E-discovery in Today's Construction Environment: Guidelines for Documentation

November 15, 2006

Presented by: Stuart Einbinder, Crowell & Moring
Christine Cwiertny, Crowell & Moring
Christopher Wall, Kroll Ontrack

crowell moring

Overview

- The Risks and Challenges of E-Discovery
- FRCP Amendments
- Pro-active E-Discovery Strategies

The New World of ESI

- 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

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)*

- Internal Hard Drives
- Floppy Disks
- PCMCIA Cards
- Notebook Computers
- Personal Digital Assistants
- Microdisks
- Flash USB Devices

How accessible is your data?

- Tape Back-Ups
- External Hard Drives
- Offsite Storage
- Internet
- Digital Voicemail
- Proprietary Systems
- Video Conferences

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

Challenges (cont'd)

Typical e-mail system

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

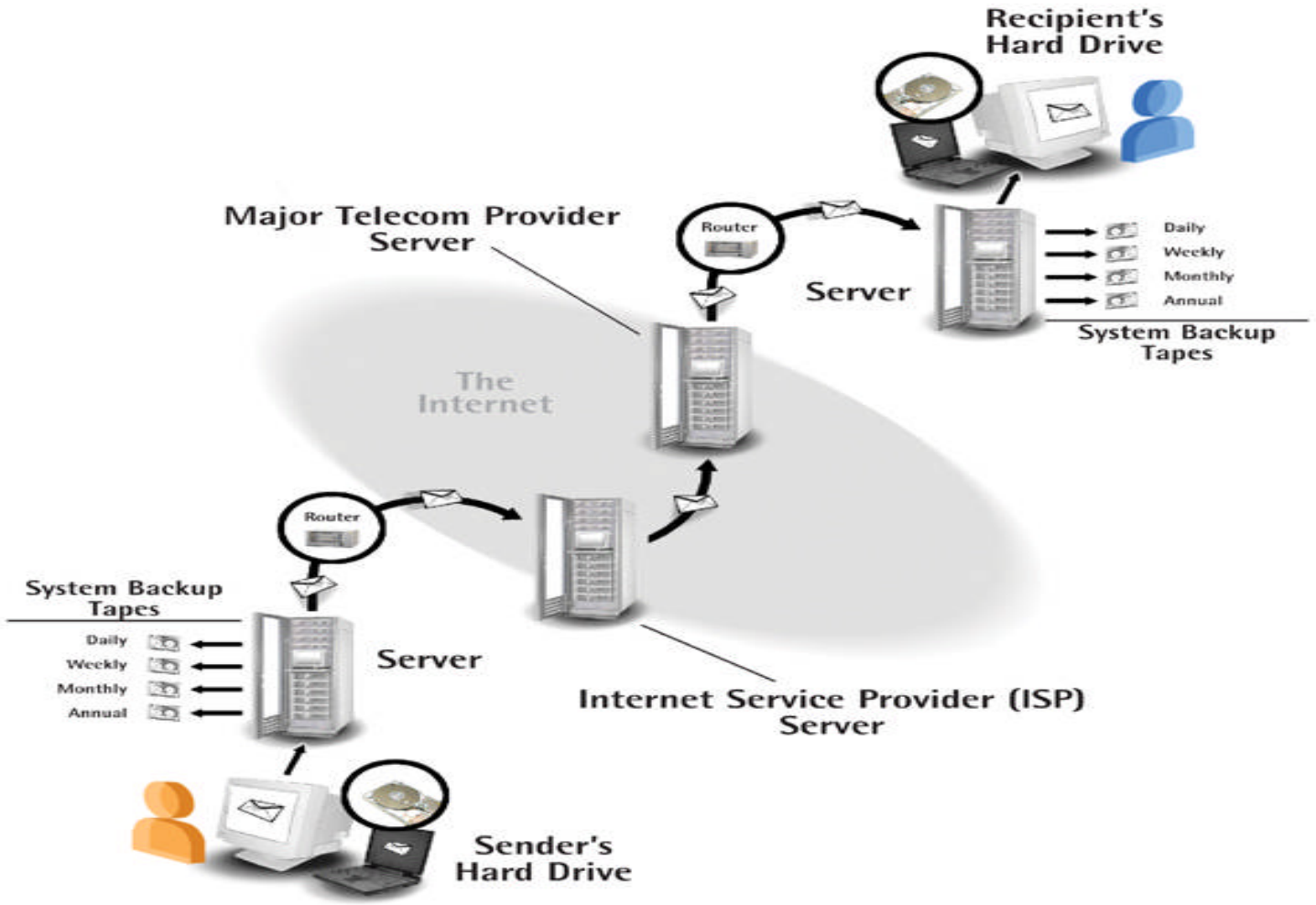
= 3,125,000 E-mail Messages

(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

Challenges


Recipient's Hard Drive
Major Telecom Provider Server
Router
Server
Daily
Weekly
Monthly
Annual
System Backup Tapes
The Internet
Router
System Backup Tapes
Daily
Weekly
Monthly
Annual
Server
Internet Service Provider (ISP) Server
Sender's Hard Drive

Challenges (cont'd)

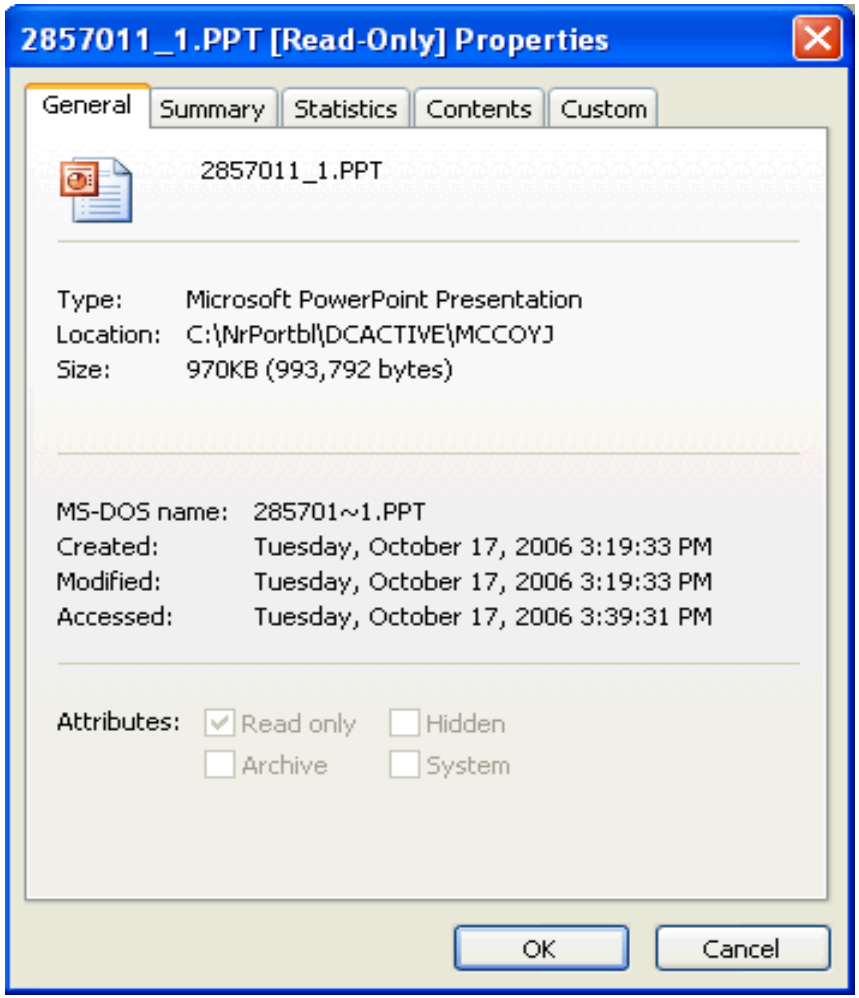
One printed Word document can have many electronic copies

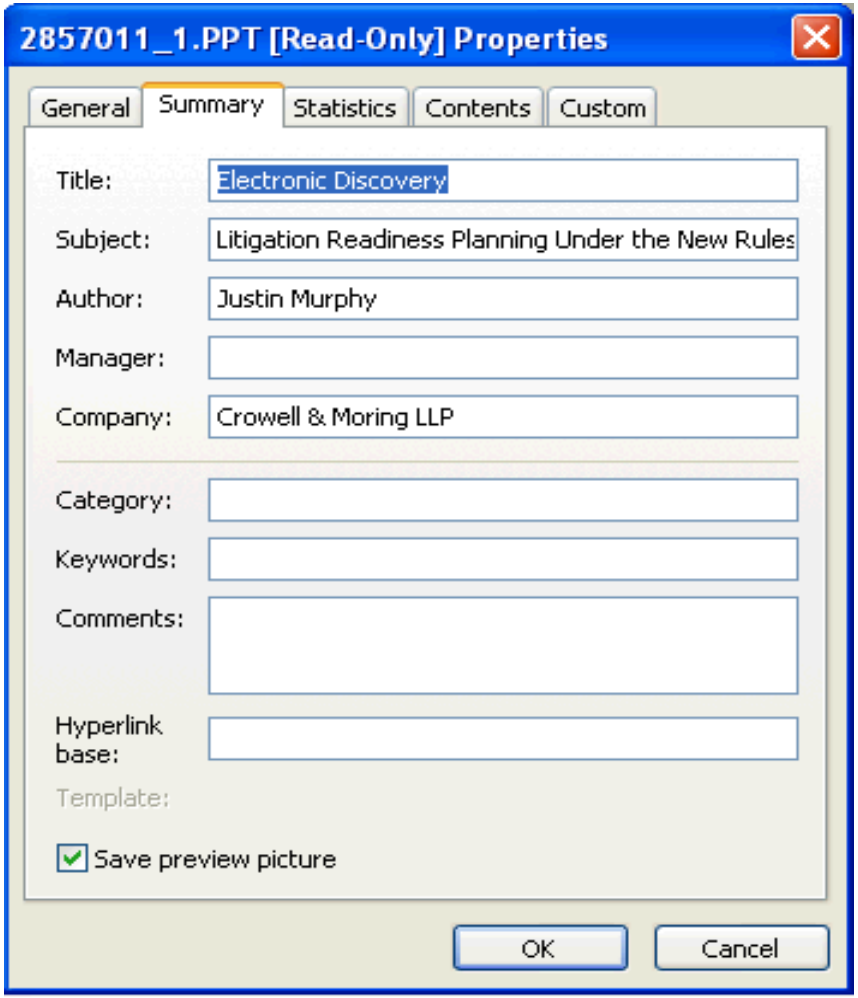
1 hard drive + 12 monthly backups	13
3 internal recipients	39
5 drafts reviewed by recipients	195
E-mail used to circulate drafts and final of the document	Over 1,000

The Additional Challenge of Metadata

- 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?





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

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
- 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.

Real Outcomes

Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc.

- 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
  - **$29.2 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

Real Outcomes (cont'd)

- 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

The Rules Governing Electronic Discovery

Duty of Preservation

- 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.

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
- Steps to ensure preservation/avoid spoliation
  - Document retention policies
  - Hold orders

The New Amendments to FRCP

- 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

Amended FRCP 26 & 16 – "Frontloading"

- 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

Amended FRCP 34 – Form of Production

- 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

Amended FRCP "Reasonability" Standards

- "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

Proactive E-Discovery Strategies

Litigation Readiness Planning – I

- E-Discovery Audit
  - » Assess corporate litigation vulnerabilities
  - » Collect and review information management and document retention policies
  - » Identify custodians and sources of data relevant to high-risk litigation
  - » Audit select custodians to identify compliance with corporate policies

Litigation Readiness Planning - II

- 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 Planning – III

- Litigation Readiness Plan includes:
  - » 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.
  - Periodically re-issue the litigation hold.
  - Monitor on-going compliance.
- Sender:
  - Someone with corporate clout, *e.g.* General Counsel, compliance officer, etc.

Contact Information

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