



Education

COMPUTING

LITIGATING IN THE CLOUD

Steven W. Tepler, Esq.
Senior Counsel, KamberEdelson, LLC

- 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.
- Although the author/presenter is an attorney, nothing in this presentation is intended to be, or should be construed to be legal advice or an opinion of counsel. If you need legal advice or a legal opinion please contact an attorney in your jurisdiction.
- 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.

➤ Cloud Computing Increases Digital Evidence Security and Management Risks

- ◆ Electronically Stored Information (ESI) has taken center stage in litigation. Storage IT Security stakeholders are now front line participants in litigation. Poor ESI storage management policy and process can result in evidence spoliation (data destruction). The damage can be financial, reputational, and even criminal. Cloud computing only amplifies enterprise litigation risks. Corporate counsel as well as Cloud service providers must be risk-aware, and adapt SLA terms to reflect new risks. Customers should understand these risks when architecting cloud based service and negotiate SLA terms accordingly.

First, a *Mea Culpa* – I am a lawyer

I advise clients*

I litigate in court*

***Disclaimer: But I'm not doing this here. Seriously, if you need advice or counsel, consult an attorney in your jurisdiction.**

Ok, back to “Litigating in the Cloud”...



- **Cloud Services** - Consumer and Business products, services and solutions that are delivered and consumed in real-time over the Internet
- **Cloud Computing** - an emerging IT development, deployment and delivery model, enabling real-time delivery of products, services and solutions over the Internet (*i.e.*, enabling cloud services)
 - ◆ Source: IDC: <http://blogs.idc.com/ie/?p=190>

- Off-site, third party provisioning
- Accessed via Internet
- Provisioning
 - ◆ Self-service requesting
 - ◆ Near real-time deployment
 - ◆ Dynamic and fine-grained scaling
- UI is browser based
- System Interface – web services APIs
- Shared Resources/Common versions, customization
“around” shared services

Cloud Computing: Only Three Shortcomings

- Inadequate or No Security Provisioning
 - ◆ By Cloud Computing providers
- Inadequate or No Understanding of Emerging Legal Issues
 - ◆ By Cloud Computing Providers
 - ◆ By Corporate/Enterprise Counsel
 - ◆ By IT Consultants
- Failure to recognize legal liability potential arising from poor/no security, or from understanding of emerging legal issues

Cloud Computing Native Security Attributes

This Slide Intentionally Left Blank

Legal Attention Paid to Cloud Computing

This Slide Intentionally Left Blank

That was easy. We can play golf now.

Can't we?

Well, not quite yet...

Cloud Computing Means Data May Always Be in Transit

- Corporate Counsel's New Nightmare
 - ◆ Identify who, when and “where”
 - Query: Where is “where” in Cloud Computing? Lawyers and regulators will want to know
 - ◆ Where is data located, how to find it when required to produce in litigation
 - ◆ Custody and control: Is data preserved, who has duty to preserve, how to demonstrate adequacy
 - ◆ Document/Record Retention Policies – how to account for Cloud Computing attributes
 - ◆ IT Vendors/Consultants – how to write agreements that take legal issues into account

- May be subject to privacy laws and regulations
- May be subject to laws requiring provably persistent data integrity
- May be required by law or regulation to be securely stored or archived
- May be subject to conflicting laws from different jurisdictions (other countries)
- Examples:
 - ◆ SOX, GLB, FFIEC, HIPAA, 21 CFR Part 11, Basel II

- Presumed?
- Disclaimed?
- Offered as part of basic service?
- Offered as option?
- How contracted for?
 - ◆ Between whom (think potential third party beneficiaries)
- How audited, enforced?
- Who gives reps and warranties?
- Who drafts the SLA?
 - ◆ Attorneys (choke)? Business development (gag)?

Cloud Computing and Litigation Considerations

- 2006 – The Year Litigation Changed
- December 1, 2006 - Effective Date of Electronic Discovery Amendments to the Federal Rule of Civil Procedure (FRCP)
- eDiscovery changes the litigation and corporate information landscape

- New eDiscovery rules and existing evidentiary authentication and admissibility requirements increase scrutiny on stored information, and the entire storage ecosystem
- Storage Security Industry and corporate counsel are presented with new eDiscovery and Evidentiary Challenges to develop new ways to store data with provably persistent data integrity

Rules? What rules?

An eDiscovery Sampler

- FRCP 26(a)(1) – Initial Disclosures
- ...A party **must**...provide...
- ...electronically stored information...in the custody, or control of the party, and that the party may use to support its claims...

- Terms to Keep in Mind:
 - ◆ Custody
 - ◆ Control

- **FRCP 34 – ESI Production Requests**
- Inspect, Copy, Test or Sample Electronically Stored Information (ESI)
- Stored in any medium
- **Wherever** stored (*n.b.* – start thinking “cloud”)
- Requestor may specify form and format of production
- **FRCP 45 – Non-Party Subpoenas**
 - ◆ Join the discovery party even when you’re not a party

- **FRCP 37 – Failure to Make Disclosure or Cooperate in Discovery – Sanctions**
- Attorneys fees
- Adverse inferences
- Exclusion of evidence
- Default, dismissal, judgment

Ok, golf now?

Sorry, not just yet...

Spoliation...is Evidence Destruction



Spoliation...in the Cloud



➤ **Information Security Policy and Process Failures Can Lead to Spoliation:**

- ◆ To Impose/Maintain “Litigation Hold”
- ◆ To suspend data or document “Retention Policy”
- ◆ To understand what “preserve” means
- ◆ To understand when “preservation” must begin
- ◆ To understand what, where, how to search
- ◆ **To Maintain Proper Information Security Policy and Process**

➤ **Sanctions:** Adverse inferences, default, dismissal, criminal liability

Information Security is The Flip Side of eDiscovery

➤ **Common Drivers:**

- ◆ **Search**
- ◆ **Identification**
- ◆ **Collection**
- ◆ **Attribution**
- ◆ **Preservation**

➤ **Legal Issue Considerations:**

- ◆ **Privacy**
- ◆ **Integrity**
- ◆ **Accessibility**
- ◆ **Regulatory Obligations (HIPAA, GLB, SOX, etc.)**
- ◆ **Auditability**

- **Corporate Counsel (in house or retained) must be fully engaged**
 - ◆ **Investigate security profile of cloud based services**
 - ◆ **Engage vendors, consultants or other qualified individuals to ascertain whether offerings are “security-free” (meaning non-existent)**
 - ◆ **Make informed risk-assessment of security level required to be incorporated into service provided to enterprise**
 - ◆ **Require representations and warranties as to level of security offered, and require periodic audits**

- Understand the technology
 - ◆ IT Management should educate counsel (or hire outside consultants)
- Negotiate contracts for cloud computing, cloud storage products and services with a shared definitional understanding
 - ◆ Or explain what you think you meant by what you wrote in light of what you think the other party thinks you meant by what you wrote...

- Attorneys must take responsibility for ensuring that their clients conduct a comprehensive and appropriate document search.” Excerpted from *Qualcomm v Broadcom* (2008)

eDiscovery in the Cloud – Some Advice from the Courts

- “The Committee’s concerns are heightened in this age of electronic discovery when attorneys may not physically touch and read every document within the client’s custody and control.
- For the current “good faith” discovery system to function in the electronic age, attorneys and clients must work together to ensure that both understand how and where electronic documents, records and emails are maintained and to determine how best to locate, review, and produce responsive documents.

- 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

ESI and Hearsay Evidence

- **Hearsay** – An out of court statement created by a (generally) unavailable “declarant” used at trial to prove the truth of the matter asserted
 - ◆ Hearsay is inadmissible evidence (can’t be used in Court), unless an exception applies
 - ◆ Hearsay Exceptions Include – Records of regularly conducted activity

Simple, eh what?

➤ FRE Rule 803(6) Records of Regularly Conducted Activity

- ◆ A memorandum, report, record, or data compilation, in any form, of acts, events, conditions, opinions, or diagnoses, made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record or data compilation, all as shown by the testimony of the custodian or other qualified witness...unless the source of information or the method or circumstances of preparation indicate lack of trustworthiness.

Simple ESI Admissibility Logic Tree

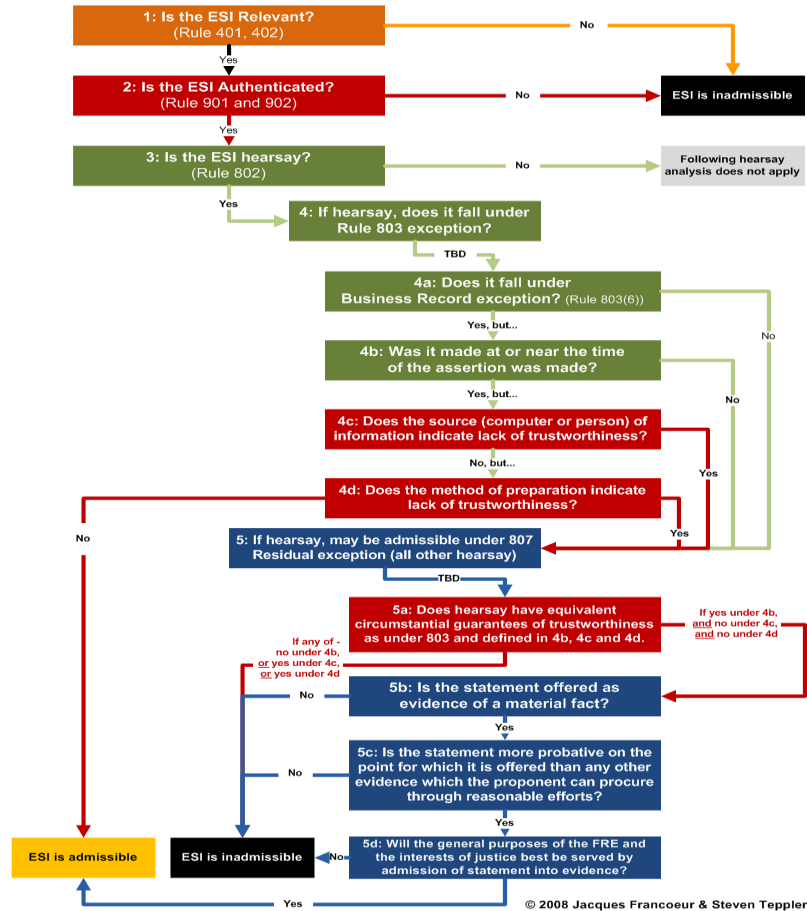
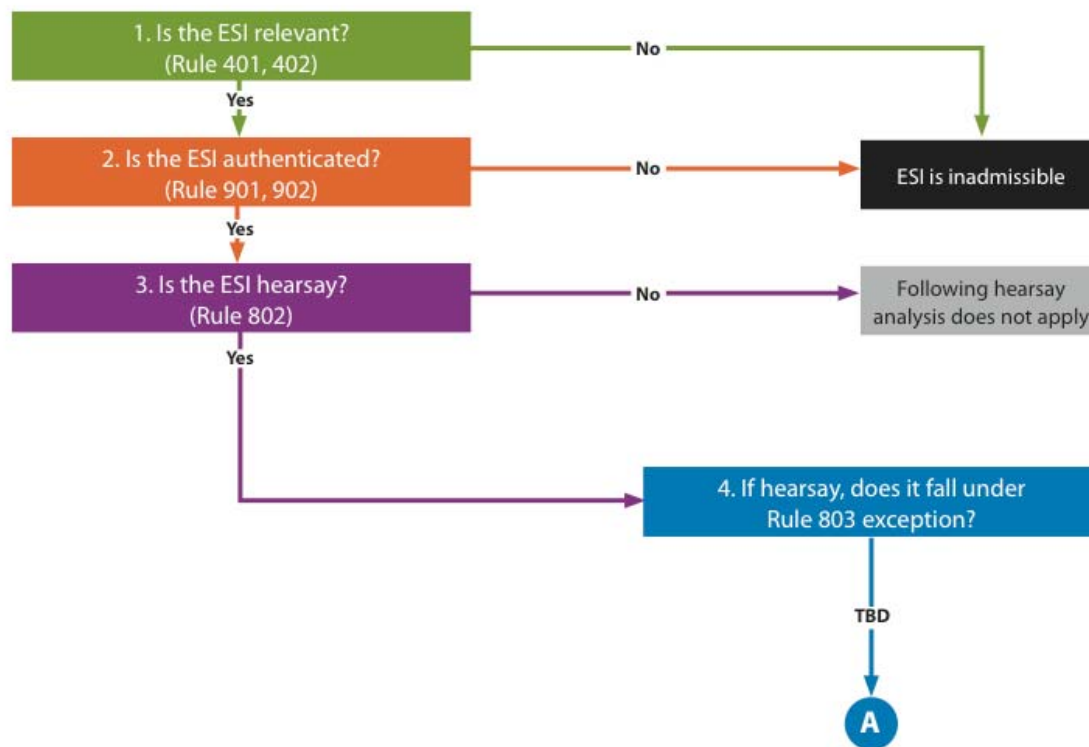


Figure 11: ESI Admissibility Decision Tree

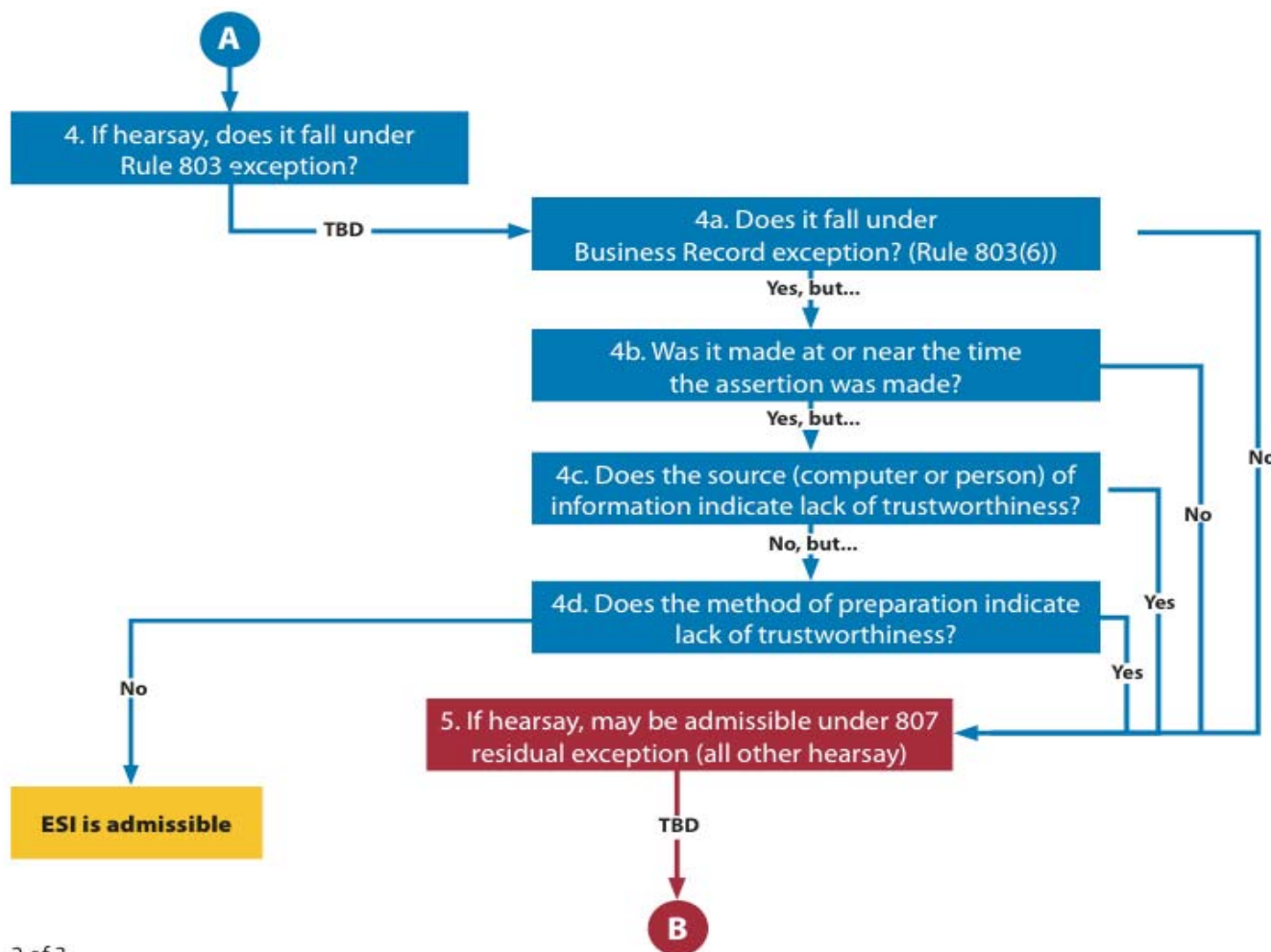
So, shall we make this more simple?

Simple Admissibility Logic Tree



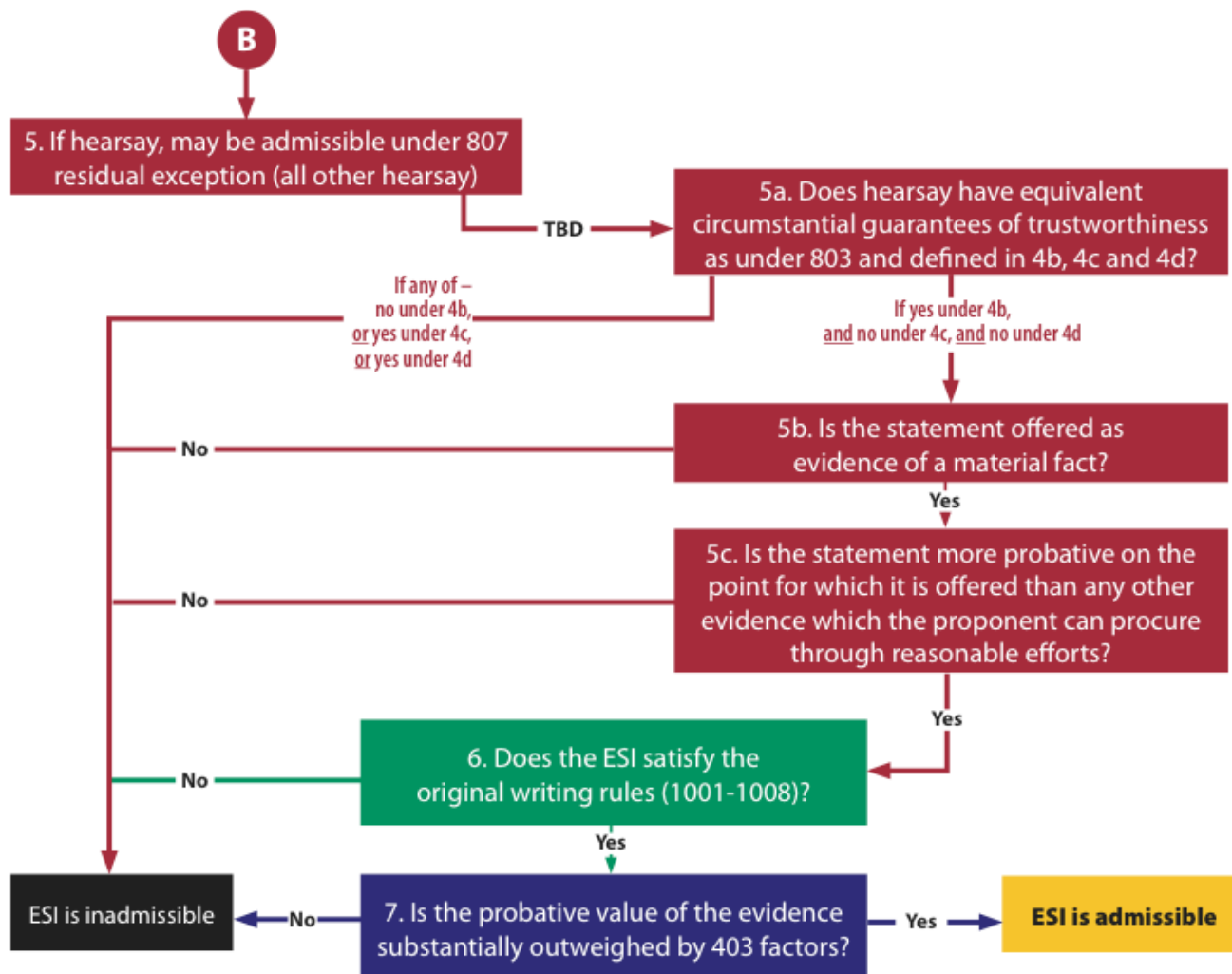
1 of 3

Simple Admissibility Logic Tree -2-



2 of 3

Simple Admissibility Logic Tree -3-



3 of 3

© 2008 Jacques Francoeur and Steven Teppler

Simple, eh what?

➤ **Discovery in the Cloud**

- ◆ **Identification in the Cloud**
- ◆ **Search in the Cloud**
- ◆ **Metadata in the Cloud**
- ◆ **Collection in the Cloud**
- ◆ **Production in the Cloud**
- ◆ **Maintaining Integrity in the Cloud**
- ◆ **Spoliation in the Cloud**

and,

- ◆ **Sanctions in the Cloud**

- **ESI Admissibility and Authentication in the Cloud**
 - ◆ **Authentication in the Cloud (Fed. R. Evid. 901)**
 - ◆ **Hearsay in the Cloud (Fed. R. Evid. 801, 803, 806)**
 - **Business Record Exception In the Cloud**
 - ◆ **Custody (Security) in the Cloud**
 - ◆ **Trustworthiness in the Cloud**
 - ◆ **Provably persistent integrity in the Cloud**
 - ◆ **Spoliation in the Cloud**
 - and...*
 - ◆ **Sanctions in the Cloud**

➤ **How does this affect Storage Industry Stakeholders?**

- ◆ **Solutions Architects?**
- ◆ **Storage Solutions Providers?**
- ◆ **Standards Setting Bodies?**
- ◆ **Storage Security Vendors?**
- ◆ **Customers?**

➤ **Solutions Providers – Cloud Contracting**

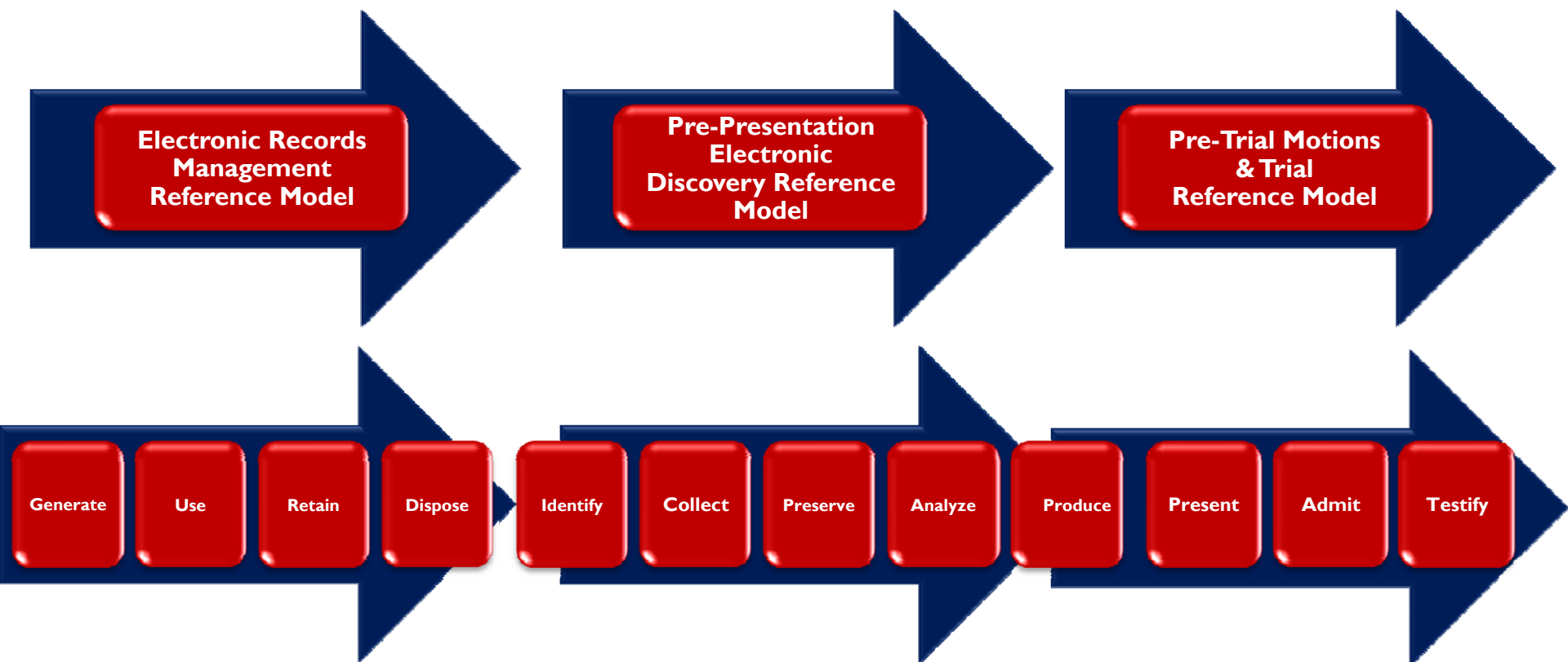
- ◆ **Provisions for customer ESI set forth in SLA or other agreements**
- ◆ **Disclaimers for loss, alteration, destruction, irretrievability, non-searchability**
- ◆ **Upstream indemnification**
- ◆ **Disclaimers for security breach or vulnerability that results in eDiscovery or evidentiary sanction**
- ◆ **Storage host disclaimers for acts by insiders (employees, etc.) resulting in loss, or...**
- ◆ **SLA upsell for added security and integrity mechanisms guaranteeing availability and integrity**

Cloud-Directed Legal Considerations

- ▶ **Customers – Contracting in the Cloud: Customers will insist (now or soon) on SLA terms to ensure**
 - ◆ **Legal or regulatory compliance**
 - ◆ **Searchability**
 - ◆ **Demonstrable custodial care (*i.e.*, security)**
 - ◆ **Provably persistent data integrity and reliability**
 - ◆ **Demonstrable storage security and integrity for ESI in the cloud will also be driven by regulatory requirements (SOX, HIPAA, GLB, FFIEC)**

- ◆ **Understanding ESI issues and obligations of client as they relate to client's technology infrastructure, then architect solutions**
 - ◆ **Where data is generated and located**
 - ◆ **Network and storage mapping**
 - ◆ **How data is stored and backed up**
 - ◆ **Document Retention Policies, development , audit and enforcement (in conjunction with IT)**
 - ◆ **Control**
 - ◆ **Duty to Preserve – what, when, and how**
 - › **The topic for another informative seminar**

The Digital Evidence Life Cycle



➤ Litigation in the Cloud is here

- ◆ **Storage industry security and integrity standards will help enterprise meet legal discovery and evidentiary preservation obligations, but must be continually adapted to reflect increasingly diverse (read “cloud computing”) and ever more stringent discovery and admissibility challenges**
- ◆ **Large market opportunities exist for storage industry participants to anticipate and architect solutions to meet heightening eDiscovery and digital evidence authentication demands**
- ◆ **SLA must be adapted to reflect emerging risks and opportunities**

- 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

Steven W. Teppler

Eric A. Hibbard