

The Age of Electronic Discovery Has Arrived

Are You Ready?

SBM
STATE BAR OF MICHIGAN
labor &
employment law section

Presented By:
James J. Boutrous II
September 27, 2007



BUTZEL LONG
ATTORNEYS AND COUNSELORS

Program Contents

- ÷ Amendments to the Federal Rules of Civil Procedure regarding Electronically Stored Information. FRCP 16, 26, 33, 34, 37 and 45.
- ÷ Review and understanding of computer network by in-house counsel, IT Department, and outside counsel.
- ÷ Based upon the above, the development of an electronic information retention policy that is grounded in business reality and legal requirements.
- ÷ Development of a protocol for a "Legal Hold."
- ÷ Development of protocol for the production of electronic information, when necessary.

Electronically Stored Information (“ESI”)

÷ The Way Businesses Operate Has Changed:

- ⚠ Over 99% of new information stored in the US is stored electronically – most is never printed on paper.**
- ⚠ Sources estimate that by this year, e-mail volumes will reach 60 billion messages.
- ⚠ One terabyte of electronic information equals 50 million pages or 20,000 boxes of paper.



÷ Courts and the FRCP drafters recognize this growth so the rules on electronic discovery are evolving.

**Peter Lyman and Hal R. Varian, How Much Information 2003?, 1 at <http://www.sims.berkeley.edu/research/projects/how-much-info-2003>

Amendments to the FRCP (effective 12/1/06)

5 E-Discovery Areas:



1. Early Attention to E-Issues
2. Accessibility of E-Data
3. Assertion of Privilege after Production
4. Written Discovery and E-data
5. Limit to Sanctions for Loss of E-Data

FRCP Amendments

- ÷ Apply to all cases filed after December 1, 2006, and to **all cases then pending** to the extent practicable (See Paragraph 3 of the Supreme Court's Order approving the amendments).
- ÷ FRCP Advisory Committee Notes are rich with explanations of the changes
- ÷ Advisory Committee added ESI language to capture all types of electronic data
- ÷ New rules emphasize controversies over scope often to be resolved by balancing of burdens

Early Readiness Mandated (FRCP 16(b), 26(f) & Form 35)

- ÷ Must understand ESI in first 120 days of lawsuit
- ÷ Must attend pre-discovery Rule 26(f) conference to negotiate e-discovery issues within weeks of service of summons/complaint
- ÷ Best to be prepared to stipulate, if possible
- ÷ Best to propose a discovery plan and schedule re: ESI
- ÷ Create an E-discovery Response Team: outside counsel, in-house counsel, client IT, records management personnel and HR personnel

FRCP Amendments

EARLY ATTENTION TO E-ISSUES, ACCESSIBILITY & PRIVILEGE:

- ÷ FRCP 16(b) court conference: Process for parties and court to address ESI disclosure and discovery. Courts expect parties to be fluent in client's network architecture
 - ! Advisory Committee Note states that parties must also identify by category/type the sources of potentially responsive ESI that a party is neither searching nor producing with enough detail for opposing counsel to evaluate the burden/cost and likelihood of finding discoverable information in that source. **Those sources must still be preserved.**
- ÷ FRCP 26(f) meet and confer: Parties shall “attempt to agree” on disclosure of ESI
- ÷ Form 35: Add to the List of Topics in Court Report

FRCP Amendments

EARLY ATTENTION TO E-ISSUES, ACCESSIBILITY & PRIVILEGE:

- ÷ FRCP 26(a)(1)(B) initial disclosures: Without waiting for discovery request, a party must provide a copy of or description by category of “all” ESI that the disclosing party may use to support its claims or defenses.
- ÷ FRCP 26(a)(3) pretrial disclosures: Must identify “all” ESI a party expects to offer and may offer if the need arises.

FRCP Amendments

EARLY ATTENTION TO E-ISSUES, ACCESSIBILITY & PRIVILEGE:

- ÷ FRCP 26(b)(2)(B) accessible data: Party “need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost.”
- ÷ FRCP 26(b)(5) information produced: Provides procedure for addressing inadvertent production of privileged material before the court.

FRCP Amendments

WRITTEN DISCOVERY & E-DATA

- ÷ FRCP 33 interrogatories: Response referring to business records includes review of ESI and provides requestor access to such.
- ÷ FRCP 34(b) document production: Adds broad language re: production of ESI and allows the requestor to specify production format. Establishes framework to resolve disputes.

Subpoenas (FRCP 45)

- ÷ Similar to process for requesting ESI from a party
- ÷ Protects non-parties from costs/burdens that parties must normally bear

Amendments to FRCP

LIMIT TO RULE-BASED SANCTIONS FOR LOSS OF E-DATA

- ÷ FRCP 37 protective order: Producing party may seek protective order. Creates a narrow safe harbor from court sanctions, absent exceptional circumstances, if the electronic information is lost as a result of the “routine good-faith operation” of computer system recycling or overwriting.

Destruction of ESI and “Safe Harbor” from Sanctions

- ÷ Very Limited Protection for “good faith routine modification, overwriting and deletion of information that attends normal use.” (FRCP 37(f))
- ÷ Good Faith: did party take “reasonable steps to preserve after it knew information was discoverable”? (i.e., litigation hold followed)
- ÷ Routine Operation: through operations “designed, programmed and implemented to meet the party’s technical and business needs”

Rule-Based Sanctions - Limited Only

- ÷ Even if ESI loss is unintentional and despite good faith efforts – Rule 37 only prevents Rule 37 sanctions
- ÷ Court retains inherent authority to order sanctions for spoliation under case law or based on statutory/regulatory violations
- ÷ **Key:** Spoliation law grounded in common law not the rules.

ESI Effect on Retention Policies

THE ISSUE:

Record Management Programs Get
“Trumped” by a Litigation Hold

Pre-Litigation Planning Is Key

- ÷ Better to revise policy with ESI in mind before aware of potential litigation when common law duty to preserve triggered
- ÷ Mapping of network architecture early so it is available for all cases – consistency
- ÷ Better to be proactive, than reactive
- ÷ Reduces costs and human capital involved with each new case
- ÷ Reduces potential volume of ESI

Retention Policy Interaction with ESI Discovery

÷ Need a Discovery Plan

- ÿ Identify the Key IT personnel
- ÿ Identify Record Management Managers
- ÿ Identify the critical systems
- ÿ Identify the relevant applications
- ÿ Understand the record retention program and monitor uniform enforcement of it

Key Elements for Records Retention Policy

- ÷ Need a clear written policy that includes ESI, as well as hard copies
- ÷ Train employees to follow it
- ÷ Disseminate the policy across the company
- ÷ Issue periodic reminders to employees
- ÷ Assign gatekeeper to prevent deletion and loss of ESI if litigation anticipated

Records Retention Policy Issues

- ÷ Existence of Policy useless if not followed (i.e., are backup tapes actually recycled after specified time?)
- ÷ Policies will likely be an area of written discovery and depositions
- ÷ Creation of E-discovery response team is critical

Duty to Preserve - Goals

- ÷ Implement reasonable, not heroic measures
- ÷ Coordinate/communicate with key players in the organization early

Preservation & Litigation Holds

- ÷ Send a Preservation Letter/Notice once litigation is filed *or reasonably anticipated*
 - ! e.g., EEOC charge, informal complaint of product failure to company, threat to sue letters/discussions

Duty to Preserve – What Does it Mean?

÷ DON'T:

- ⚠ Delete files/e-mails
- ⚠ Defragment or compress hard drives
- ⚠ Add new software or operating systems
- ⚠ Access subject files until forensically sound image made

÷ DO:

- ⚠ Suspend all relevant record retention policies
- ⚠ Create complete forensically sound image of servers etc.
- ⚠ Stop recycling of backup tapes
- ⚠ Turn off auto delete functions on e-mail etc.

Preservation & Litigation Holds

÷ Preservation Letter/Notice:

- ! Ensure preservation letter sent to all key personnel (including IT department) by communicating with them directly re: preservation duties.
 - ! Counsel may need to interview key personnel re: procedures for retaining and managing ESI – especially e-mails.
- ! Reiterate litigation hold instructions “regularly” and monitor compliance.
(*Zubulake*: it is not sufficient for counsel to simply notify employees that there is a litigation hold and expect that the party will then retain and produce all relevant information)

- ÷ Designate E-Discovery Response Team: responsible for locating all sources of relevant information, conducting interviews, segregating and preserving ESI.

Litigation Hold

- ÷ Must Preserve Inaccessible Data too (e.g., backup tapes maintained solely for the purpose of disaster recovery).

Preservation Orders

- ÷ Know who the key players are in IT
- ÷ Understand the parameters of what company can commit to doing
- ÷ Do not let internal IT proceed unsupervised
- ÷ Be conservative if you suspect you need to call a third-party expert for discovery, do so

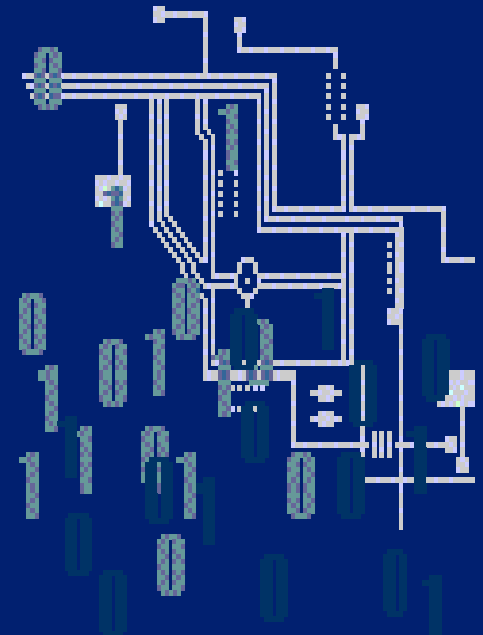
Data Sources: Where is the Relevant Data Stored?

- ÷ Office Computers/Personal computers
- ÷ Laptops
- ÷ PDAs
- ÷ CDs, DVDs, floppy disks
- ÷ Flash/thumb drives, memory cards
- ÷ Personal folders
- ÷ Deleted e-mails; documents
- ÷ Network Servers
- ÷ Mainframes
- ÷ Backup tapes
- ÷ Legacy systems
- ÷ Cell Phones
- ÷ Answering Machines
- ÷ Voicemail
- ÷ Other archive media or third-party storage media



Documents = Electronic Formats

- ÷ E-mails (in-box, sent items, deleted items, foldered & archived items)
- ÷ Instant messages
- ÷ Word processing programs
- ÷ Databases and spreadsheets
- ÷ Proprietary software
- ÷ PowerPoint slides
- ÷ Web pages
- ÷ Audio
- ÷ Video



Production of Electronic Data

- ÷ Strategy
- ÷ Analysis of the Document Request
- ÷ Collection Plan
- ÷ Sorting for Relevant Documents
- ÷ Review of the Documents/Data
- ÷ Production of Documents/Data

Must Understand Company's Computer and Information Systems

- ÷ *Zubulake* and its progeny require outside and in-house counsel to understand the digital technology used by the client and identify the gaps between the accessible data and data incorporated into the client's retention/records management program.
- ÷ Problem: Focus is usually on documents existing on company server(s) and that is where document retention policies are focused – not locally stored information.
- ÷ Company's network architecture should be mapped at outset of the case BEFORE initial court scheduling conference to avoid costly and expansive discovery obligations.

Corporate Designee Depositions

- ÷ Identify information managers, records retention managers and technologists
- ÷ Advisory Committee Notes: these depositions permissible per Rule 30(b)(6)

Corporate Designee (cont.)

÷ Prepare someone to attest re:

- ⚠ Where ESI is located, how kept, volume of data, how ESI created, retention/destruction policies/practices.
- ⚠ How e-mail works (archives/deletion protocol).
- ⚠ How files are named and stored.
- ⚠ Explain backup tape system (how often, purpose accessibility).
- ⚠ Instant Messaging – is it archived?
- ⚠ Voice Mail – is it saved digitally?
- ⚠ Who has access to the information?
- ⚠ Is Records Retention policy audited? Is it followed?

Managing the E-Data Acquisition

- ÷ ESI is not just data – it's evidence

- ÷ Chain-of-Custody is Key
 - ÿ Who collected ESI?
 - ÿ How ESI processed?
 - ÿ How prove ESI not altered?
 - ÿ How address/defend spoliation allegations?
 - ÿ Document collection, processing, production

- ÷ In-house IT department vs. Outside Forensic Vendor

Metadata

Data about the Data

- ÷ Metadata is discoverable
- ÷ All digital information generates metadata that remains unseen in the paper format
- ÷ Several types of metadata
- ÷ Beware: metadata can be inadvertently lost/modified by just accessing a file, copying the information, burning to a CD/DVD, forwarding e-mail messages and moving data between different operating systems

Issues & Strategies Raised by Key Cases:

- ÷ Active vs. Stored Data
- ÷ Accessible vs. Inaccessible Data
- ÷ Test run – sampling
- ÷ Key search terms

What Does Accessible Mean?



÷ Accessible Examples:

- ! Active files, CDs, DVDs, and current systems
- ! Those systems accessed in the usual course of business

÷ Usually producing party bears the cost of production

What Does Inaccessible Mean?

- ÷ **Inaccessible Examples:** disaster back up tapes, archives, legacy systems, unallocated or slack space.
 - ! Essentially inaccessible data needs to be brought back to life. Thus, potential for cost-shifting to requesting party.
 - ! Investigation/interviews of client necessary to determine if these are truly inaccessible for your client.
 - ! General purpose of backup tapes is to restore records in a disaster (crash, fire etc.) Some clients, however, may use them as an archival system and that may make them “accessible data.”

Recommended Tiered-Approach for Dealing with Inaccessible Data

- ÷ Preserve it – still obligated to preserve under common-law/statutory duties and court may order production anyway
- ÷ Produce accessible data first
- ÷ Identify sources of inaccessible data

Know Your Local Rules in State Court Too

- ÷ Guidelines for State Trial Courts approved 8/06
 - non-binding
- ÷ Michigan Rules Are Drafted and Awaiting Further Action.
 - § No formal action has been taken on these proposed amendments.
 - § To some extent they track the Federal Rule revisions, but there are few notable exceptions. In particular, there is a broad duty to preserve rule (MCR 2.302 (B)(5)) and a safe harbor provision that seems to be broader/better than that of the Federal Rules (MCR 2.312).

Best Practices re: ESI

- ÷ Create & implement written document retention/destruction policy
- ÷ Map network architecture – where does each type of ESI live? (i.e., who, what, where, how, when)
- ÷ Organize ESI storage efforts to reduce time, cost, and human capital related to locating, retrieving and producing ESI

Best Practices re: ESI

- ÷ Create E-discovery Response Team: establish working relationship among in-house legal department, IT department and Records management
- ÷ Create Litigation Hold plan and procedure to suspend retention policy and routine destruction of potentially discoverable ESI
- ÷ Designate and train IT department and/or record management employee(s) to act as corporate designee to testify regarding ESI issues

Best Practices re: ESI

- ÷ Establish ongoing working relationship with outside counsel so they are equipped to deal with opposing counsel and court early in case to negotiate reasonable ESI scope, preservation, privilege protection, and production issues; and to challenge overly broad and expensive requests .

E-Discovery Golden Rule

Get Control of the Scope of
E-Discovery as Quickly as Possible

Assistance is Available and Ready

Butzel's E-Discovery Team:

- ÷ **Maureen Taylor**, taylor@butzel.com, (313) 983-7494
- ÷ **Deborah Swedlow**, swedlow@butzel.com, (734) 213-3266
- ÷ **Carol Romej**, romej@butzel.com, (248) 593-2098
- ÷ **Tim Labadie**, labadiet@butzel.com, (313) 983-7466
- ÷ **Jim Boutrous**, boutrous@butzel.com, (313) 225-7010

Or contact your regular Butzel attorney

QUESTIONS?

