Electronic Discovery: Litigation Holds, Data Preservation and Production

April 27, 2010

Daniel Munsch, Assistant General Counsel
John Lerchey, Coordinator for Incident Response

E-Discovery Rules

- Federal Rules of Civil Procedures amended effective December 1, 2006 formally making Electronically Stored Information (ESI) subject to discovery (E-Discovery) and imposing new institutional obligations
- Must show that we have policies / practices in place to demonstrate that “we are doing the right things and have the audit trail to prove it”

Key E-Discovery Requirements -1

- Must preserve historical and prospective ESI from destruction
- Must provide description by category and location of all ESI in our control which may be relevant to the case
- Must produce ESI in original format if relevant, not privileged, and reasonably accessible

Key E-Discovery Requirements -2

"Counsel has the duty to properly communicate with its client to ensure that 'all sources of relevant information [are] discovered' . . . To identify all such sources, counsel should 'become fully familiar with [its] client's document retention policies, as well as [its] client's data retention architecture' . . . This effort would involve communicating with information technology personnel and the key players in the litigation to understand how electronic information is stored." *Phoenix Four, Inc. v. Strategic Resources Corp.*, 2006 WL 1409413 at *5 (S.D.N.Y., May 23, 2006) (*quoting Zubulake v. UBS Warburg LLC*, 229 F.R.D. 422, 432 (S.D.N.Y. 2004) ("*Zubulake V*")).

Short Summary

- "By now, it should be abundantly clear that the duty to preserve means what it says and that a failure to preserve records -- paper or electronic -- and to search in the right places for those records, will inevitably result in the spoliation of evidence." *The Pension Comm. of Univ. of Montreal Pension Plan et al v. Banc of America Securities, LLC, et al.*, 05 Civ. 9016 (S.D.N.Y. 2010).

Risks Associated with Spoliation of Evidence

A finding of spoliation can lead to:

- Sanctions - fines / penalties
- Adverse inference instruction to jury
- Reversal of burdens of proof
- Dismissal of claims or defenses
- Ultimate loss of the case (monetary judgment, injunctive relief, loss of IP, etc)
- Damaged reputation
- Can’t afford one bad precedent . . .

Examples . . .

- *Coleman Holdings v. Morgan Stanley* (Florida Cir. Ct. 2005) – Court in effect reversed burden of proof against *Morgan Stanley* in fraud case; Jury returned verdict for plaintiff of 1.5 billion dollars; Court awarded 15 million dollars in fines for failure to comply with discovery obligations.

- *Zubulake v. USB Warburg* (SDNY 2004) – adverse inference instruction (emails not produced would have negatively impacted case); defense counsel partly to blame for not locating and producing emails; $29 million damages awarded to plaintiff by jury.

- *U.S. v. Philip Morris USA, Inc.* (D.D.C. 2004) – Defendants ordered to pay costs related to spoliation of relevant e-mails in addition to $2.75 million in monetary sanctions. Key employees precluded from testifying.

- *TR Investors v. Genger* (Del. Ch. Dec. 2009) – Defendant was sanctioned for "wiping" the unallocated space on his company's computer server despite a court order barring any disposal of company-related documents. The sanctions included a raised burden of proof for defendant on any defense or counterclaim, production of documents that defendant claimed were privileged, and payment of plaintiffs' reasonable attorney fees and costs, which the court suggested should be $750,000.

Our Challenges

- Rules of Civil Procedure do not dictate how to hold, preserve, and search ESI.
- The “double-edged sword” of being Carnegie Mellon
- Computing environment at Carnegie Mellon
  - Distributed, ephemeral, disparate, outsourced, ...
- Many sources of relevant ESI
- Non-standard practices (e.g. retention)
- New technologies don’t work in our environment
- Resources, skills, tools, and processes for preserving, targeting, and harvesting ESI

Role of OGC and ISO

- Office of the General Counsel ("OGC")
  - Determine when litigation is anticipated
  - Determine who may possess potentially relevant ESI and issue litigation holds to those individuals.
  - Coordinate preservation and production of ESI
  - Review ESI for legal necessity, relevancy and privilege
- Information Security Office ("ISO")
  - Become familiar with relevant computer architecture
  - Act as University's technical witness in court
  - Coordinate technical process and procedure with departments and individuals.
  - Preserve information on centralized computer systems

E-Discovery Process

Preservation

1. Anticipated litigation
2. OGC issues a litigation hold
3. Recipients of the litigation hold preserve potentially relevant ESI

Production

4. OGC, ISO, departmental IT staff and litigation hold recipients work together to search for and collect potentially relevant ESI
5. OGC Reviews ESI for legal necessity, relevancy and privilege
6. Relevant Non-privileged ESI Produced to Opposing Counsel

Litigation Holds

- When litigation is “reasonably anticipated,” the OGC will issue Litigation Hold Memos to any faculty or staff members who may possess potentially relevant ESI.
- You may receive a litigation hold directly from the OGC or it may be forwarded to you by a supervisor or a colleague.
- Appropriate systems administrators and other IT staff are typically included on litigation hold distributions.

Litigation Holds

- What information is provided in a litigation hold memo?
  - Identity of the parties to the litigation
  - Brief description of the legal claims
  - Explanation of the scope of the litigation hold
  - Likely sources of potentially relevant ESI
  - Generalized technical advice about how to protect and preserve potentially relevant ESI.

Sources of ESI

- Potentially relevant evidence may be stored in any computer or electronic device that you use for any work related purpose
- Examples
  - Local disk / hard drive
  - Shared storage
  - Backup systems
  - PDA & cell phones
  - Removable media (CDs, DVDs, flash drives, etc.)

Sources of ESI

- Potentially relevant evidence may be stored contained in a variety of file types such as:
  - Email
  - Databases
  - Electronic documents (Word, Excel, text files, program code, etc.)
  - Voicemail
  - Text messages
  - Calendars

Preserving ESI

- Potentially relevant ESI must be preserved in its original electronic form, so that all information contained within it (including metadata) may be available for inspection.
- The Information Security Office and your departmental IT staff will assist you in preserving relevant information.
- What does this mean?
  - Do not delete potentially relevant information
  - Do not alter potentially relevant information
  - Suspend any automatic deletion / overwriting
  - Consult with IT staff or ISO before upgrading to a new computer or discarding an old computer.
  - Printing out documents IS NOT sufficient.

Recommended User Practices

- Send business related email using a Carnegie Mellon email account or a departmental email account.
- Organize data using separate folders for business related and personal data. Further separations such as filing by project or topic can help to isolate related items.
- Be aware of what systems are used to store your data.
- Know whether or not your data is being backed up.
- Configure dual delivery when forwarding business related email to a personal email account.
- If using a mobile device for email, be sure to "cc" your university or departmental account on all university business correspondence.

Computing Infrastructure & Production

- As the case proceeds, OGC and ISO will work with you and your departmental IT staff to analyze your computing structure.
- Representatives from the OGC and ISO may meet with you to develop a better understanding of ESI in your possession, custody or control.
- OGC and ISO will also work with you to develop a plan for searching and producing ESI.
- Before being produced to opposing counsel, all ESI will be reviewed by the OGC for legal necessity, relevancy and privilege.

How long will this last?

- A litigation hold will remain in effect until the statute of limitations has expired with respect to an anticipated claim or – if litigation has commenced – when the lawsuit and all appeals have been concluded.
- It is not uncommon for a litigation hold to remain in effect for several years.
- It may also take months or years to move from the preservation stage of e-discovery to the production stage.

Reminders & Withdrawals

- From time to time the OGC will issue reminders via emails about the status of active litigation holds. Typically such reminders are issued annually or biannually.
- Litigation holds remain in effect until withdrawn by the OGC.
- Withdrawing a Litigation Hold
  - Judicial resolution
  - Settlement
  - Statute of limitations

Thank You

Questions or Comments?

For more information visit www.cmu.edu/iso/compliance/e-discovery/index.html