Electronic Discovery and Litigation Readiness: Litigating Under the New Federal Rules

December 7-8, 2006

Presented by:  Randall L. Erickson, Crowell & Moring
                Stuart J. Einbinder, Crowell & Moring
                Christine E. Cwiertny, Crowell & Moring
                Christopher Wall, Kroll On Track
Overview

- The Risks and Challenges of E-Discovery
- FRCP Amendments
- Pro-active E-Discovery Strategies
- E-Discovery Technologies and Vendors
- Questions
While electronically-stored information ("ESI") has been around for decades, there has been relatively little involvement by the courts in E-Discovery issues until recently because:

» Litigation often focused on historical events
» Sufficient information available in hard copy format
» Lack of sophistication regarding how to engage in E-Discovery
» Litigation equivalent of MAD ("mutually assured destruction")
What is Electronic Discovery?

- The exchange of any discoverable (i.e., relevant, non-privileged) information maintained in an electronic format, including:
  - E-mail
  - Word processing files
  - Presentations
  - Databases
  - Spreadsheets
  - Electronic calendars
What is Electronic Discovery? (cont’d)

How accessible is your data?

- Internal Hard Drives
- Floppy Disks
- PCMCIA Cards
- Notebook Computers
- Personal Digital Assistants
- Microdisks
- Flash USB Devices
- Tape Back-Ups
- External Hard Drives
- Offsite Storage
- Internet
- Digital Voicemail
- Proprietary Systems
- Video Conferences

How accessible is your data?

What is Electronic Discovery?
What is Electronic Discovery? (cont’d)

- But E-Discovery also may include:
  - Digital voicemail
  - Internet and Intranet sites
  - Blackberries and other PDAs
  - Text messages and IM messages
  - Internet blogs, chat rooms, etc.
  - Videoconferences
Challenges

- Increasingly vast quantities and types of electronic information are being created
  - Just 2 years ago, average gigs/custodian ≈ 1 to 3
    - 1 gig ≈ 70,000 pages (≈ 30 boxes)
  - Today, average gigs/custodian ≈ 3.5 to 5+
  - Printed documents comprise less than 5% of documents
Typical e-mail system

- 500 employees x
- 25 e-mail messages per employee per day x
- 250 workings days/year

= 3,125,000 E-mail Messages

(Does not include additional copies of e-mails found on back-up and recovery systems)
Challenges (cont’d)

- **Persistence**: Electronic documents tend to stay around a lot longer
- **Proliferation**: Ease of copying, forwarding and searching exponentially increases volume
- **Volatility**: ESI subject to inadvertent alteration
- Most corporate IT systems are not designed for litigation discovery or regulatory compliance
- Most document retention policies are not litigation focused
One printed Word document can have many electronic copies

<table>
<thead>
<tr>
<th>Description</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 hard drive + 12 monthly backups</td>
<td>13</td>
</tr>
<tr>
<td>3 internal recipients</td>
<td>39</td>
</tr>
<tr>
<td>5 drafts reviewed by recipients</td>
<td>195</td>
</tr>
<tr>
<td>E-mail used to circulate drafts and final of the document</td>
<td>Over 1,000</td>
</tr>
</tbody>
</table>
Whereas paper documents are found in limited locations that can be readily identified, electronic information resides in many locations, such as:

- Office servers
- Desktops
- Laptops
- Home computers
- Portable media (disks; jump drives)
- PDAs
- Web servers
- Digital cameras
- Back up tapes
- Other archival systems
Metadata = information about an electronic document that is not visible on the face, but is embedded within the document, such as:

- Dates on which document was created, modified, accessed and printed
- Track changes in Office-suite documents
- Spreadsheet formulas
What Does Metadata Look Like?

- **Title:** Electronic Discovery
- **Subject:** Litigation Readiness Planning Under the New Rules
- **Author:** Justin Murphy
- **Company:** Crowell & Moring LLP
Why Does Metadata Matter?

Metadata may expose critical details:

» Alterations to document text may be exposed by hidden metadata
» Track changes describe the development of a document over time
» The actual date on which a document was created may be ascertained
» The actual account used to send an e-mail may be discovered
Consequences

- Custodians may retain documents despite document retention policies
- Archival systems may maintain far more data than necessary for business purposes
- Litigation hold orders very difficult to implement without clear understanding of where potentially responsive data resides
- Potentially responsive documents may be inadvertently destroyed
- E-Discovery requests may be handled inconsistently across the enterprise
Why Does It Matter?
Potential Outcomes

- Courts increasingly intolerant of E-Discovery errors/omissions
  - Penalties for failure to preserve
    - Monetary Sanctions
    - Adverse Inference Charge – presume evidence destroyed goes to the merits of the case and is adverse
    - Preclusion of Evidence
    - Default Judgment
- Difficulty meeting tight litigation deadlines
- Problematic documents surface in discovery
- Decisions regarding the method and manner of collecting, reviewing and producing e-documents impact the key substantive issues in the case
- Discovery costs can skyrocket due to more documents
MISTAKES

It could be that the purpose of your life is only to serve as a warning to others.

- Despite an SEC regulation requiring email retention for two years, Morgan Stanley overwrote emails, failed to timely process hundreds of backup tapes, and failed to produce email attachments and email.

- The court noted Morgan Stanley “gave no thought to using an outside contractor to expedite the process of completing the discovery, though it had certified completion months earlier; it lacked the technological capacity to upload and search the data at that time, and would not attain that capacity for months.”

- The court issued an adverse inference instruction, noting “[t]he conclusion is inescapable that [the defendant] sought to thwart discovery.” In May 2005, relying on that instruction, the jury awarded $1.45 billion in total damages against Morgan Stanley.
Real Outcomes

- **Zubulake v. UBS Warburg**
  - Series of E-Discovery rulings, including preservation obligations (esp. back-up tapes) & standards for cost shifting to requesting party
  - Adverse inference instruction as a sanction + costs of new depositions, motion, and restoring documents
  - In-house and outside counsel have an affirmative and continuing duty to monitor compliance with “hold” orders and that all documents in possession of business persons have been produced
  - **$29.3 million judgment** (compensatory and punitives)

- **U.S. v. Philip Morris**
  - Failure to turn off e-mail auto-delete and failure of employees to retain relevant e-mail results in:
    - All witnesses who failed to abide by the order and document retention precluded from testifying
    - **$2.75 million fine** + cost of deposition on e-mail destruction
AdvantaCare Health Partners v. Access IV

» Employee took proprietary info from employer, covered up those efforts, and started competing business

» Court grants default judgment where co-defendant wiped two hard drives clean, continued deleting files after court had issued sanctions order for destruction of electronic evidence, and did not delete former employer’s proprietary info after ordered to do so. Thousands of former employers’ files found on office and home computers.

» Default judgment also applied to co-defendant, who did not engage in misconduct, because she left compliance with the court’s orders up to her colleague
Real Outcomes (cont’d)

- **Williams v. Sprint**
  - Court considers sanctioning defendant for locking cells and cleaning metadata in Excel spreadsheet after magistrate ordered production in electronic format as kept in the ordinary course
  - If responding party has concerns about privileges or misuse of data by requesting party, must make an objection; cannot unilaterally “scrub” metadata
The Rules Governing Electronic Discovery
When does the duty to preserve begin

» May well be prior to receipt of complaint

» Arises when a party is aware or should be aware that evidence in its possession or control is relevant to existing or potential litigation.

» Litigation must be probable, not merely possible.

» Duty exists even in the absence of any preservation order or discovery request.

- FRCP Amendments do not change the duty to preserve
Duty of Preservation (cont’d)

- Who has obligation to preserve
  - “Possession, custody, or control”
  - May be more than just employees – may include subsidiaries and affiliates; agents; lawyers; other third parties
  - What about 3rd parties?
- Steps to ensure preservation/avoid spoliation
  - Document retention policies
  - Hold orders
- Risks/penalties of spoliation
Parties should attempt to reach agreement on:

» Extent and definition of preservation obligation
» Identification of responsible persons
» Form and method for notifying document and data custodians of their preservation obligations
» Mechanism for monitoring, certifying and auditing compliance
» Modifying routine business procedures, particularly with respect to electronic data
» Protecting volatile electronic materials
» Cost of preservation, including possible sharing
» Updating agreement as discovery progresses
Supreme Court approved amendments to FRCP addressing E-Discovery issues on April 12, 2006
Amendments effective December 1, 2006
In general, amendments take a reasonable and balanced approach to addressing burdens and risks associated with E-Discovery
E-Discovery Issues Addressed At Outset of Case

» Rule 26(a)(1)(B): Adds mandatory disclosure obligation regarding categories and locations of electronic information

» Rule 26(f)(3): Parties are directed to discuss E-Discovery issues at the initial conference
  • Including form of production and preservation
  • Form 35 calls for a report to the court on this discussion

» Rule 16(b): Court should address provisions for E-Discovery in initial scheduling order
Form of Production -- Rule 34(b)

» Requesting party may specify form of production – “native format” issues (including metadata)

» If not specified, producing party may produce in form “ordinarily maintained” or “reasonably usable”

» If ordinarily maintained in searchable format, should be produced in searchable format
Inadvertently Produced Privileged Material

» Rule 26(b)(5)(B): Party may assert privilege after production, which if disputed can be resolved by court

» Rule 26(f): Adds to discovery plan the parties’ proposal for court to enter order adopting their agreement on waiver

» Rule 16(b): Provides for court to address parties’ agreement re privilege waiver in scheduling order

However, privilege waiver issue not resolved
“Reasonable” Standards

- Rule 26(b)(2)(B): Party need not produce electronic information that is “not reasonably accessible because of undue burden or cost”
  - Can be overcome by “good cause”
  - Court can order cost shifting
  - Applies to production, not preservation

- Rule 37(f): Court will not impose sanctions for failing to produce electronic information lost as a result of routine operation of IT systems
  - Subject to preservation obligations
Amended FRCP 45 – 3d Party Discovery

- Similar provisions to Rules 26 and 34
- Third party only required to produce “reasonably accessible” ESI
- Requesting party must file motion challenging claim of not reasonably accessible
- For “good cause,” court may still order production even if information is not “reasonably accessible”
- Similar provisions regarding production of privileged information
Government agencies have very specific requirements for E-Discovery -- e.g., DOJ definition of a “document”

» “all written, recorded, and graphic materials and all electronic data of every kind . . . includes electronic correspondence, . . . metadata, embedded, hidden and other bibliographic or historical data describing or relating to documents created, revised, or distributed on computer systems. . . .”

» “data stored in personal computers, portable computers, workstations, minicomputers, personal data assistants, archival voice storage systems, group and collaborative tools, electronic messaging devices, portable or removable storage media, mainframes, servers, backup disks and tapes, archive disks and tapes, and other forms of online or offline storage, whether on or off company premises”
California’s Code of Civil Procedure §2017.710 et seq. provides for the use of technology in conducting discovery

» Upon stipulation of the parties or an order of the court, discovery may be conducted and maintained in electronic media and by electronic communication

» Procedures adopted must promote cost-effectiveness and efficiency, but may not impose an undue burden upon any person
Discovery under California law

- Bearing costs of electronic discovery
  » “If necessary, the responding party at the reasonable expense of the demanding party shall, through detection devices, translate any data compilations included in the demand into reasonably usable form.” Cal. Code of Civ. Proc. §2031.280(b)
  » Based on Cal. Code of Civ. Proc. §2031.280(b), demanding party must pay “reasonable” expense incurred by responding party for a “necessary” translation of data from back-up tapes into reasonably usable form

Duty to Preserve

» Corporations may destroy documents for which they anticipate no further need pursuant to a routine document retention policy
  • Policy must be reasonable given facts and circumstances surrounding the relevant documents
  • Policy must be instituted in good faith
Discovery under California law

- Duty to Preserve
  - Filing of complaint
    - Duty may also be triggered by pre-litigation correspondence between counsel for the parties
  - Contemplation of litigation, rather than mere possibility
    See Willard, supra
  - Party knows or should know that documents will be material at some point in future
    See Willard, supra, citing Lewy v. Remington Arms Co., Inc. (8th Cir. 1988) 836 F.2d 1104
Discovery under California law

- Sanctions for spoliation of evidence
  - Charge of obstruction of justice (Cal. Pen. Code §135)
  - Adverse inference instruction (Cal. Evid. Code §§412, 413)
Proactive E-Discovery Strategies
Litigation Readiness Planning – I

- E-Discovery Audit
  - Assess corporate litigation vulnerabilities
  - Collect and review information management and document retention policies
  - Map corporate information management infrastructure
  - Identify custodians and sources of data relevant to high-risk litigation
  - Audit select custodians to identify compliance with corporate policies
  - Plan for designated corporate witness
Importance of combined effort among IT, affected business units, and litigation counsel

- Litigation counsel rarely have in-depth knowledge or understanding of company’s information systems and storage.
- IT personnel rarely have understanding of the legal issues and obligations.
- Only the users know how systems are actually used
Litigation Readiness Plan includes:

- Plan for identifying relevant custodians and data sources
- Plan for implementing document preservation orders
- Detailed, technical plan for collecting potentially relevant electronic material
  - E-Mail servers
  - Local drives
  - Shared drives
  - Internet/Intranet sites
  - Other
Risk Reduction Strategy – Corporate Content Policy

- Rules governing acceptable content for electronic documents
- Particularly applicable to e-mail, IM and blogs
- More than etiquette -- a serious attempt to reduce the risk of inflammatory and damaging content
- Commercially available software can search and monitor e-mail and e-documents for problematic words, phrases and concepts
- Oversight responsibility of Compliance Officer
Risk Reduction Strategies –
Documentation and Designation

» Document both preservation and collection processes

» Designate “owner” of both the preservation and collection processes

» Consider designated “owners” to maximize consistency across different cases

» Consider designated corporate ESI witness/witnesses to maximize consistency and to develop expertise
Risk Reduction Strategy – Document Retention Policy

» Establish rules governing retention of paper and electronic information – for systems and individual users
» Implement rules at the IT system level and make no exceptions
» Effectively (and often) communicate rules to individual users
» Enforce policy as part of corporate culture
» Suspend rules on advice of counsel in the event of litigation or investigation
» Assign an owner (Compliance Officer?) to the policy to ensure it is kept current and enforced
ESI Preservation – Avoid Spoliation

- Implement Litigation Hold Order
- Timing:
  - Issue as soon as litigation is reasonably anticipated.
  - May issue a “blanket” order first to ensure immediate preservation and follow up with more detailed order.
  - Periodically re-issue the litigation hold.
  - Monitor on-going compliance.
- Sender:
  - Someone with corporate clout, e.g. General Counsel, compliance officer, etc.
Preservation Strategies

- **Recipients:**
  - Communicate directly with key witnesses and custodians about their preservation obligations.
  - Do not rely on “cascading” – *i.e.*, relying on high level personnel to advise their peers and subordinates.
  - Direct recipients to convey to counsel names of potential witnesses and custodians who did not receive the order.

- **Scope:**
  - Define potentially relevant information.
  - Explain better to be over inclusive than under inclusive.
  - Emphasize that the order trumps any company record retention policies.
E-Discovery Technologies and Vendors
Dealing with E-Discovery Vendors

- **Preservation / Collection**
  - Increasing need for IT witness on preservation and collection issues
  - Collection methods must preserve all metadata
  - Outsource to vendor or use in-house IT expertise?

- **Processing / Production**
  - Price and quality can vary dramatically
  - Commodity business with many capable providers
  - Often tied to hosting services
E-Discovery Technologies and Vendor Selection

- **Review / Hosting**
  - Latest trend: Concept categorization (a/k/a “Intelligent Review”)
  - Match the application to the project needs (one size does not fit all)
    - Volume of material / timeline for production
    - Method of review
    - Amount of coding
    - Lifespan of project
- Mix and match the services and vendors best suited for your project
- Negotiate your own deal
Questions?
Contact Information

- **Randall Erickson**
  - 949-263-8400
  - rerickson@crowell.com
- **Stuart Einbinder**
  - 949-263-8400
  - seinbinder@crowell.com
- **Christine Cwiertny**
  - 949-263-8400
  - ccwiertny@crowell.com
- **Christopher Wall**
  - 703-668-1357
  - cwall@krollworldwide.com