Best Practices in eDiscovery
ACC – Dallas
March 29, 2007

Moderator: Jack Halprin, Esq. | Sr. eDiscovery Product Manager
jack.halprin@guidancesoftware.com
Participants

- **J. Wes Billingsley, Esq.**
  - Counsel, Thompson & Knight LLP

- **Daniel Lim, Esq.**
  - Assistant General Counsel, Guidance Software

- **Charles Ross**
  - Senior Manager, Risk Management, McAfee, Inc.
Agenda

What are the practical effects of the new eDiscovery amendments and how can you ensure compliance, reduce costs and mitigate additional corporate risk?

- How do you ensure that your company’s preservation processes stand up to challenges from opposing counsel at the Rule 26 conferences?
  - How has the duty to preserve ESI been interpreted?

- How can the right tools keep you in the Rule 37(f) “safe harbor” and help you craft an effective records management program?
  - What protection can you expect from the safe harbor provision?

- How can the right internal tools help you meet the challenges of the FRCP amendments and reduce corporate risk?
  - What should be the impact of forensics in eDiscovery and investigations?

- How can a company-wide eDiscovery solution slash your costs and virtually eliminate the need for outside vendors?
Selected Amendments to the FRCP:

- **Early Attention:**
  - Rule 16(b): Pretrial Conference
  - Rule 26(f): Discovery planning conference
  - Rules 33 & 34: Speak to form of production for ESI

- **Systemized Process:**
  - Rule 37(f): “Safe harbor” from sanctions
  - Rule 26(b): Reasonably Accessible Data (backup tapes) & “clawback provision”
  - Rule 34(a): Opponent access to network absent defendable process

- Unchanged from before: The preservation duty applies **only** to relevant data
Rule 16(b): Pretrial Conferences: Scheduling & planning

- **Rule 16(b)(5):** provisions for disclosure or discovery of electronically stored information

- **Rule 16(b)(6):** any agreements the parties reach for asserting claims of privilege or of protection as trial preparation material after production

- **Rule 26(f):** Discovery planning conference, disclosure or discovery of ESI, and form of production. Also adds these topics to the discussion:
  1. “to discuss any issues relating to preserving discoverable information”
  2. “any issues relating to disclosure or discovery of electronically stored information, including the form or forms in which it should be produced;”
Duty to preserve extends to only potentially relevant information.

- “Clearly [there is no duty to] preserve every shred of paper, every e-mail or electronic document, and every backup tape…Such a rule would cripple large corporations.” Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 217 (S.D.N.Y. 2004) (“Zubulake IV”)

- “The duty to preserve evidence, once it attaches, does not extend beyond evidence that is relevant and material to the claims at issue in the litigation.” Hynix Semiconductor Inc. v. Rambus Inc., 2006 WL 565893 (N.D.Cal. Jan. 5, 2006) at *27.
Rule 37(f): Safe Harbor: no penalties when ESI deleted due to routine operation of IT Systems, if reasonable preservation steps taken

- Procedures must be: established, documented, and operational
- Systemized framework for early attention (preservation/“litigation hold”) must be in place

Addresses sanctions, not preservation
How Deep is the Harbor?

- Absent “exceptional circumstances”
- Affects only “sanctions” “under the rules”
- Routine operation of computer systems
- Good faith undefined, but…
  - Must comply with court order, or agreement
  - May require intervention to modify or suspend routine operation to prevent loss
  - May require intervention to prevent loss of information on sources not reasonably accessible
Defensable Process?
Custodian Self-Collection in the Courts

  - “It is not sufficient . . . for a company merely to tell employees to 'save relevant documents,'... this sort of token effort will hardly ever suffice.”
  - Court faults “the lack of specificity in defining what documents would be relevant to litigation”

  - Court demands Company outline steps taken to preserve, search and collect ESI in response to discovery request
  - “That data pertinent to this litigation was not preserved, and appears to have been destroyed . . . is neither comprehensible nor acceptable”

  - Court states that “Health Net’s process for responding to discovery requests was utterly inadequate”
  - “Health Net relied on the specified business people within the company to search and turn over whatever documents they thought were responsive, without verifying that the searches were sufficient. The process, in sum, was one of looking for selected specific documents by a specific person rather than all responsive documents from all Health Net employees who had such documents. Many of these specific employee-conducted searches managed to exclude inculpatory documents that were highly germane to Plaintiffs’ requests.”
Records Management Initiatives are no longer an option!

- Based on the amended Federal Rules:
  - Without a defensible, systemized, and repeatable process for dealing with ESI, corporate defendants can be subject to huge penalties under Rule 37(f): Safe Harbor

- A corporate RMI will make the eDiscovery process easier, cheaper, faster.

- A RMI will give the corporation knowledge of its ESI

- A good forensics tool can help achieve the goals of a systemized, defensible, repeatable process
GOAL: Preserve Forensically Sound Copy of Evidence

SOLUTION: Digitally capture & tag evidence

- Capture an exact copy
  - Prove with hash value
- Prove the data doesn’t change between the point of capture and trial
  - Proper chain of custody
PROACTIVE APPROACH REQUIRED:

- Rule 26(a)(1)(B) requires a description by category and location of all ESI
- Rule 30(b)(6) witness
  - required to know nature and extent of enterprise ESI
- Use forensics tools to be proactive:
  - Know and understand the enterprise
- Be prepared under the FRCP
  - Records Management Initiative or Document Retention Policy
Forensically sound data collection tools are required

- To work in conjunction with:
  - Records Management Initiatives & ECM & Email Archiving Solutions

- Forensically sound tools allow:
  - IT & Legal to maintain control over the enterprise data
  - Find data across the enterprise
  - A collection process in compliance with the Federal Rules

- **What is Forensically Sound: Daubert/Frye test:**
  - Has the theory or technique:
    - been reliably tested;
    - been subjected to peer review and publication;
    - Have a known or potential rate of error for the method used;
    - been generally accepted by the scientific community.
Benefits of Bringing the Process In-House

Key benefits:

- Ownership & Control over the process and enterprise data
- Repeatable & Defensible Process
  - Court validated search & collection tools
  - Decrease spoliation risks
- Reduced overall costs
  - Less business interruption
  - Faster response times
  - Fixed Cost: Lower Short & Long Term Costs
  - Remote Collection & Culling at Point of Collection
    - Cuts travel expenses and reduces/eliminates interruption to business
Defensible & Repeatable Process

In-House eDiscovery allows for a repeatable process

- In conjunction with a Records Management Initiative/Records Retention Plan
- Ownership of solution allows for same procedures each time
- Compliance with Rule 37(f)---safe harbor for repeatable defensible process
- Preparation for early attention requirements and pretrial conferences
- Prevent eDiscovery fire drill with a proactive approach
“To the extent that it may not be feasible for counsel to speak with every key player, given the size of a company or the scope of the lawsuit, counsel must be more creative. It may be possible to run a system-wide keyword search; counsel could then preserve a copy of each "hit." [FN75] Although this sounds burdensome, it need not be. Counsel does not have to review these documents, only see that they are retained. For example, counsel could create a broad list of search terms, run a search for a limited time frame, and then segregate responsive documents. . .

**FN75.** It might be advisable to solicit a list of search terms from the opposing party for this purpose, so that it could not later complain about which terms were used.
Current Practice of Outsourced eDiscovery: Downsides

Outsourcing is not the most effective method:

- High Costs (up to $3500 per GB or more to process & collect data)
- Inefficient, redundant steps taken
- Usually Outsourced, Managed by Outside Counsel
- Results in Poor Relationship Between Legal and IT
- Not Tied to Records Management Initiatives
- No institutional memory: no carryover of process

May Not be in Compliance with the New Federal Rules
An effective in-house eDiscovery process with the proper forensics tools, alongside a Records Management Initiative can:

- **Save Time**
  - RMI & Forensics tools allow you to know where the ESI is stored

- **Reduce Effort**
  - Knowing where the ESI is reduces efforts required for collection/preservation

- **Eliminate or Reduce Consultant/Service Provider Fees**
  - In-house process utilizes Legal & IT to complete the collection

- **Prevent Sanctions**
  - Protection under 37(f) safe harbor

**Comply with the FRCP amendments**
Case Study 1:

- Document production request in a civil litigation matter
  - 1050 workstations and a dozen file servers connected (approximately 28 terabytes in aggregate)
  - Required to collect all user PST files on workstations; and search all user created data for keyword terms and collect responsive files
  - With Systemized Process: 2 weeks, $140k, no disruption
  - Non-Systemized (Outsourced): 3 months $3.5 million, extensive business disruption
Case Study 2:

- **Document Collection for Class Action Lawsuit:**
  - National Corporation: approx. 1100 custodians @ 120 locations
  - Collection parameters called for an inclusive search, with forced collection of all PDF’s, Tiff’s, and PST’s. PLUS 1100 Exchange mailboxes, 1100 file shares, and post collection culling

- **Without In-House Solution (Outsourced):** Requires full forensic image of each workstation drive plus extensive business disruption: Estimated cost of minimum $4 million

- **With In-House Solution:** Actual Cost of $280k, no business disruption
  - Client will recoup the entire cost of the software, which it now has in house for future collections, during the initial engagement.
  - At the end of process, client has carry-over benefits towards handling the next case.
Additional Benefits of eDiscovery/Forensics Tools: Enterprise Investigative Capability

- You’ve built or are looking to build:
  - A systemized framework for collecting and analyzing information from people and systems in effort to reduce risk
  - The ability to quickly get answers in a way that is in line with the law and recognized best practices
  - The ability to preserve information in a forensically sound way

- Forensically sound eDiscovery tools allow:
  - IT & Legal to maintain control over the enterprise data
  - Find data across the enterprise
  - A collection process in compliance with the Federal Rules
Forensics tools have many uses beyond eDiscovery

- **Records Retention Audits**: Forensics tools can be used to search for and identify different forms of ESI across the enterprise

- **Compliance Enforcement**: Forensics tools can assist by identifying, collecting and removing files that are determined to violate an organization’s policies

- **Data Leakage**: A good forensics product can scan for credit card numbers, social security numbers, etc.

- And…
Fraud Detection and Mitigation: Financial Auditing/Fraud & Employee Investigations

Intellectual property issues such as:
- Corporate espionage
- Quarterly Financials & Marketing plans
- M&A
- Research data theft

Employee integrity
- Employee misconduct
- Policy violations
- Harassment or other employee confrontations
- Inappropriate content

Policy
- Computer use
- Conduct
- Document control

Regulatory compliance
- SOX
- GLBA