or sample any tangible things which constitute or contain matters within the scope of Rule 26(b) and which are in the possession, custody or control of the party upon whom the request is served . . .



The Amendments: “Electronically Stored Information”

- Electronic records are distinct from “documents”
- No substantive definition is provided
- Scope of the meaning is quite flexible and inclusive
- Contemplates changing technology



Potential Impact

- Parties must think broadly about potential sources of information subject to discovery

Examples:

- Instant messages
 - Digitized voicemail or unified messaging systems
 - Text messages
 - Security data
- Parties must develop sound methods for preservation, harvest, review and production of information





Form of Production

Form of Production Under Current Rule 34

- FRCP 34

“A party who produces documents for inspection shall produce them . . .

→ as they are kept in the usual course of business

or

→ shall organize and label them to correspond with the categories in the request.”



The Amendments: Form of Production

- FRCP 34(b)(ii) Form of Production

“If a request for electronically stored information does not specify the form or forms of production, a responding party must produce the information in a form or forms . . .

→ in which it is ordinarily maintained

or

→ in a form or forms that are reasonably usable”



Recent Cases on Form of Production

- Two recent cases:
 - *Williams v. Sprint/United Mgmt. Co.*, 230 F.R.D. 640 (D. Kan. 2005)
 - *Hagenbuch v. 3B6 Sistemi Elettronici Industriali*, 2006 WL 665005 (N.D. Ill. March 8, 2006)



A Brief Detour to Metadata . . .

- “Information describing the history, tracking, or management of an electronic document.”
Advisory Committee note to the Federal Rules of Civil Procedure 26(f).
- “Information about a particular data set which describes how, when, and by whom it was collected, created, accessed, or modified and how it is formatted (including data storage demographics such as size, location, storage requirements and media information).” *The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age, App. F (2005).*



Potential Impact on Preservation

- Preserve electronic files in their native format
- Avoid modifying metadata by opening, printing, copying, or forwarding files
- Best practice: snapshot



Potential Impact on Review

- Privilege review should include review of metadata
- Metadata can replace objective coding
- Best practice: electronic native review in database



Potential Impact on Production

- Options:
 - Native production
 - Ordinary course
 - No ability to redact or Bates label
 - No ability to “lock down” files
 - Image production with extraction of metadata and searchable extracted text
 - Reasonably usable
 - Limit native production to agreed-to file types





Early Meet and Confer

The Amendments: Establish ESI as part of discovery process

- Rule 16(b) – confirms the court’s ability to address ESI discovery issues in 16(b) orders.
- Rule 26(f) – requires parties to confer regarding, and to develop a discovery plan addressing, ESI:
 - Must include “form or forms” of production
 - Must include waiver of privilege issues



Potential Impact

- Parties must familiarize themselves with:
 - IT infrastructure
 - All potential sources of relevant data
 - Proposed methods and costs of preservation, harvest, review, and production
 - Potential problems, such as legacy systems, proprietary databases
- Provides opportunity to discuss cost-saving options:
 - Narrow scope of discovery
 - Culling methods
 - Clawback
- Appointment of eDiscovery liaison





Two-Tier Discovery

The Amendments:

Data inaccessible due to “undue burden or cost”

- Rule 26(b)(2)(B)
 - Party may object to discovery of ESI “not reasonably accessible because of undue burden or cost”
 - If confronted with a motion to compel, party must then demonstrate inaccessibility and, for good cause, may still be subject to judicial discovery order



Accessible vs. Not Reasonably Accessible

Accessible Data

- Network files
- Active e-mail
- “Archived” e-mail
- Unemptied trash
- Hard drive contents

Not Reasonably Accessible Data

- Back-up tapes
- Legacy data



Potential Impact

- Parties must familiarize themselves with:
 - IT infrastructure
 - All potential sources of relevant data
- Parties must identify and sort data by accessible vs. “not reasonably accessible”
- The obligation to preserve “not reasonably accessible” data remains



Clawback



The Amended Rules: Clawback

“Hostage Exchange”

- ***Inadvertent*** production addressed
 - Notification
 - Within a reasonable time period
 - Return, sequester, destroy
- Producing party must then follow FRCP 26(b)(5)(A)
 - Express claim of privilege
 - Describe the nature of the document
 - Assessment by opposition



Potential Impact

- May entice litigants to forgo privilege review
- Uncertainty remains as to whether waiver protection travels with records to other cases or jurisdictions



A Case in Point ...

***Hopson v. The Mayor and City of Baltimore*, 235 F.R.D. 228 (D. Md. 2005)**

- Privilege review of electronically stored information is difficult and costly primarily because of the sheer volume and lack of organization of such information.
- One solution, as reflected in the pending revisions to the Federal Rules of Civil Procedure, is to encourage the use of non-waiver agreements.
- Such agreements do not address the question of whether the privilege has actually been waived, but simply allow the producing party to assert a claim of privilege after production, if the privileged materials end up being disclosed.
- Final disposition depends on the applicable law of privilege.



On the Horizon ... FRE 502?

An *inadvertent* disclosure should not constitute a waiver if the holder of the privilege or work product protection

- (1) took reasonable precautions to prevent disclosure, and
- (2) took reasonably prompt measures, once the holder knew or should have known of the disclosure, to rectify the error.



The Amended Rules: A “Safe Harbor” for Routine Operations

Rule 37(f)

Electronically stored information.

Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, **good-faith** operation of an electronic information system.



Safe Harbor Explored ...

- Likely to afford limited protection from spoliation claims
- Existence of preservation order not required
- Parties still required to adequately preserve data



Safe Harbor Explored ...

- Preservation still requires:
 - Institution of litigation hold
 - Identification and suspension of any automated IT systems that purge data
 - Auto-delete or email janitors
 - Back-up tape rotation
- Broad discretion given court
 - Litigant's conduct
 - Characteristics of ESI at issue



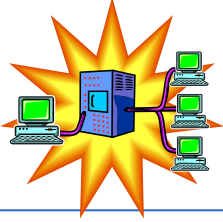


So, What Does All This Mean For Us?

Get Your E-data House In Order: Litigation Response Planning

- Checklist of Action Items
 - Map your Information Technology
 - Infrastructure
 - Develop a Data Inventory
 - Prepare a Litigation Response Plan
 - Modify Retention Policies
 - Consider Technology Options
 - Inventory your Litigation Portfolio
 - Enforce your Retention Policy
 - Train your workforce

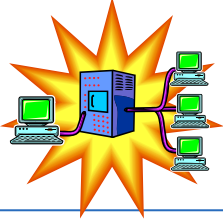




Map Your IT Infrastructure

- Email - Current System and Migration History
- Network Drives - Home/User Drives, Departmental/Project Drives
- Hard Drives - Desktops, Laptops, Home, Stand-Alone Computers, PDAs, portable devices and media
- Backup Architecture – Current and Off-line, Rotation, Retention Policy
- Legacy Systems and Data





Develop a Data Inventory

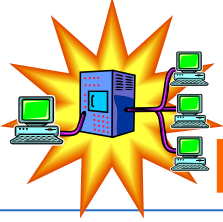
- Possible sources:
 - Email
 - Word Processing
 - Databases
 - Calendaring Systems
 - Proprietary Applications
 - Financial/Business Management Applications
- Identify
 - Current locations and volume of live data
 - Back ups
 - Legacy systems and data
 - Other storage locations
 - Hard drives
 - Portable devices



Prepare a Litigation Response Plan

- Prepare a litigation response org chart
- Identify roles and responsibilities
- Memorialize a litigation response checklist
- Develop deployment scenarios





Modify Storage Policies and Practices

- Modify policies on storage and retention of e-data to address business needs and minimize litigation risk
 - Why are you keeping this stuff?
 - Policy on limiting local installations
 - Policy on hard drive access to administrative personnel
- Ensure record retention policies reflect changes





Consider Technology Options

- E-mail Management
 - Enterprise solutions
 - Outsourcing
 - Off-site Archiving
- Automated Content Based Record Retention
- Electronic Litigation Repository
- Review Tools





Inventory your Litigation Portfolio

- Identify
 - Current Cases, Investigations, Subpoenas
 - All pending litigation holds
- Identify all data implicated by ongoing holds



Enforce your Retention Policy

- You do have one, right?
- Purge data:
 - NOT implicated by ongoing holds
 - NOT required to be maintained by retention policy
- Migrate legal hold and compliance data to established system
 - Track content for ongoing and future litigation





Protocols and Documentation

- IT Architectural Scheme
- Data Inventory
- Modern Record Retention Policy
- Litigation Response Plan
- Litigation Hold Database
- Discovery Checklist
- Litigation Hold Template
- Employee Training Materials
- 30(b)(6) Witness Materials
- Form Initial Disclosures
- Form 35 Discovery Plan
- Form agreements with opposing counsel



For Additional Information



Stephanie A. "Tess" Blair, Esq.
Partner and Director
Morgan Lewis Legal Logistics
215.963.5161
sblair@morganlewis.com



Robert B. "Barry" Wiggins, Esq.
Assistant Director
Morgan Lewis Legal Logistics
202.739.5040
rwiggins@morganlewis.com



Scott A. Milner, Esq.
Assistant Director
Morgan Lewis Legal Logistics
215.963.5016
smilner@morganlewis.com



Denise E. Backhouse, Esq.
Assistant Director
Morgan Lewis Legal Logistics
212.309.6364
dbackhouse@morganlewis.com





Ready or Not, Here They Come: The Amended Federal Rules and What They Mean for eDiscovery