



Education

How E-Discovery Will Affect Your Life as a Storage Professional

David Stevens, Carnegie Mellon University

- The material contained in this tutorial is copyrighted by the SNIA.
- Member companies and individual members may use this material in presentations and literature under the following conditions:
 - ◆ Any slide or slides used must be reproduced in their entirety without modification
 - ◆ The SNIA must be acknowledged as the source of any material used in the body of any document containing material from these presentations.
- This presentation is a project of the SNIA Education Committee.
- Neither the author nor the presenter is an attorney and nothing in this presentation is intended to be, or should be construed as legal advice or an opinion of counsel. If you need legal advice or a legal opinion please contact your attorney.
- The information presented herein represents the author's personal opinion and current understanding of the relevant issues involved. The author, the presenter, and the SNIA do not assume any responsibility or liability for damages arising out of any reliance on or use of this information.

NO WARRANTIES, EXPRESS OR IMPLIED. USE AT YOUR OWN RISK.

➤ How E-Discovery Will Affect Your Life as a Storage Professional

- ◆ Mention the term E-Discovery to a storage professional and watch their reaction. They may run away and hide. Storage Professionals today face the daunting task of being able to quickly know where every email, word document and database file lives and how to get it back in a hurry in the event of a catastrophe. With the recent update to the Federal Rules of Civil Procedure (FRCP) a storage professional now has even more pressure to potentially know the content inside those files.
- ◆ This session helps the storage professional understand the new Federal Rules of Civil Procedure (FRCP) that were recently updated. We will also look at an e-discovery request from the perspective of a storage professional. Finally, we will provide some recommendations on how to prepare for an e-discovery request.

- Lay a foundation that will help you better understand the changes to the Federal Rules of Civil Prosecution (FRCP) that govern E-Discovery.
- Provide some guidance on preparing for an E-Discovery request
- After completing this tutorial, you should be able to:
 - ◆ Speak more intelligently about E-Discovery
 - ◆ Understand the implications of the December 1, 2006 FRCP amendments
 - ◆ Know what to expect to do for an E-Discovery request

- Definitions of Important Terms
- Introduction to E-Discovery
- Important Federal Rules of Civil Procedure (FRCP) changes
- How to prepare for an E-Discovery request

DEFINITIONS OF IMPORTANT TERMS

Important Terms (I)

- **Electronically Stored Information (ESI)**
 - ◆ Any data that is stored on electronic or electromagnetic devices.
- **Personally Identifiable Information (PII)**
 - ◆ Any data about an individual that could, potentially identify that person, such as a name, fingerprints or other biometric data, email address, street address, telephone number or social security number.
- **Federal Rules of Civil Procedure (FRCP)**
 - ◆ Regulations that specify procedures for civil legal suits in United States Federal Courts.

Important Terms (2)

➤ Litigation Hold

- ◆ A condition whereby a company must preserve all relevant data and information that pertains to a formal litigation request or a reasonable anticipation of litigation.

➤ Adverse Inference

- ◆ Inference that destroyed or missing evidence (data) would have been harmful to a party who failed to provide it.

Important Terms (3)

➤ Cull-down/De-Dupe

- ◆ De-duplication of identical information or to take a rather large dataset and reduce it to a more relevant and manageable size.

➤ Spoliation

- ◆ The destruction or significant alteration of evidence or the failure to preserve the property for another's use as evidence in pending or reasonably foreseeable litigation.

➤ Sanctions

- ◆ Usually a monetary fine, imposed against a party to a legal action or his/her attorney, for violating rules of procedure.

What is E-Discovery?

- It is the pretrial process of discovering pertinent information or data stored on electronic, digital, magnetic, wireless, optical, electromagnetic media or devices by one or both parties that are involved in a legal action or proceeding.
- Typically an expensive process for many organizations because they are ill-prepared.

Why Should You Care?

- According to Gartner...
 - ◆ 98% of companies with over \$1 billion in revenue are involved in 1-20 lawsuits with claims over \$20 million
 - ◆ The average suit costs over \$1.5 million to defend
 - ◆ Spending on E-Discovery software technologies and service offerings is forecast to grow between 25% and 35% annually through 2012
- Lawyers involved in complex commercial litigation regularly handle cases with 2 million to 3 million pages of documents

➤ Potential Impacts to data/information handling

- ◆ Classify/organize data (at creation)
- ◆ Strict adherence to policies
 - Follow data destruction and retention policies
- ◆ Retrieval and search
 - Search for data on remote data stores

➤ Standard of Care

- ◆ Stiff fines for Companies who “cover-up” data
 - Qualcomm Inc. v. Broadcom Corp.
 - Zubalake v. UBS Warburg, LLC
- ◆ Sanctions!

OVERVIEW OF FRCP CHANGES

➤ Rule 16:

- ◆ Pretrial Conferences; Scheduling

➤ Rule 26

- ◆ General Provisions Governing Discovery; Duty of Disclosure

➤ Rules 33

- ◆ Interrogatories to Parties

➤ Rule 34

- ◆ Production of Documents, Electronically Stored Information, and Things and Entry Upon Land for Inspection and Other Purposes

➤ Rule 37

- ◆ Failure to Make Disclosures or Cooperate in Discovery; Sanctions

➤ Rule 45

- ◆ “Third-party” Subpoena

- **Qualcomm Inc. v. Broadcom Corp.**
 - ◆ Qualcomm failed “to produce tens of thousands of documents”
 - ◆ Qualcomm to pay Broadcom \$8.5M
- **Murphy Oil USA, Inc. v. Fluor Daniel, Inc.**
 - ◆ Murphy Oil ordered to pay \$6.2M for data recovery
- **Zubulake v. UBS Warburg, LLC**
 - ◆ UBS ordered to pay the costs of any depositions or re-depositions and to reimburse plaintiff

HOW TO PREPARE FOR AN E-DISCOVERY REQUEST

Phases of E-Discovery

- Phase 1: Information Management
- Phase 2: Identification
- Phase 3: Preservation
- Phase 4: Collection
- Phase 5: Processing

- Make sure you follow your data/ESI retention policy
 - ◆ If you don't have one make sure you get one...FAST!
- Make sure you routinely audit compliance of your data/ESI retention policy
 - ◆ Destroy backup tapes on a schedule (virtual/physical)
 - ◆ Do not keep email longer or shorter than policy states
 - ◆ Routinely look for ESI on managed corporate assets
- Understand routine processes

What Can be Discovered? “Samples”

- E-mail
- Spam
- Instant Messaging chats
- Word Processing files
- Text documents
- Spreadsheets
- Databases
- PDF documents
- CAD/CAM files
- Websites
- Images
- Charts/Graphs
- Audio files
- Electronic calendars/agendas
- Digital video
- Voicemail

Where Data Hides “Samples”

- SAN/NAS device
- SAN/NAS snapshots
- Physical/Virtual Tapes
- Physical/Virtual Servers
- Laptops/Desktops
- Flash media
- Metadata
- Applications
- Source Code
- Remote Offices
- CD/DVD
- Mobile Phones/Blackberries
- Phone Systems

- Structured information that describes, explains, locates, or otherwise makes it easier to retrieve, use, or manage an information resource
- Hides in ESI
 - ◆ Word documents
 - ◆ Photos
 - ◆ Backup tapes
- Must be preserved in “native” format
 - ◆ FRCP Rule 34

Identification

- Know where pertinent ESI lives.
- Start with a larger pool of ESI then determine how much of it applies to the case.
- Take into consideration the claims of the case and think about what may be asked for before it is requested.
- Do you know where your backup tapes live?

- Understand your storage architecture
- Preserve all ESI you can think of
 - ◆ Make witnesses/third-parties aware of their duty to preserve ESI (FRCP Rule 45)
- Suspend most automated ESI destruction processes
 - ◆ Suspend destroying of backup tapes
 - ◆ Suspend automated email deletion
- Establish a Chain of Custody

- This is the phase where you actually gather the ESI and store it for processing.
 - ◆ Online/Offline sources
 - ◆ Backup/Archive sources
- Preserve metadata
 - ◆ Creation/Deletion timestamps
 - ◆ Last modified/Last accessed timestamps
- Establish a single point of contact for gaining access to the collected ESI
- Preserve the Chain of Custody

- What ESI should be processed?
 - ◆ Email only?
 - ◆ Email on a particular mail server?
- What timeframe should be processed?
 - ◆ August 31 – September 30
 - ◆ August 21
- Use E-Discovery tools to aid in this phase.
- Should data be converted to a different format?
 - ◆ Will metadata be destroyed in the process of conversion?

Exceptions to the Rule

- Alabama
- Colorado
- Delaware
- Georgia
- Hawaii
- Kentucky
- Massachusetts
- Nevada
- New Mexico
- Oklahoma
- Oregon
- Pennsylvania
- Rhode Island
- South Carolina
- South Dakota
- Vermont
- Washington
- West Virginia
- Wisconsin

- “At least 37 United States District Courts now require compliance with special local rules, forms or guidelines addressing the discovery of electronically stored information. In some districts where there are no local rules or court-mandated forms, individual judges have created their own forms or set out their own preferred protocols for e-discovery.”

Be Aware Of...

➤ Regulatory Drivers (Domestic US)

- ◆ Sarbanes-Oxley (SOX) Act
- ◆ Graham-Leach-Bliley Act (GLBA)
- ◆ Health Insurance & Accountability Act (HIPAA)
- ◆ Securities Exchange Act (SEC) Rules 17a-3 and 17a-4

➤ Regulatory Drivers (International)

- ◆ European Union Data Protection Directive of 1995
- ◆ Canada: Personal Information Protection and Electronic Documents Act (PIPEDA)
- ◆ UK: Data Protection Act 1998

- All evidence (including ESI) must be admissible before it can be used at trial
- The Federal Rules of Evidence (FRE) govern the admissibility of all evidence (including ESI) for use at trial
- In order to be admissible, ESI must be authenticated (legal term)
- Authentication means laying a foundation about the who, what, where and when sufficient for a jury to find that evidence is what it purports to be

- Be aware of the FRCP changes
- Begin thinking about storage processes and retention policies
- Know where ESI lives
- Know how to preserve ESI
- Make sure you know how to collect ESI and maintain a chain of custody
- Begin investigating E-Discovery tools to help with the processing of ESI
- Consult Legal Counsel about admissibility of evidence

- Make sure you follow your data/ESI retention policy
 - ◆ If you don't have one make sure you get one...FAST!
- Make sure you routinely audit compliance of your data/ESI retention policy
 - ◆ Do not keep email longer or shorter than policy states
 - ◆ Routinely look for ESI on managed corporate assets
- Understand what needs to be done at each phase.
 - ◆ Establish a set of internal best practices
- Involve your legal team immediately.

YOU SAID YOU WANTED TO HELP?

➤ SNIA Security Technical Work Group (TWG)

- ◆ **Focus:** Requirements, architectures, interfaces, practices, technology, educational materials, and terminology for storage networking.
- ◆ http://www.snia.org/tech_activities/workgroups/security

➤ Storage Security Industry Forum (SSIF)

- ◆ **Focus:** Marketing collateral, educational materials, customer needs, whitepapers, and best practices for storage security.
- ◆ <http://www.snia.org/ssif>

Additional Resources

- Federal Rules of Civil Procedure, December 1, 2006
 - ◆ <http://judiciary.house.gov/hearings/printers/110th/civil2008.pdf>
 - ◆ <http://www.law.cornell.edu/rules/frcp/>
- Electronic Discovery Reference Model
 - ◆ <http://www.edrm.net>
- Electronic Discovery Law
 - ◆ <http://www.ediscoverylaw.com>
- The Sedona Conference
 - ◆ http://www.thesedonaconference.org/publications_html
- Wikipedia
 - ◆ <http://www.wikipedia.org>
 - › Federal Rules of Civil Procedure
 - › Electronic Discovery
 - › Discovery (law)
- Payment Card Industry (PCI)
 - ◆ <https://www.pcisecuritystandards.org/tech/index.h>

- Please send any questions or comments on this presentation to SNIA: tracksecurity@snia.org

**Many thanks to the following individuals
for their contributions to this tutorial.**

- SNIA Education Committee

**Eric A. Hibbard, CISSP, CISA
Roger Cummings
Larry Hofer, CISSP
Steven W. Tepler, Esq.**

**Marty Foltyn
Chris Lionetti
Walter Wong
David Stevens
SNIA SSIF**

Appendix Slides

➤ Rule 16(b)

- ◆ Alert the court that you may need to perform discovery of ESI.
- ◆ It also puts a timeframe on how quickly you must perform discovery of ESI.

Rule 26 Changes

➤ Rule 26(a)

- ◆ You must disclose ESI or documents in order to support its claims or defenses.

➤ Rule 26(b)

- ◆ You must produce ESI that is pertinent to the case, not privileged and reasonably accessible.
- ◆ You must also identify the sources or ESI you will NOT be making accessible.

➤ Rule 26(f)

- ◆ Also known as the “meet & confer” meeting.
- ◆ You need to preserve, to the best of your ability, all the details of the original ESI if not producing the original
- ◆ You also have the ability to recall privileged information

Rule 34 Changes

➤ Rule 34(a)

- ◆ Defines the scope of the request and formally mentions ESI.
- ◆ It also vaguely defines all forms of computer-based information

➤ Rule 34(b)(i)

- ◆ ESI must be maintained in original format if possible

➤ Rule 34(b)(ii)

- ◆ If ESI can't be produced in original form then the requesting party has the option to state what form they want it.

Rule 37 Changes

➤ Rule 37(a)(2)(A)

- ◆ If you fail to disclose information then you may be forced to disclose the information and may be sanctioned

➤ Rule 37(f)

- ◆ Routine operations

➤ Sanctions!

- ◆ Attorneys fees
- ◆ Adverse Inferences
- ◆ Default, dismissal, judgment against

Rule 45 Changes

- You may be requested to produce ESI even if you are not a party to the litigation.
- May specify the form or forms in which ESI must be produced.
- If not specified then the ESI must be produced in the “form or forms which the person ordinarily maintains it.”