Education

Legal Issues Relevant to Storage

Presented by David L. Stevens
Carnegie Mellon University

Author: Eric A. Hibbard, Hitachi Data Systems

SNIA Legal Notice

- The material contained in this tutorial is copyrighted by the SNIA unless otherwise noted.
- 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.

Abstract

Legal Issues Relevant to Storage

Many organizations face the challenge of implementing protection and data security measures necessary to comply with a wide range of regulatory, statutory, and other legal requirements. Because storage systems (actually the data they contain) play an important part in many of these issues, storage managers and administrators may be asked to assist in supporting a variety of legal actions as well as help their organizations guard against data transgressions having legal consequences. Thus, they need to be capable of taking abstract regulatory, statutory and other legal requirements and translating them into implementable solutions. In addition, they must be able to partner with the legal community to ensure these solutions address the organization's compliance requirements and that the support is timely and responsive.

This session describes the legal issues storage security professionals are likely to encounter as part of their role as the focal point for securing storage systems.

Introduction

- Many organizations face complying with a wide range of regulatory, statutory, and other legal requirements.
- Storage managers and administrators may be asked to:
  - assist in supporting a variety of legal actions
  - take abstract legal requirements and translate them into implementable solutions
  - help their organizations guard against data transgressions having legal consequences

Summary of Legal Areas

- Discovering pertinent stored information or data by parties involved in a legal action or proceeding (Electronic discovery)
- Protecting the confidentiality of private information (Privacy)
- Administration, management, and control of information and data related to an event so that it can be used to prove the circumstances of an event (Evidence Management & Forensics)
- Addressing accountability and responsibility issues
- Factoring in the geopolitical boundaries and the jurisdictional implications

Electronic Discovery

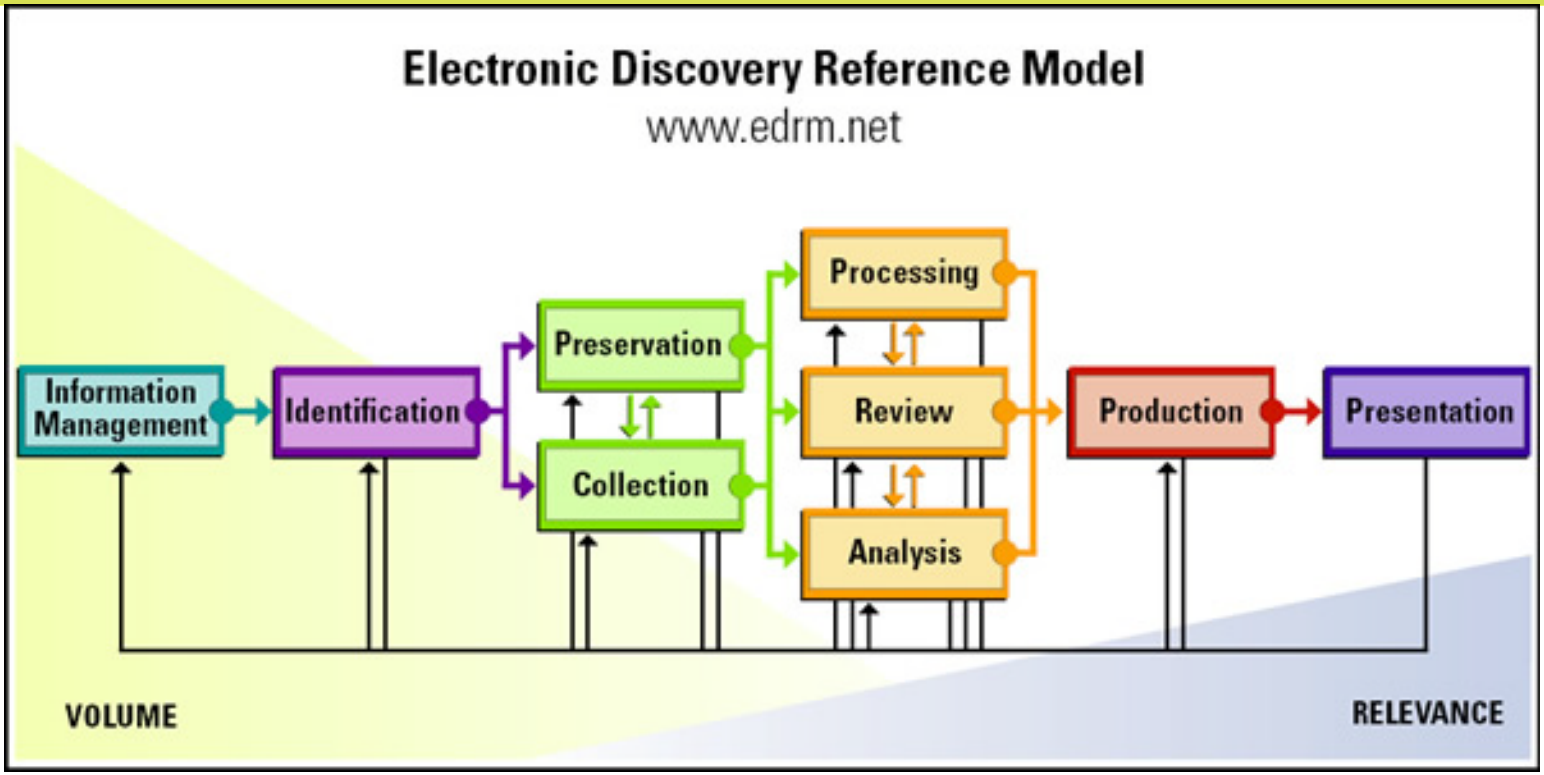
eDiscovery Definitions

- ***Electronic discovery (eDiscovery)*** – The pretrial process of discovering pertinent stored information or data by one or both parties involved in a legal action or proceeding.
- ***Electronically Stored Information (ESI)*** – Computer generated data or information of any kind and from any source, whose temporal existence is evidenced by its storage in, or on any electronic medium, wherever located, now existing or developed in the future, and irrespective whether such medium is real, virtual or otherwise.
- ***Native data format*** – The original, non-derived format and structure of data, together with its associated metadata.
- ***Spoliation of evidence*** – The intentional or negligent destruction, hiding, alteration, withholding or concealment of withholding of evidence relevant to a legal action.

Problem Summary: eDiscovery

- eDiscovery has been predominantly U.S. based
  - Federal Rules of Civil Procedure (FRCP) is a set of regulations that specify procedures for civil legal suits within United States District (federal) Courts
  - Many state courts' civil procedural rules closely follow or adopt similarly worded rules
  - The standard for discoverability is generally that the discovery must be "reasonably calculated to lead to the discovery of admissible evidence" – Rule 26(b)(1)
- Most or all "common law" countries have some form of eDiscovery regulations and provisions.
- Several countries have implemented "blocking" statutes to thwart U.S. discovery requests

Electronic Discovery Reference Model



- **Information Management –** Getting your electronic house in order to mitigate risk & expenses should electronic discovery become an issue, from initial creation of electronically stored information through its final disposition.
- **Identification –** Locating potential sources of ESI & determining its scope, breadth & depth.

Electronic Discovery Reference Model (cont.)

- **Preservation –** Ensuring that ESI is protected against inappropriate alteration or destruction.
- **Collection –** Gathering ESI for further use in the electronic discovery process (processing, review, etc.).
- **Processing –** Reducing the volume of ESI and converting it, if necessary, to forms more suitable for review & analysis.
- **Review –** Evaluating ESI for relevance & privilege.
- **Analysis –** Evaluating ESI for content & context, including key patterns, topics, people & discussion.
- **Production –** Delivering ESI to others in appropriate forms & using appropriate delivery mechanisms.
- **Presentation –** Displaying ESI before audiences (at depositions, hearings, trials, etc.), especially in native & near-native forms.

Storage Relevance: eDiscovery

- eDiscovery requirements can present several challenges
  - locating ESI,
  - ESI preservation,
  - identifying relevant ESI, and
  - producing and receiving ESI.
- Litigation holds on ESI must be honored to avoid evidence spoliation (and possible sanctions).
- In-house and external counsel must become familiar with ICT infrastructure (i.e., lawyers become ICT literate).
- Subject matter experts can be subpoenaed to testify about and explain corporate electronic document retention means and methods, policies and procedures.

Evidence & Forensics

Evidence & Forensics Definitions

- ***Authentic*** – For evidence, being found by a jury (or trier of fact) to be what it purports to be and thus being worthy of trust, reliance, or belief.
- ***Authentication*** – The act of meeting the threshold level for admissibility, but not necessarily of authenticity, of evidence (e.g., ESI).
- ***Authenticity*** – The property, condition, or quality of being worthy of trust, reliance, or belief because the proponent (offeror) has shown enough corroborating evidence to a jury (or trier of fact) to warrant such.
- ***Chain of custody*** – A process that tracks the movement of evidence through its collection, safeguarding, and analysis lifecycle by documenting each person who handled the evidence, the date/time it was collected or transferred, and the purpose for the transfer.
- ***Forensics*** – The use or application of scientific knowledge to a point of law, especially as it applies to the investigation of crime.
- ***Evidence preservation*** – *A* process to maintain and safeguard the integrity and/or original condition of the potential digital evidence.
- ***Provenance*** – Information regarding an item's source, origin, custody and ownership.

Problem Summary: Evidence & Forensics

- Courts are increasingly treating digital evidence in the same way as more traditional documents; they have noted that digital evidence tends to be more voluminous, more difficult to destroy, easily modified, easily duplicated, potentially more expressive, and more readily available.
- In the digital world, most actions leave traces in the digital record that may be of significance in legal actions. The challenge of digital forensics is to
  - collect these traces as unobtrusively as possible
  - minimize impact to ongoing business operations
  - preserve the ability of these traces to be admitted as evidence in a legal proceeding.

Storage Relevance: Evidence & Forensics

- Necessitate an evidence lifecycle management strategy that assists with chain of custody, authenticity, and data authentication.
- A forensic data collection in a storage environment can be disruptive and present many challenges
  - Procedural (size, sources of information, etc.)
  - Technological (formats, access, virtualization, etc.)
  - Completeness (identifying all relevant information)
- Services such as encryption and deduplication present their own special challenges that must be addressed during planning for the collection process.

Privacy

Privacy Definitions

- ***Confidentiality*** – The property that data cannot be accessed by unauthorized parties.
- ***Personally identifiable information (PII)*** – Any data about an individual that could, potentially identify that person.
- ***Privacy*** – The right of an entity (normally an individual or an organization), acting on its own behalf, to determine the degree to which the confidentiality of their private information is maintained.
- ***Privacy breach*** – An event that exploits a vulnerability to reveal PII, or creates a loss of control over PII.

Problem Summary: Privacy

- Many countries—the U.S. being a notable exception—consider privacy to be a fundamental human right.
- Privacy protection laws have been introduced in a significant number of countries.
- The types of "protected" data can vary significantly
- Privacy violations can include the unlawful storage of personal data, the storage of inaccurate personal data, or the abuse or unauthorized disclosure of such data.

Factors Influencing Privacy Safeguarding Requirements (ISO/IEC 29101)

- The PII principal's preference for privacy;
- General legal and regulatory requirements for the safeguarding of the individual's privacy and the protection of his/her PII;
- Sector-specific factors such as industry regulations, professional standards, company policies;
- The terms of contracts between the PII controller and PII principals, PII processors or third parties;
- Business factors predetermined by a specific business application or in a specific use case context; and
- Other factors that can affect the design of ICT systems and the associated privacy safeguarding requirements.

General Privacy Considerations (ISO/IEC 29101)

- It should be possible to pull together definitive records of what PII is known/stored about people (including PII recorded in logs and backup);
- It should be possible to identify and describe all PII, no matter how it is collected (including internal generation);
- It should be possible to know and control the physical location of all PII, including all copies thereof;
- A list of individuals who have or may have had access to PII should be maintained;
- The real need for routine audit logging of a process that includes or creates PII should be assessed as part of system design;

General Privacy Considerations (ISO/IEC 29101) cont.

- The design of privacy controls should include the security of backed up and archived data when it contains PII;
- The same privacy controls which are used to secure collected PII should be applied to secure any derived PII if the sensitivity or risk level if the PII is the same as that of the original PII (e.g. transaction histories in e-retailing applications, behavioral PII used for profiling);
- Memory dumps and other line or activity traces created by technically skilled people who have access to PII should be subject to security and privacy policies;
- The supporting data architecture should define the extent to which data assets are shared across entities;
- The need and capacity to record privacy inquiries (e.g. to resolve disputes) should be considered in applications based on databases containing PII;

General Privacy Considerations (ISO/IEC 29101) cont.

- Change management procedures for web applications should protect against inadvertent changes that affect privacy, e.g., ensure that changes to web forms do not change the nature or amount of PII collected or ensure that PII is secured by the destruction of obsolete and defective equipment or media;
- The design of privacy controls should include the management of ephemeral or incidental PII, e.g. help desk or customer service logs; and
- It should be possible to know the details of all other parties to whom the PII has been disclosed, including the purposes for which the PII was disclosed and the conditions, limitations under which it is retained, and also including the identity and role of the person in each party who is responsible for managing the PII.

Storage Relevance: Privacy

- The use of some form of data classification can help identify the data that need protection as well as the nature of the protection
- Encryption, when used correctly, can be an important tool to protect data confidentiality
- Breach notification requirements for protected data may necessitate data monitoring to help identify suspected data breaches
- Data movements (like data replication associated with DR/BC solutions) must respect geopolitical boundaries to avoid privacy violations

Accountability & Responsibility

More Definitions

- ***Care*** – Level of active concern, or lack of negligence, towards avoidance of possible dangers, mistakes, pitfalls, and risks, demanded of a party as a duty or legal obligation. See also due care and duty of care.
- ***Due diligence*** – Measure of prudence, responsibility, and diligence that is expected from, and ordinarily exercised by, a reasonable and prudent person under the circumstances.
- ***Due care (Duty of care)*** – Degree of care that an ordinary and reasonable person would normally exercise, over his or her own property or under circumstances like those at issue. The concept of due care is used as a test of liability for negligence.

Problem Summary: Accountability & Responsibility

- Increasingly, government officials and corporate executives are being held personally accountable for their actions or lack of action
- Inappropriate data handling or malicious attacks on data can cause individuals and organizations to incur liabilities (civil litigation)
- Unauthorized possession or access of regulated data can result in penalties and force "costly" breach notifications
- Adherence (or lack thereof) to organizational policy can be an important factor in determining negligence

Storage Relevance: Accountability & Responsibility

- Protections may be necessary in the storage infrastructure to guard against unauthorized, accidental or intentional corruption, modification, or destruction of data
- The risks associated with data breaches can be significant for some organizations, so prudence dictates the use of reasonable measures (like following best practices) to guard against these breaches
- Proper data preservation and disposal activities are necessary for an organization to meet its legal obligations
- Policies are important administrative controls to facilitate proper data handling

Jurisdiction & Cross Border Data Transfers

Problem Summary: Jurisdiction & Cross Border Data Transfers

- Many countries regulate the handling and storage of certain types of data
- Some governments are also struggling to deal with
  - Critical questions about the limits of their jurisdiction over the Internet.
  - Regulating their citizens' (and organizations') activities on the Internet.
- Organizations have adopted computing models that allow data to reside in many locations
  - Complicates the matter of who has authority or jurisdiction over this data when it is in flight
  - Jurisdiction is less complicated for data when it is at rest; however, there may be multiple entities asserting their authority.

Storage Relevance: Jurisdiction & Cross Border

- The use of some form of data classification can help identify the data that have geopolitical restrictions
- Data movements (like data replication associated with DR/BC solutions) must respect geopolitical boundaries to avoid violations
- Multiple, overlapping jurisdictions can result in an untenable position (like U.S. discovery requests for data residing in France)
- Data breaches on foreign soil can be considered illegal technology transfers

Final Thoughts

Final Thoughts

- Legal issues and requirements are beginning to impact storage infrastructures and personnel, and this trend is expect to continue.
- Several of the topics addressed in this session represent emerging areas of the law, so expect changes and further developments.
- When dealing with the legal community, expect answers like "it depends and it depends on wheat our obligation is to provide you the information you seek"
- Compliance is often cited as a driver for security, but a close inspection will often show that compliance is being driven by legal elements.

Q&A / Feedback

- 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
Steven Teppler, Esq.
Larry Hofer, CISSP, PE
David Stevens
Richard Austin, CISSP
Andrew Nielsen, CISSP, CISA
Gianna DaGiau

SNIA Security TWG

For More Information

Useful Web Resources

- ABA E-Discovery & Digital Evidence (EDDE) Committee, http://new.abanet.org/sections/scitech/ST203001/Pages/default.aspx
- The Sedona Conference®, http://www.thesedonaconference.org/
- Wikipedia – Common Law, http://en.wikipedia.org/wiki/Common_law
- SNIA Dictionary, http://www.snia.org/education/dictionary/

Useful Printed Resources

- Books
  - *Foundations of Digital Evidence* , Paul, 2008, ISBN-13: 978-1604421040
  - *Real Digital Forensics: Computer Security and Incident Response*, Jones, Bejtlich, Rose, 2006, ISBN-13: 978-0321240699
  - *Electronic Discovery and Digital Evidence in a Nutshell*, Scheindlin, Capra, The Sedona Conference, 2009, ISBN-13: 978-0314204486
  - Electr*onic Discovery and Digital Evidence: Cases and Materials*, Scheindlin, Capra, The Sedona Conference, 2008, ISBN-13: 978-0314191311
  - *Electronic Evidence: Law and Practice*, Second Edition, Rice, 2009, ABA, ISBN-13: 978-1604420845
  - *Electronic Evidence and Discovery: What Every Lawyer Should Know Now*, Second Edition, Lange, Nimsger, 2009, ISBN-13: 978-1604423822
- ISO/IEC Information Technology -- Security techniques standards: (including drafts)
  - ISO/IEC 27037 Guidelines for identification, collection and/or acquisition and preservation of digital evidence (CD)
  - ISO/IEC 29100 Privacy framework (3rdCD)
  - ISO/IEC 29101 Privacy reference architecture (CD)

SNIA Security Organizations

- 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: Educational materials, customer needs, whitepapers, and best practices for storage security.
  - http://www.snia.org/ssif