



The World Leader in Digital Investigations

ACC AMERICA
Association of Corporate Counsel
Southern California Chapter (ACCA-SoCal)

The Honeymoon is Over: Update on Recent Case Law Applying the New Federal Rules

ACC Southern California
March 28, 2007

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

© 2007 Guidance Software, Inc. All Rights Reserved.

DUFF & PHELPS

Participants

- **James Lynch**

- Partner, Latham & Watkins

- **Martha Gooding**

- Partner, Howrey

- **Kevin Dorse**

- Partner, Jones Day

- **John Patzakis**

- Chief Legal Officer, Guidance Software Inc.

- Update on New Case Law Addressing:
 - Discovery of Inaccessible ESI (FRCP 26(b)(2)(B))
 - Safe Harbor, (Rule 37(f))
 - Form of Production, (Rule 34(b))
 - Early Attention/Litigation Hold Defensibility, (Rules 26, 16)
- Update on New Maryland USDC Protocol

The New Concept of Accessibility

- Rule 26(b)(2)(B): “A party need not provide discovery of (ESI) from sources that the party identifies as not reasonably accessible because of undue burden or cost.”
- On motion, the party from whom discovery is sought has burden to demonstrate inaccessibility
- Even if that showing is made, the court may still order discovery upon showing of good cause.
- Key Committee Notes:
 - Inaccessible ESI is still subject to preservation obligations
 - Requesting Party Should First Seek and Evaluate Accessible ESI

Ameriwood v. Liberman ("Ameriwood I")

P A G E 4

- Trade secret case in which "mirror images" of defendants' computers and other electronic storage equipment was especially relevant
- District Court accepted defendants' arguments that "mirror images" were not "reasonably accessible" within the meaning of Rule 26(b)(2)
- Mirror images were discoverable nevertheless, and plaintiffs -- who did not resist cost shifting -- would pay to create such images.
- Keys: (1) mirror images were "inaccessible" because of undue burden or cost; (2) unique facts made "inaccessible" data discoverable.

Ameriwood v. Liberman ("Ameriwood II")

P A G E 5

- Defendants moved to compel production of three categories of plaintiff's documents relevant to the argument that plaintiff's declining sales were unconnected to defendants' conduct.
- The District Court found that one category of documents was not "reasonably accessible" due to "undue burden or expense," because responsive documents included some 52,000 emails and 4,400 other files.
- Defendants failed to show "good cause" for the production under Rule 26(b)(2), because the request was "not narrowly tailored" to seek information relevant only to its defenses.
- Keys: (1) 55,000 electronic documents is "unduly burdensome?"; (2) failure to tailor document requests can result in an "all or nothing" outcome under the "good cause" standard.

Semsroth v. City of Wichita

- Police officer suing City for employment discrimination sought emails from 117 employees contained on one disaster-recovery back up tape. Defendants moved for an order shifting to Plaintiff all or part of the cost to restore and search the tape.
- Magistrate Judge refused to shift costs because the \$2k to \$3k cost of restoring and searching the tape did not make the data "inaccessible" because of "undue burden." But the Judge struck certain "key words" from the search and limited the search to 50 custodians.
- Judge also ruled that the defendants' decision to store the emails on a disaster-recovery back up tape was reasonable, given the purpose.
- Keys: (1) refusing to shift costs for restoration of back-up tapes is not a good start under the Rules -- would the outcome be different if more tapes were involved?; (2) Court rejects bright-line rule connecting restoration costs with "undue burden."

Rule 37(f) “Safe Harbor”

- “Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide [ESI] lost as a result of the routine, good faith operation of an electronic information system.”
- 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

Turner v. Resort Condominiums *(D. Ind. July 2006)*

- Sanction sought for failure to comply with pre-suit preservation letter requiring, for indefinite time:
 - No modification/deletion of any ESI on any media or device
 - No upgrade/replacement of hardware or software
 - Copy all hard drives
 - Save all data after preservation letter

Turner : Sanctions Denied

- Preservation Letter did not “accommodate the routine day-to-day needs of a business with a complex computer network” and demanded action beyond legal obligations
- Pending amendment to Rule 37(f) “recognizes that discovery should not prevent continued routine operations of computer systems”
- No evidence of bad faith alteration or destruction
- Plaintiff got “much of what she sought to preserve and all relevant information”

Cache de Poudre Feeds v. Land O' Lakes, Inc.
(D. Colo. March 2, 2007)

- Sanction request for destruction of relevant documents
- Rule 37(f) – “limited protections against sanctions”
 - Consistent with *Zubulake* “general rule” that litigation hold does not apply to inaccessible back-up tapes, which may be recycled per company policy/schedule
 - After litigation hold, may not continue routine practices that ensure potentially relevant and readily available information is no longer reasonably accessible

- Counsel was “less than thorough” in preservation efforts
 - Expunged hard drives of key players who departed after case commenced (eliminated readily accessible source; noting ease of copying hard drives)
 - Directed employees to preserve documents “relevant” to litigation, but let employees define relevance and accepted uncritically what employees provided

Land O' Lakes: Sanction Granted

- GC & Outside Counsel failed to coordinate and oversee discovery
 - GC failed to independently verify completeness of employees' production
 - GC failed to verify assumption that former employees' e-mails would be on shared computer drives of current employees
 - GC permitted erasing of former employee hard drives, without validating completeness of discovery production (GC wrongly assumed no back-up tapes kept for more than 10 days)
 - No reasonable basis for retained counsel's written assurance that "every effort" had been made to produce all relevant documents

Rule 34(a) Request for Production

- “The request may specify the form or forms in which ***electronically stored information*** is to be produced.”
- “If objection is made to the requested form or forms for producing ***electronically stored information*** — or if no form was specified in the request — the responding party must state the form or forms it intends to use.”
- “Unless the parties otherwise agree, or the court otherwise orders:
 - (ii) if a request does not specify the form or forms for producing ***electronically stored information***, a responding party must produce the information in a form or forms in which it is ordinarily maintained or in a form or forms that are reasonably usable; and
 - (iii) a party need not produce the same ***electronically stored information*** in more than one form.”

- USDC reverses Magistrate's sanction preventing Dell's use of ESI at trial
- Dell exported ESI into CaseData document review platform
- Original ESI stored in Dell system had "electronic directory structure" with "live user interfaces"
- Magistrate found Dell's production did not afford DE "same resources" as Dell

- USDC held “Rule 34 does not necessarily require that documents be produced in an identical format”
- The ESI produced was searchable
- Dell “satisfied the requirement that [ESI] was produced in the usual course of business”
- “The court also concludes that the information was produced in a manner that was reasonably useable”

- Proposed protocol drafted by joint bar-court committee
- “not adopted by the court but may be of assistance to counsel”
- Detailed and technically sophisticated application of ESI amendments to FRCP

- Rule 34: “ESI should be produced ... as Static Images ...in eitherTIF files ... or PDF”
- “load files should be produced together with Static Images” if created in converting native files to Static Images
- Meta-Data “need not be routinely produced”
- Party seeking production of Native File ESI must demonstrate “particularized need”
- Producing party must “maintain a separate file as a Native File and ... should not modify the Native File in a manner that materially changes the file and the Meta-Data”

- Rule 26 (f) Conference of Parties.
 - Parties encouraged to exchange ESI information before Conference about: Network design, types of databases, database dictionaries, security access logs, ESI retention policies, IT org chart
 - Before Conference counsel must:
 - Implement litigation hold
 - Designate IT person “to act as ESI coordinator” and discuss whether parties should have her participate in Conference
 - Become familiar with details of client’s current and past ESI

“The proposed amendments to Rule 16, Rule 26(a) and (f), and Form 35 present a **framework** for the parties and the court to give **early attention to issues relating to electronic discovery**, including the frequently-recurring problems of the **preservation of the evidence**

”

.....

-Judicial Conference Commentary on the Proposed Rule Amendments, September 2005

- At Rule 16 Conference, Counsel Must Be Prepared to Discuss ESI Preservation Efforts Taken at the Outset of Case

The Initial Disclosure Rules 26(a) & (f)

■ Key Guidance From New Judicial Handbook:

“All too often, attorneys view their obligation to ‘meet and confer’ under Federal Rule of Civil Procedure 26(f) as a perfunctory exercise. When ESI is involved, judges should insist that a meaningful Rule 26(f) conference take place and that a meaningful discovery plan be submitted.”

--*Managing Discovery of Electronic Information: A Pocket Guide for Judges*;
Federal Judicial Center, 2007

Phoenix Four v. Strategic Resources Group 2006 WL 1409413 (S.D.N.Y)

P A G E 22

- Defendants Preservation Efforts Scrutinized
- Defendant Failed to Timely Produce Relevant ESI Stored on Unmapped Server Partition
- Counsel “never undertook the more methodical survey of the ... sources of information that Judge Scheindlin outlined in *Zubulake V.*”
- “I am guided by the proposed amendments to [Federal Rule of Civil Procedure 26](#), which...essentially codify the teaching of *Zubulake IV & V*”
- Conclusions:
 - At Outset of Case, In House Counsel Must Understand Information Systems Architecture and Where Relevant ESI is Located.
 - A Pre-Established and Systemized Identification and Preservation Process Must Be in Place

- Plaintiff Brings Motion to Compel over Questionable eMail Production
- Court Not Satisfied with Defendant's Explanation of its Efforts
- "The producing party has the obligation to search available electronic systems for the information demanded...The new Federal Rule of Civil Procedure pertaining to electronically stored information makes this explicit.
- Court Applies Negative Correlation of Rule 26(b)(2)(B): "The obvious negative corollary of this rule is that *accessible* data must be produced at the cost of the producing party."
- "It cannot be argued that a party should ever be relieved of its obligation to produce accessible data merely because it may take time and effort to find what is necessary."

- **Will Defendant's Process Withstand This Scrutiny?:**

"Once the search is completed...Defendant must also file a statement under oath by the person who conducts the search, **explaining how the search was conducted**, of which electronic depositories, **and how it was designed to produce and did in fact produce all of the emails I have just described**. I must insist that the person performing the search have the **competence and skill to do so comprehensively**. An evidentiary hearing will then be held, at which I expect the person who made the attestation **to testify and explain how he or she conducted the search**, his or her qualifications to conduct the search, and why I should find the search was adequate."

- At This "Process Defense" Hearing (scheduled for April 5, 2007), Defendant Will Need to Demonstrate That Best Practices Processes and Technology were Employed

INTERMISSION



The World Leader in Digital Investigations

ACC AMERICA
Association of Corporate Counsel
Southern California Chapter (ACCA-SoCal)

Reducing Corporate Risks and Costs by Leveraging Technology for eDiscovery and Digital Investigations

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

© 2007 Guidance Software, Inc. All Rights Reserved.

DUFF & PHELPS

Participants

- **Michael F. Kelleher, Esq.**

- Partner, Folger Levin & Kahn LLP

- **Anthony J. Knaapen**

- Litigation Discovery Coordinator, Chevron Corporation

- **Victor Limongelli, Esq.**

- President, Guidance Software Inc.

- **Robert A. Shives, Jr., Esq.**

- Sr. Director & Assoc. General Counsel, Fujitsu America

Legal Standards are Changing



"We should be in good shape provided the judge doesn't go all 'legal' on us."

Agenda

- **Meeting the challenges of the FRCP amendments and reducing corporate risk using forensics technologies**
 - Custodian self-collection
 - Production of inaccessible data
 - Rule 37(f) “safe harbor”

- **Electronically Stored Information (“ESI”)**
 - Not just an FRCP issue
 - Same forensics technologies/tools, same technicians, and same processes can be used proactively for:
 - Effective records management
 - Data Privacy (PII) compliance and auditing
 - Reactive use for internal investigations

Risk Reduction Case 1: Custodian Self-Collection

■ **Case 1: Custodian Self-Collection**

- Not systemized or easily defensible; can alter relevant ESI
- eDiscovery not a core competency of rank-and-file employees
- Judgment calls being made by individual custodians – ripe for attack by your opponent

■ **Goal:** Reduce litigation and reputation risk; save money

Risk Reduction Case 1: Custodian Self-Collection in the Courts

- ***Samsung Electronics Co., Ltd. v. Rambus, Inc.***, 439 F.Supp.2d 524, 565 (E.D. Va. 2006)
 - “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”
- ***Exact Software North America, Inc. v. Infocon, Inc.***, 2006 WL 3499992 (N.D. Ohio, Dec. 5, 2006)
 - 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”
- ***Wachtel v. Health Net, Inc.***, 2006 WL 3538935 at *8 (D.N.J., Dec. 6, 2006)
 - 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.”

Risk Reduction Case 2: Resisting Requests for Inaccessible Data

- **Rule 26(b)(2)(B):** “A party need not provide discovery of [ESI] from sources that the party identifies as not reasonably accessible because of undue burden or cost.”
 - The producing party has the burden to demonstrate inaccessibility
 - Key committee notes:
 - Inaccessible ESI is still subject to preservation obligations
 - Requesting Party Should **First Seek and Evaluate Accessible ESI**

- **Goal:** Effectively resist discovery of inaccessible ESI

Risk Reduction Case 3: Taking Advantage of the Safe Harbor

- **Rule 37(f) “Safe Harbor”:** no penalties for deleting ESI due to routine operation of IT systems **if** reasonable preservation steps taken
 - Must be due to **Routine Operation** and in **Good Faith**
 - Procedures Must be: Established, Documented and Operational
 - Systemized Framework For Early Attention (Litigation Hold) Must be in Place

- **Goal:** Avoid spoliation claims but use 37(f) if needed

- **A systemized process using forensics technology to search for, collect and preserve potentially relevant ESI across the corporate network from a central location allows for a reasonable search process**
 - Legal department controls search criteria
 - IT uses technology to complete collection/preservation
 - Same process and technology used for every case
 - Early attention will have been achieved
 - Reasonable preservation steps will have been taken
 - Can blunt request for inaccessible data

Proactive Uses of Technology: Other Uses for Forensics Tools

■ Records Management

- **Goal:** Make RM policies operational
- **Solution:** use forensics technology to audit data stores and identify noncompliant data across the network from a central location

■ Data Privacy (PII) Compliance

- **Goal:** eliminate unauthorized customer data (PII) from the corporate network to reduce risk of data leakage
- **Solution:** use forensics technology to audit data stores and identify **and remediate** (i.e. “wipe”) PII from unauthorized locations from a central location

- Part 3 of today's presentation will address in detail
- Goal: Quickly investigate allegations
 - Whistleblower hotlines
 - Fraud
 - IP Theft
 - HR matters (harassment, etc.)
- Solution: using network-enabled computer forensics technology to search for, collect, preserve, and analyze potentially relevant evidence across the corporate network from a central location

- Legal department drives down costs and risks by controlling:
 - Electronic Discovery
 - Records Management
 - Data Privacy Issues
 - Internal Investigations

- Same tools, same technicians, and same processes
 - Avoid reliance on ad-hoc approaches (service providers hired to “put out the fire”)
 - Forensics tools can be a big part of the picture

INTERMISSION



The World Leader in Digital Investigations

ACC AMERICA
Association of Corporate Counsel
Southern California Chapter (ACCA-SoCal)

Using eDiscovery and Data Analytics for Auditing, Fraud Detection and Employee Investigations

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

© 2007 Guidance Software, Inc. All Rights Reserved.

DUFF & PHELPS

Agenda

How do you use the tools for an internal eDiscovery process in specific cases?

- Forensics and internal investigations: using your eDiscovery infrastructure for financial auditing and detecting financial fraud.
- Conducting internal employee investigations using your eDiscovery and forensic tools.

Participants

■ **Mike Gurzi**

- VP, Professional Services Development, Guidance Software, Inc

■ **Jenai Marinkovic**

- Sr. Mgr. Enterprise Security, DIRECTV

■ **Matthew Petrich**

- Director, Legal Business Solutions, Duff & Phelps

eDiscovery tied to Forensics:

- “Computer Forensics is simply the application of computer investigation and analysis techniques in the interest of determining potential legal evidence (Judd Robbins).”

- Electronically Stored Information (ESI) is key to this relationship
 - ESI is easily altered, deleted, moved
 - ESI, if not properly preserved, is very unstable.

- Forensics tools are required alongside a records retention policy in order to complete the eDiscovery process and comply with the amendments to the FRCP:
- How eDiscovery and Computer Forensics intersect:
 - Tell me what is out there
 - Tell me who has what
 - When was the last time something was used
 - Identify and destroy/remove data that is a liability
 - Preserve unique data

Additional Benefits of eDiscovery/Forensics Tools: Enterprise Investigative Capability

P A G E 44

■ 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

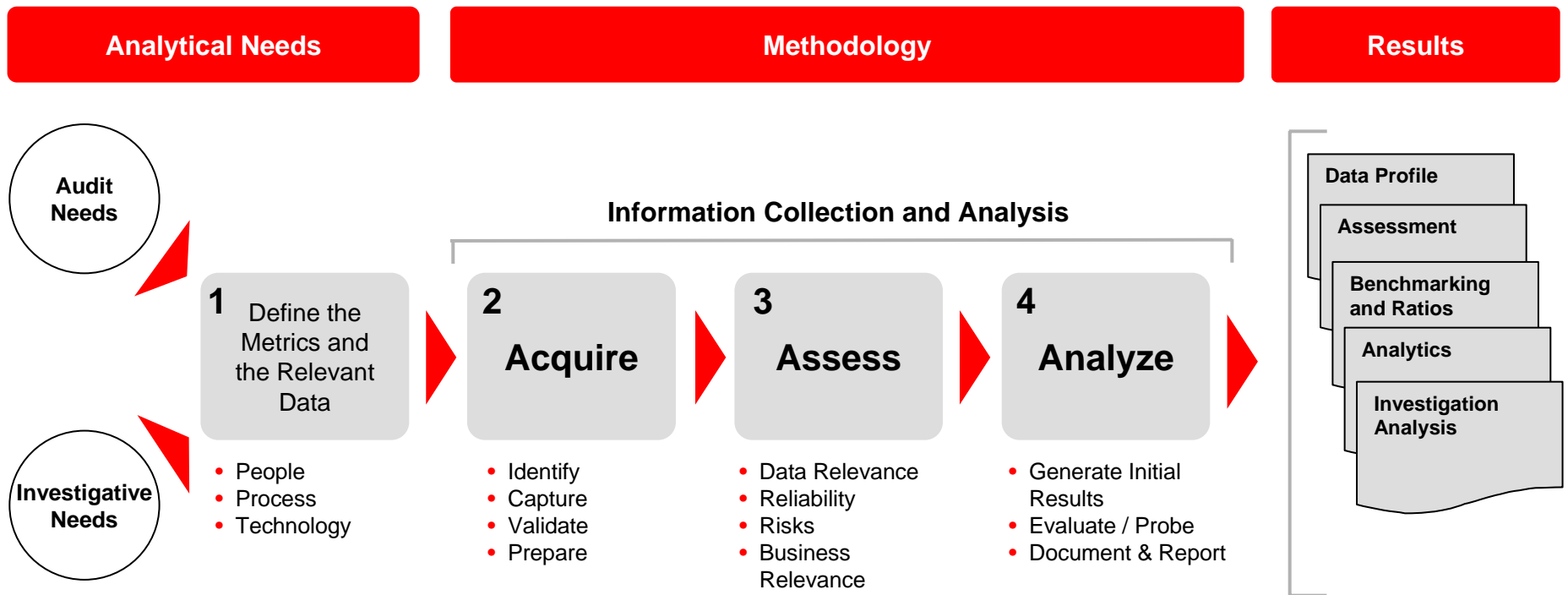
Additional Benefits of eDiscovery/Forensics Tools: Enterprise Investigative Capability

Forensics tools have many uses beyond eDiscovery

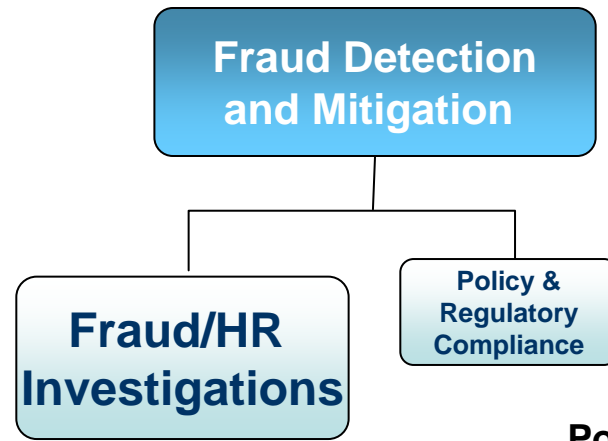
- **Records Retention Audits:** Forensics tools can be used to search for and identify different forms of ESI across the enterprise
- **Compliance Enforcement:** Forensics tools can assist the by identifying, collecting and removing files that are determined to violate an organization's policies
- **Data Leakage:** A good forensics product can scan for credit card numbers, social security numbers, etc.
- **And...**

Auditing, Fraud Detection and Employee Investigations

Analytic Support – Enable investigative teams to focus on the creation of ratios and metrics on “real time” data to improve on the quality of the investigative analysis. This type of investigative methodology will allow for technology tools and processes to be fully utilized in any type of audit or investigation.



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

- People
- Process
- Technology
 - Using your forensics & eDiscovery tools to complete the investigation

- Benefits of using forensics tools to collect from a remote location
 - No disruption to employee/business
 - Ability to reconstruct data where necessary using forensics

Internal Employee Investigations

- People
- Process
- Technology
 - Using your forensics & eDiscovery tools to complete the investigation

- Benefits of using forensics tools to collect from a remote location
 - No disruption to employee/business
 - Ongoing investigations can be carried out with ease

Series Conclusion

- **You can satisfy eDiscovery obligations while reducing risk, in compliance with the FRCP amendments & case law**
- Use Technology to Preserve Potentially Relevant Info
 - This will allow document systems to continue to operate, thus minimizing impact on operations
- Do Not Rely Solely on the Cooperation of Employees
 - Automating the search for information can minimize the impact of employee noncompliance with the litigation hold or investigation
- Use Accurate Tools
 - When processing computer evidence for judicial purposes, a party has “a duty to utilize the method which would yield the most complete and accurate results.” *Gates Rubber Co. v. Bando Chem. Indus., Ltd.*, 167 F.R.D. 90 (D.C. Col. 1996).