

ISACA – Electronic Discovery



Wednesday, January 28, 2009

Presented by:

Katie Jensen

**Navigant Consulting,
Inc.**

KJensen@NavigantConsulting.com

(312) 583-6828

Rick Schoeneck

Accenture

Dave Tonisson

**Sonnenschein Nath &
Rosenthal LLP**

DTonisson@Sonnenschein.com

(312) 876-2860

Electronic Discovery Introduction



“The reality of electronic discovery is it starts off the responsibility of those who don’t understand the technology and ends up the responsibility of those who don’t understand the law.”

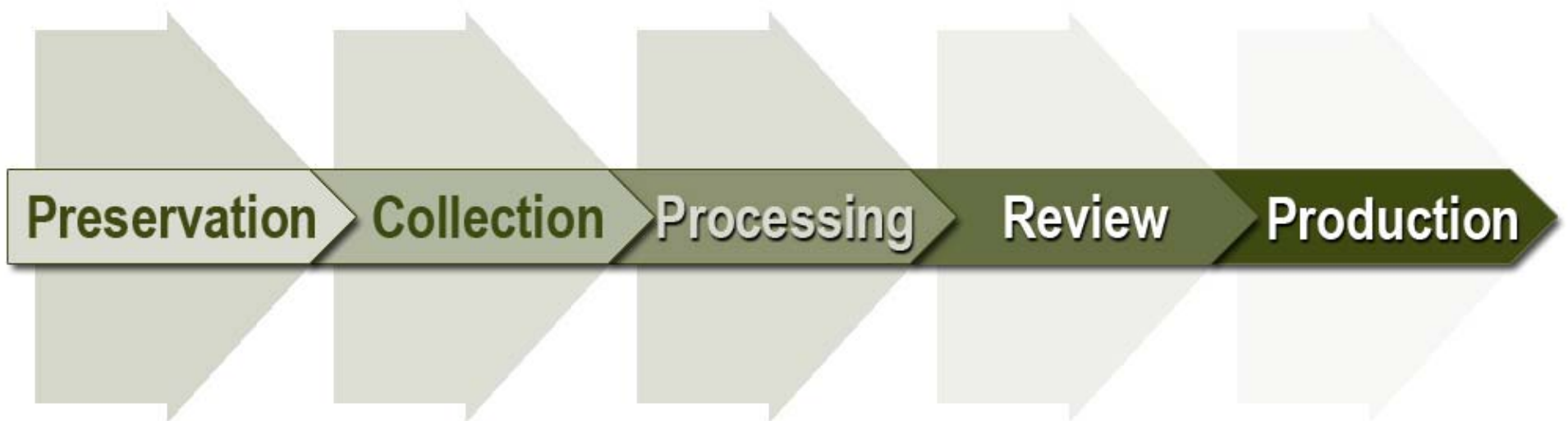
Craig Ball, *Corporate Counsel*, “The Perfect Preservation Letter,” April 2005.

Electronic Discovery Defined



Electronic Discovery is the process of preserving, collecting, processing, reviewing and producing electronic data in response to civil or criminal legal matter.

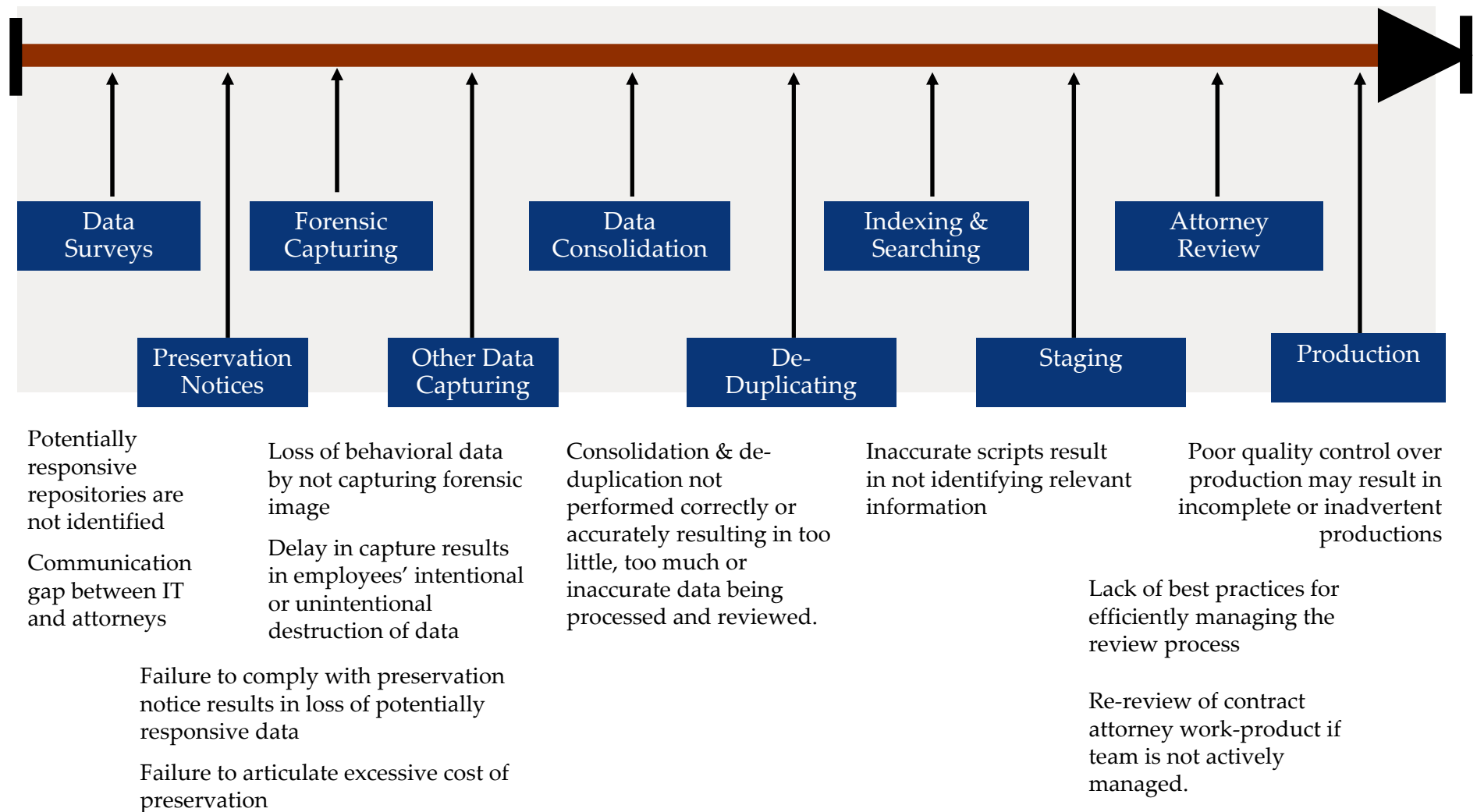
Traditional e-Discovery Lifecycle:



"Privileged and Confidential, ©2009
Navigant Consulting, Inc."

NAVIGANT
CONSULTING

Risk Factors in Discovery Lifecycle



"Privileged and Confidential, ©2009
 Navigant Consulting, Inc."

Electronic Discovery Lessons Learned



Preservation

- » Delay or insufficient communication in providing notice
 - Records retention practices that are not in sync with the legal process
 - Directed to business personnel, not IT owners
 - Lack of centralization of process
 - Lack of agreement between parties as to what should be preserved
- » Technical decisions that impact legal
 - Inadvertent deletions
 - Inconsistent practices across the company
 - HR disconnects on departed and renamed employees

Collection

- » "Do it yourself" Collections
 - Reliance on Internal IT staff that is already over-taxed
 - Leaving interpretation to business custodians
- » Use of Forensic Collection Practices
 - Attempting to save costs in the wrong areas
 - Not establishing chain of custody
 - Not following industry standards
- » International Privacy Issues

Processing

- » Processing the data without agreement on policies or standardized procedures
 - What is a duplicate?
 - What data types and sources will be processed?
- » Vendor Black Box
- » Difficult Data
 - Foreign languages
 - Password locks
 - Odd data types

Review

- » Review Management
 - Right tool for right matter
 - Lack of content based expertise in the process
 - Proper deployment of contract attorneys
 - Failure to take advantage of new technologies that facilitate faster reviews
- » Incomplete review caused by incomplete data
- » Keyword search terms aren't always accepted
- » Reporting Issues
- » Quality Control/ Statistical Testing Issues

Production

- » Print and native production issues
- » Not providing for inadvertent disclosure
- » Data not provided in a reviewable format
- » Negotiating upfront on what form production will take
- » Poorly negotiated Metadata agreements
- » Failure to enforce Protective Orders in native productions

"Privileged and Confidential, ©2009
Navigant Consulting, Inc."

NAVIGANT
CONSULTING

Lesson 1:



Communicate Knowledge of Systems & Processes

- IT systems and organization
- Data repositories
- Retention, destruction and recycling processes
- Updated “data map” is crucial – think beyond email and file servers
- Need to be able to convey internal & external data and it’s accessibility
- Back-up policies



Lesson 2:



Understand the Downstream Costs:

- Cost for storage consistently going down, so employees store more information, causing increasing costs to review that data
- 500 GB external storage drive = \$150
- Keyword filtering of 500 GB, resulting in 200 GB to review
 - (\$350 - \$1000/GB) = \$175K – \$500K
- Loading of 200 GB (~2M documents)to online review
 - (\$800 - \$2000/GB) = \$160K - \$400K
- Cost to review
 - (~400 documents per day @ \$55/hour) = \$2.2M

Lesson 3:



Involve Legal in Software Decisions:

- **Introducing any new systems into the corporations infrastructure without input from Legal could have severe consequences**
- **Examples:**
 - **Company's IT department decided to install Instant Messaging without consulting with Legal to understand the discoverability issues**
 - **Selection of email system can cause complex and expensive collection (Groupwise, Eudora, etc.)**

Lesson 4:



Ensure Proper Collection and Chain of Custody:

Collection Methodologies:

- **“Drag & Drop”** – Users or IT manually copy files and email to a folder or external media for further processing. NOT advisable as some metadata is changed during the copy process and logging is not available.
- **Active Data Copy** – IT or consultants use commercial tools (e.g., RoboCopy, SafeCopy2 & Vice Versa Pro) to copy data and preserve all meta data. Logging is available.
- **Forensic Image Capture** – IT or consultants create a mirror image of the media using industry standard tools to capture both active and inactive data. Logging is always performed and validation of collected data is required.
- **Backup Tape Capture** – IT or consultants backup the various data sources to tape. Tape can be slow and problematic to process.

Lesson 5:



Develop an Off Boarding Process:

- Consider possible legal holds on data sources before deletion or re-commissioning hardware
 - Laptops, PCs
 - Blackberrys, PDAs
 - Cell Phones
 - External Storage Devices
 - Loose media (CDs, DVDs)
- Ensure that process is consistently applied

Risks & Pitfalls – Preservation Case Law



Samsung Electronics v. Rambus, 439 F.Supp.2d 524 (E.D. Va. 2006) echoes the criticism of cursory compliance efforts including the misplaced reliance on custodian self-collection, stating that “[i]t is not sufficient ... for a company merely to tell employees to ‘save relevant documents’ ... this sort of token effort will hardly ever suffice.”

- **The Court determined that the defendants’ lack of consistent systematic and effective processes to collect and preserve relevant ESI demonstrated spoliation of evidence.**
- **"...in order to have an effective suspension of the document destruction plan during litigation, employees must be specifically instructed respecting what documents are relevant to the litigation (and thus cannot be destroyed) and what documents are not relevant (and thus can be destroyed).**
- **Must instruct on subject matter and kinds of documents to preserve**

Risks & Pitfalls – Preservation Case Law



Wachtel v. Health Net, Inc., 2006 WL 3538935, (D.N.J. Dec. 6, 2006), the Court found 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 Court made clear that having a paralegal merely email preservation notifications is insufficient, noting that “Despite the document hold, thousands of employees’ emails failed to be searched.”
- The Court found that “even when [defendant’s] employees could search their emails, their searches were *sporadic* rather than *systemic*.”
- The Court, concluding that these failings constituted bad faith, imposed harsh evidentiary and monetary sanctions.

Risks & Pitfalls – Preservation Case Law



Treppel v. Biovail Corp., 2008 U.S. Dist. LEXIS 25867 (S.D.N.Y. Apr. 2, 2008), the Court finds defendant's methods of collecting and preserving ESI "clearly inadequate." Court cites failure to preserve backups after notice from plaintiffs, inconsistent email access and retention policies.

- **Court orders additional backup searches and "thorough forensic examination" of CEO's laptop, all at defendant's expense**