CLE - Electronic Discovery
Announcement

Date/Time: February 23, 2007 1:00 - 3:00pm
Location: 40 No Pearl St. Albany – 16th floor Conference Room, 40 North Pearl Street, Albany, NY

2 hours CLE in Law Practice Management

Description:

Over the past ten (10) years courts have consistently held that electronic "documents" are as discoverable as paper documents. Recent amendments to the Federal Rules of Civil Procedures (FRCP), effective December 1, 2006, explicitly make "electronically stored information" discoverable. Nearly all lawsuits filed today involve some form and degree of Electronic Discovery (eDiscovery), and the stakes are higher than ever.

Attorneys have certain duties throughout the eDiscovery process, as outlined in Zubulake v. USB Warburg, LLC (I-V). Further, in cases where the producing party violates the discovery agreement or breaches its duty to preserve evidence, the court may impose severe sanctions upon the producing party or grant relief to the demanding party.

Attorneys, law firms and businesses and government agencies must understand and abide by FRCP timelines, and be prepared to meet the complex challenges of eDiscovery to ensure fair, cost-effective and speedy disposition of legal matters.

AGENDA
Electronic Discovery CLE

Total session time – **2 hours**.

1. Introduction to Electronic Discovery – **5 minutes**

2. Current Legal Landscape – **30 minutes**
    a. Discussion of recent amendments to Federal Rules of Civil Procedure
    b. Discussion of seminal case law
    c. Differences between New York state law and Federal rules
    d. Legal issues to be covered:
        i. Duty to Preserve Electronically Stored Information
            1. When duty arises
            2. Duties of the producing party
            3. Duties of attorneys
        ii. Scope of Electronic Discovery
        iii. Allocation of Costs
        iv. Attorney-Client Privilege
            1. Protocols for conducting privilege review
            2. Use of "clawback" agreements

3. Electronic Discovery Planning and Preparation – **30 minutes**
    a. Records Management
    b. Preparing agency environment for electronic discovery
    c. Formation of an e-discovery / litigation response team
    d. When to consider using an outside vendor
    e. Guidelines for selecting an e-discovery vendor

4. Mechanics of Electronic Discovery – **30 minutes**
    a. Initial disclosures
    b. Preparation for the Rule 26(f) conference
    c. Data collection and preservation
    d. Data recovery and forensics
    e. Data filtering and processing
    f. Privilege review
    g. Production of electronic evidence
    h. Expert testimony

5. Practical Considerations – **15 minutes**
    a. Legally defensible discovery processes to pre-empt objections and challenges by adversary
    b. Use of Preservation Orders to compel protection of ESI
    c. Costs of electronic discovery
    d. Ethical and strategic considerations related to the use of vendors

6. Conclusion and Open Questions – **10 minutes**

ELECTRONIC DISCOVERY

CLE

2/23/07

Table of Contents

Electronic Discovery CLE

Total session time – **2 hours**.

1. Introduction to Electronic Discovery – **5 minutes**

2. Current Legal Landscape – **30 minutes**
    a. Discussion of recent amendments to Federal Rules of Civil Procedure
    b. Discussion of seminal case law
    c. Differences between New York state law and Federal rules
    d. Legal issues to be covered:
        i. Duty to Preserve Electronically Stored Information
            1. When duty arises
            2. Duties of the producing party
            3. Duties of attorneys
        ii. Scope of Electronic Discovery
        iii. Allocation of Costs
        iv. Attorney-Client Privilege
            1. Protocols for conducting privilege review
            2. Use of "clawback" agreements

3. Electronic Discovery Planning and Preparation – **30 minutes**
    a. Records Management
    b. Preparing agency environment for electronic discovery
    c. Formation of an e-discovery / litigation response team
    d. When to consider using an outside vendor
    e. Guidelines for selecting an e-discovery vendor

4. Mechanics of Electronic Discovery – **30 minutes**
    a. Initial disclosures
    b. Preparation for the Rule 26(f) conference
    c. Data collection and preservation
    d. Data recovery and forensics
    e. Data filtering and processing
    f. Privilege review
    g. Production of electronic evidence
    h. Expert testimony

5. Practical Considerations – **15 minutes**
    a. Legally defensible discovery processes to pre-empt objections and challenges by adversary
    b. Use of Preservation Orders to compel protection of ESI
    c. Costs of electronic discovery
    d. Ethical and strategic considerations related to the use of vendors

6. Conclusion and Open Questions – **10 minutes**

Speaker Biography

Michael Deyo leads the Electronic Discovery practice for JANUS Associates. He has been involved in the computer forensic and information security fields for seven years, working in both technical and project management roles. Mike has assisted several law firms in drafting electronic discovery motions and pleadings. He regularly leads and conducts computer forensic investigations for law firms, government agencies, and private businesses. Mike recently delivered a presentation on e-Discovery to the NYC Bar Labor and Employment Law Committee, and has served as an instructor and presenter for computer forensic workshops and seminars at national and state information security conferences for the past four years.

Mike holds a Bachelors Degree in Economic Crime Investigation and Computer Forensics from Utica College of Syracuse University. He is currently in his final semester at Albany Law School and will obtain his law degree this May. His unique combination of technical skills, practical experience, and legal training enables him to provide unique insight and solutions in matters involving Electronic Discovery and the use of electronic evidence.

Electronic Discovery

Michael Deyo
Practice Manager
JANUS Associates, Inc.

Copyright © 2007 Michael Deyo

Course Outline

- Introduction to Electronic Discovery
- Overview of Legal Issues and Rules
- Practical Considerations for Electronic Discovery Planning and Preparation
- Mechanics of Electronic Discovery

Copyright © 2007 Michael Deyo

Introduction to Electronic Discovery

- Broad Discovery Rights Under Fed. R. Civ. P.
- Shift From Paper "Documents" to "ESI"
- Unique Challenges of ESI
- Seriousness of Electronic Discovery
  - *Zubulake* decisions
  - Coleman (Parent) Holdings v. Morgan Stanley & Co., 2005 WL 679071 (Fla. Cir. Ct. 2005)
  - Recent amendments to the Federal Rules

Copyright © 2007 Michael Deyo

Current Legal Landscape

- Federal Rules of Civil Procedure
- *Zubulake* Series of Opinions
- Interplay of Federal Law and New York State Law
  - The CPLR has been interpreted to be virtually parallel to the FRCP
  - New York State cases expressly cite federal cases on issues of electronic discovery
    - *See,* Delta Financial Corp. v. Morrison, 819 N.Y.S.2d 908; Ball v. State, 421 N.Y.S.2d 328

Copyright © 2007 Michael Deyo

Legal Issues and Rules

- The Duty to Preserve
  - Need to preserve ESI that is potentially relevant to litigation
    - **Step 1:** Identify "key players"
    - **Step 2:** Identify data sources for each "key player"
    - **Step 3:** Issue litigation hold notice
    - **Step 4:** Take action to preserve data
    - **Step 5:** Ongoing duty to preserve ESI

Copyright © 2007 Michael Deyo

Legal Issues and Rules

- The Duty to Preserve, Cont'd
  - When the duty arises
    - General Rule: when a party receives ***notice*** that evidence is relevant to litigation ***or*** when party reasonably should have known evidence would be relevant to ***reasonably foreseeable*** litigation
    - *See*:
      - Concord Boat Corp. – duty was triggered when complaint was filed
      - Zubulake IV – duty was triggered even before EEOC complaint was filed (6 months before termination and 10 months before lawsuit)
      - Scott v. IBM – duty was triggered before termination because IBM was dealing with a "potentially litigious" employee

Copyright © 2007 Michael Deyo

Legal Issues and Rules

- The Duty to Preserve, Cont'd
  - Duties of Parties to Litigation
    - Identify "key players"
    - Issue litigation hold
    - Implement reasonable technical measures
      - Image servers
      - Instruct "key players" to provide copies of files
      - Interrupt automated data destruction practices
      - Suspend backup tape recycling

Copyright © 2007 Michael Deyo

Legal Issues and Rules

- The Duty to Preserve, Cont'd
  - Attorney Duties
    - Locate potentially relevant information after becoming "fully familiar" with client's IT architecture
    - Issue litigation hold
    - Communicate directly with "key players"
    - Oversee evidence preservation practices of client
  - Counsel must coordinate client's discovery efforts; counsel is "more conscious of the contours of the preservation obligation" – Zubulake V

Copyright © 2007 Michael Deyo

Legal Issues and Rules

- Spoliation of Evidence
  - Spoliation = breach of duty to preserve
  - Spoliation triggers the issue of sanctions
    - Examples of sanctions:
      - Award of costs and fees
      - Adverse inference jury instruction
      - Dismissal or default judgment
    - Severity of sanction based upon party's level of culpability
      - In NY, even negligence will get adverse inference
    - Sanctions under the Rule 37 "Safe Harbor"

Copyright © 2007 Michael Deyo

Legal Issues and Rules

- Scope of Electronic Discovery
  - Rules 26 and 34 grant broad discovery rights
  - Deleted data is discoverable
  - Important limitation under Rule 26(b)(2)(B)
    - Not required to provide discovery of ESI from sources identified as "not reasonably accessible" because of undue burden or cost
    - Examples of accessible vs. inaccessible data
      - *Active files vs. deleted files*
      - Live servers vs. backup tapes

Copyright © 2007 Michael Deyo

Legal Issues and Rules

- Scope of Electronic Discovery
  - Direct access to an adversary's system
    - Rule 34 permits party to "inspect, copy, test, or sample" ESI
    - Advisory Committee cautioned that this does not create a routine right of direct access
    - Courts are split on this point
      - All will require some improper conduct by the producing party prior to ordering direct access
    - Important for producing party to follow a legally defensible protocol to preempt direct access

Copyright © 2007 Michael Deyo

Legal Issues and Rules

- Allocation of Costs
  - Under FRCP, presumption is the producing party bears the costs of production
  - Cost shifting will only be considered when discovery imposes "undue burden or expense"
    - Typically the issue will arise if production of inaccessible data is demanded
  - Court-devised protocols for cost-shifting:
    - *Rowe* – 8 factor test
    - *Zubulake* – 7 factor test

Copyright © 2007 Michael Deyo

Legal Issues and Rules

- Allocation of Costs
  - Under NY CPLR, we have the opposite presumption (*see, e.g.,* Lipco Elec. Corp. v. ASG Consulting Corp., 798 N.Y.S.2d 345)
  - Analysis begins and ends with whether discovery is permissible
    - If permissible, discovery will only be ordered if requesting party agrees to pay

Copyright © 2007 Michael Deyo

Legal Issues and Rules

- Protection of the Attorney-Client Privilege
  - Risk of Inadvertent Disclosure and Waiver
  - Review Protocols:
    - "Quick Peek" Production
    - Screened Production
  - Rule 26(b)(5)(B) – procedure for asserting claim of privilege after production
    - Just a procedure; does not govern waiver
  - Use of "clawback" agreements and protective orders

Copyright © 2007 Michael Deyo

Electronic Discovery Planning & Preparation

Copyright © 2007 Michael Deyo

E-Discovery Planning and Preparation

- Records Management Program
  - Goals:
    - Reduce the amount of discoverable data
    - Reduce the costs of review and production
    - Structure data retention program to promote cost shifting
    - Develop "litigation hold" process

Copyright © 2007 Michael Deyo

E-Discovery Planning and Preparation

- Records Management Myth #1
  - The new Federal Rules require businesses and government agencies to preserve all email, instant messages, and other electronic communications
  - The Truth:
    - There is no obligation to preserve data under the Rules unless the duty to preserve is triggered
    - Even then, only relevant ESI must be preserved

Copyright © 2007 Michael Deyo

E-Discovery Planning and Preparation

- Records Management Myth #2
  - Setting size limits for email mailboxes is a sufficient records management practice
  - The Truth:
    - Users are still able to archive messages locally or to a network drive; this complicates e-discovery
    - Need to provide training to users
    - Need to create a system of organization, not just data limitation

Copyright © 2007 Michael Deyo

E-Discovery Planning and Preparation

- Records Management Myth #3
  - The implementation of an automated data deletion process is a sufficient records management practice
  - The Truth:
    - Data deletion does not get rid of all discoverable ESI; deletion does not erase data
    - Mere implementation is dangerous without rigorous procedures for litigation response and management
    - Need to create structure for data organization, not just engage in deletion

Copyright © 2007 Michael Deyo

E-Discovery Planning and Preparation

- Records Management Myth #4
  - There is no real distinction between data backup and data archiving
  - The Truth:
    - The amended Rules and case law create this distinction (reasonably accessible vs. not reasonably accessible)
    - A label is not enough; there must be some formal process for distinguishing between backups for archival and backups for disaster recovery

Copyright © 2007 Michael Deyo

E-Discovery Planning and Preparation

Prepare Environment for Data Recovery

- Establish continuity / redundancy for critical systems
- Implement data backup solutions / E-Discovery platform
- Develop plans for legacy systems
- Provide training and conduct testing

Copyright © 2007 Michael Deyo

E-Discovery Planning and Preparation

- Building the Litigation Response Team
  - IT Personnel
  - Management
  - Inside Counsel
  - Outside Counsel
  - Vendor

Copyright © 2007 Michael Deyo

E-Discovery Planning and Preparation

- Use of Third Party Experts
  - Records Management Planning
  - Litigation Support
    - Support in drafting E-Disclosures, interrogatories, deposition questions, preservation letters, motions
    - Support in structuring discovery plan
    - Bridge the "communication gap" between IT staff and attorneys
  - Data Collection, Processing, and Hosting

Copyright © 2007 Michael Deyo

E-Discovery Planning and Preparation

- Use of Third Party Experts: Ethical and Strategic Considerations
  - Deposing the Vendor
    - Benefits of testimony vs. risks of disclosure
  - Structuring the Vendor's Report
    - Again, consider risks of disclosure
  - Maintaining Confidentiality
  - Avoiding Conflicts

Copyright © 2007 Michael Deyo

E-Discovery Planning and Preparation

- Credibility
  - Experience
    - "Copy shop" vs. firm with IT and forensics experience
  - Expertise
    - Use firms with industry recognition
    - Look for firms with attorneys on-staff
    - Look for individuals with technical certifications
  - Reputation and Past Performance
- Innovation and Technology Solutions
- Business Viability – will the vendor be around if the case goes to court?

Copyright © 2007 Michael Deyo

Mechanics of Electronic Discovery

Copyright © 2007 Michael Deyo

Mechanics of Electronic Discovery

- Litigation Hold
  - Need to initiate as soon as duty to preserve is triggered
    - **1st Step:** Identify "key players"
    - **2nd Step:** Locate data sources for each
    - **3rd Step:** Send litigation hold notice
    - **4th Step:** Follow-up with and remind each "key player"
  - Proper identification of data sources enables the development of a comprehensive and well-structured discovery plan
    - Efficient collection of relevant evidence
    - Preempt objections and court orders

Copyright © 2007 Michael Deyo

Mechanics of Electronic Discovery

- Preparation for Rule 26(f) Conference
  - Be prepared to discuss and disclose:
    - Data storage areas that contain relevant ESI, including geographic locations
    - Current personnel who may possess relevant ESI
    - List of operating systems and applications in use
    - Backup procedures and retention schedules
    - Types of data stored on backup tape; age of backup tapes; location of tapes
    - Data retention policies and enforcement mechanisms
    - Data preservation methods

Copyright © 2007 Michael Deyo

Mechanics of Electronic Discovery

- Initial E-Disclosures
  - Need to disclose:
    - "Key players" (also called "Key Custodians")
    - Sources of potentially responsive ESI
    - Relevant technical information
      - Operating system(s) – Windows, mainframe, etc.
      - Application(s) – email, database, backup, etc.
    - Sources of ESI "not reasonably accessible"
      - Backup tapes, certain legacy systems, etc.
    - Steps taken to preserve relevant ESI

Copyright © 2007 Michael Deyo

Mechanics of Electronic Discovery

- Process for E-Discovery:
  - Data Preservation and Collection
  - Data Recovery and Forensics
  - Data De-Duplication, Filtering and Searching
  - Conversion to Review Platform
  - Privilege Review
  - Production of ESI

Copyright © 2007 Michael Deyo

Mechanics of Electronic Discovery

- Data Preservation and Collection
  - Forensic Acquisition vs. Mere Copying
    - Forensic acquisition = complete mirror image
    - Mere copying = capture of "active" files
  - Advantages of forensic acquisition:
    - Captures all potentially relevant data
    - Authentication of data
    - Chain of custody

Copyright © 2007 Michael Deyo

Mechanics of Electronic Discovery

- Data Recovery and Forensics
  - Types of Data:
    - Active files
    - Deleted files
    - Hidden files
    - Corrupted files
    - Residual data (e.g. swap space, slack space)
    - Metadata
    - Protected files (e.g. password, encryption)

Copyright © 2007 Michael Deyo

Mechanics of Electronic Discovery

- Data Processing
  - De-Duplication
  - Filtering
    - System files vs. user-created files
  - Searching
    - Counsel must agree upon search terms
    - Example of Boolean search:
      - "ipod" /25 "pric!" AND "set!" OR "limit!" OR fix!"

Copyright © 2007 Michael Deyo

Mechanics of Electronic Discovery

- Conversion to Review Platform
  - Publish responsive data to document review platform
  - Hosted solution vs. in-house software
  - Select platform that will allow "tagging" and redaction
  - Consider security and user access requirements

Copyright © 2007 Michael Deyo

Mechanics of Electronic Discovery

- Privilege Review
  - Choice of review protocol – "Quick Peek" vs. screened production
  - Review Process:
    - Review documents and metadata
      - Separate relevant from irrelevant; privileged from non-privileged; code evidence under protective order
      - Maintain privilege log
    - The "Rule of 200" – multiply number of Gigabytes of data by 200 to derive estimate for man-hours
      - Ex. 20 GB x 200 = 4,000 hours
      - 4,000 hours / 10 people / 40 hr/wk = 10 Weeks!!

Copyright © 2007 Michael Deyo

Mechanics of Electronic Discovery

- Production of ESI
  - Four available formats:
    - Paper printouts
    - Quasi-paper electronic files (PDF, TIFF)
    - Load files for litigation software
    - "Native" electronic format
  - Electronic vs. paper production
    - Courts will generally require production in electronic format, due to the sheer volume of documents – Gilliam v. Addicts Rehab. Ctr. Fund

Copyright © 2007 Michael Deyo

Mechanics of Electronic Discovery

- Production of ESI
  - Quasi-paper production
    - Advantages
      - Requesting party only needs one program to view
      - Tight control over what is produced
      - Lose certain data (e.g. metadata, Excel formulas)
    - Disadvantages
      - Need to convert native files to PDF or TIFF
      - TIFF images are not text searchable
      - PDF and TIFF files do not contain metadata; may need to extract metadata and supplement production

Copyright © 2007 Michael Deyo

Mechanics of Electronic Discovery

- Production of ESI
  - Load File Production
    - Advantages
      - Quick and easy to load into litigation software (e.g. Concordance, Summation)
      - Familiar application for both parties; no need to undergo training on new review platform
    - Disadvantages
      - Need to convert native files to load files (adds time and cost to production)
      - Metadata may not be captured through conversion process; may need to extract and produce metadata

Copyright © 2007 Michael Deyo

Mechanics of Electronic Discovery

- Production of ESI
  - Native Format Production
    - Advantages
      - No need to convert data files
      - Metadata remains in-tact; Excel formulas disclosed
    - Disadvantages
      - Requesting party needs to have original application in order to view native files
      - More difficult to reference native files (can apply Bates numbering to PDF / TIFF, but not native files)
      - More difficult to redact from native files

Copyright © 2007 Michael Deyo

Mechanics of Electronic Discovery

- Legal Authority
  - Rule 34: requesting party may specify form or forms
    - If requesting party does not specify, producing party must state the form or forms it intends to use
    - Either party may object; court may order format
  - Courts are split on issue of production format
    - *In re* Priceline – court ordered production in TIFF or PDF with searchable metadata database
    - *In re* NYSE – ordered production in native format
    - Williams v. Sprint – must produce ESI with metadata in-tact
    - Wyeth v. Impax – only need to produce metadata if "particularized need"

Copyright © 2007 Michael Deyo

Mechanics of Electronic Discovery

- Best Practices for Production
  - Use two-tiered production
    - Produce accessible data first; only produce inaccessible data if necessary
    - If inaccessible data is requested, bring up the issue of cost shifting
  - Bifurcate production formats
    - Produce certain data in native format (e.g. spreadsheets, Word documents, etc.)
    - Produce other data is quasi-paper format (e.g. databases, legacy systems, obscure data files) with supplemental metadata

Copyright © 2007 Michael Deyo

Mechanics of Electronic Discovery

- Expert Testimony
  - Testify as to data recovery and forensic procedures
  - Validate or "poke holes" in recovery / forensic procedures employed by adversary and third parties
  - Provide testimony regarding costs and complexity of E-Discovery matters
  - Provide testimony regarding potential for data destruction / spoliation by adversary

Copyright © 2007 Michael Deyo

Costs of Electronic Discovery

- Quinby v. WestLB AB (S.D.N.Y. 2006)
  - **$181,013** to process over 171 backup tapes and search hard drives, plus 25% (**$45,253.32**) to expedite the project
  - Produced 59,635 "original" documents (401,420 pages)
- Zubulake v. UBS Warburg (S.D.N.Y. 2004)
  - $245 / hour plus $18.50 for "CPU Bench Utilization"
  - Total cost for restoration and searching 77 backup tapes - $177,479
  - Total cost for production - **$292,653**
- Medtronic Sofamor Danek, Inc. v. Michelson (W.D. Tenn. 2003)
  - Vendor quoted **$605,300** to process 124 backup tapes
  - The court noted that the quote of $4,881 per tape for restoration, searching, and de-duplication "appears reasonable"
- Cases do not include costs of attorney review

Copyright © 2007 Michael Deyo

Services to Enable the Practice of Law

- Business Counseling
  - Records Management
  - E-Discovery Planning and Preparation
- Litigation Support
- Discovery and Production of Electronic Evidence
  - Data Recovery and Forensics
  - Data Filtering and Processing
  - Review of Electronic Documents
  - Production of Electronic Evidence
  - Expert Testimony

Copyright © 2007 Michael Deyo

Thank You

For any additional information or material, please contact:

Michael Deyo
MichaelD@JanusAssociates.com
(518) 478-9492

Copyright © 2007 Michael Deyo

Electronic Discovery

Analysis of Recent Developments in
Electronic Discovery Law and Practice

By: Michael Deyo

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Rules

I. INTRODUCTION

"Metadata" ... "ESI" ... "native format" ... "unallocated space". Attorneys are quickly becoming forced to understand and be fluent in a new language. Electronic discovery (e-discovery) is now an essential part of litigation, and the stakes are higher than ever. No longer will courts permit ignorance or carelessness with respect to e-discovery. Attorneys engaged in litigation must ensure compliance with the recent amendments to the Federal Rules of Civil Procedure (the "FRCP" or "Rules") through the preservation and production of electronic evidence. Litigators cannot dodge issues of electronic discovery; the FRCP now mandates litigants to discuss and plan for e-discovery early in litigation. *See* Fed. R. Civ. P. 26(f). By failing to do so, attorneys not only run afoul of procedural rules and perform a disservice to clients, but also risk destruction of crucial electronic evidence.

Counsel seeking discovery in litigation must embrace e-discovery to assure the zealous representation of its clients. Counsel representing parties from whom discovery is sought must be aware of e-discovery issues to limit the burden, expense, and risks of litigation for its clients. Failures in the e-discovery process not only open attorneys and their clients to court-imposed sanctions but will also create attorney liability for professional malpractice. Recent case law is rampant with notable e-discovery failures. For example, missteps in the preservation and production of electronic evidence in Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co. Inc., prompted the court to issue an adverse inference jury instruction, which contributed to a $1.45 billion jury verdict. 2005 WL 679071, at *7 (Fla. Cir. Ct. 2005). In addition, the Judge in *Coleman* was so enraged by the defendants' discovery missteps and efforts to "stonewall" the production of e-mail that he revoked their counsel's *pro hac vice* admission (which was later

reinstated on appeal). To make matters worse, in-house counsel for Morgan Stanley publicly declared that the company intended to sue its attorneys for their mishandling of the case.

Unfortunately for attorneys and clients alike, e-discovery is fraught with risks and danger due to its complex and evolving nature. The practice of e-discovery involves addressing issues related to: (i) the duty to preserve electronically stored information (ESI); (ii) the scope of discovery; (iii) allocation of costs; (iv) preserving the attorney-client-privilege and mitigating the risk of waiver; and (v) the production of electronic evidence. The purpose of this paper is to provide an overview of recent developments in the landscape of electronic discovery law and to provide analysis of how the recent FRCP amendments will affect the legal and technical practice of electronic discovery.

A. Discovery Rules Generally

Discovery is the stage in litigation where one party discloses to another all records, documents, and other information in its exclusive possession, custody, or control that are relevant in asserting a claim or defense. In order to admit evidence into a judicial proceeding, it must first be discovered. Several discovery devices are used to obtain information from an adverse party or non-party to a lawsuit, including depositions, interrogatories, document requests, and subpoenas. The request for the production of "documents" and "things" is often the most practical and productive discovery device in litigation involving a commercial party.

A party from whom discovery is sought (the "producing" or "responding" party) is usually responsible for producing its records and documents to the "requesting" party. The requesting party is responsible for ensuing that the producing party abides by the terms and stipulations of the discovery plan, and the court is responsible for enforcing the discovery obligations of each party. The objectives of discovery are to enhance the truth-seeking function of litigation; to enable attorneys to prepare for trial in an informed and even-handed manner; to prevent

concealment or surprise; and to further the ends of justice by promoting the speedy and final disposition of legal controversies.[1]

Discovery rights applicable to litigation in federal courts are defined broadly under the FRCP. Any party may serve on another party to the lawsuit, or any person not a party to the lawsuit, a request to produce or to make available for inspection, copying, testing, or sampling any designated documents, subject to the scope of discovery permitted under Rule 26. Fed. R. Civ. P. 34(a); Fed. R. Civ. P. 45(a)(1)(C). A party must provide to other parties all documents that are in the possession, custody, or control of the producing party, and that the producing party may use to supports its claims or defenses, unless solely for impeachment. Fed. R. Civ. P. 26(a)(1)(B). Parties are entitled to obtain discovery of any non-privileged information that is relevant to the claim or defense of any party. Fed. R. Civ. P. 26(b)(1). Information protected by attorney-client privilege is generally not discoverable under Rule 26(b)(5). Information does not need to be admissible at trial in order to be discoverable, so long as the requested discovery appears "reasonably calculated to lead to the discovery of admissible evidence". Fed. R. Civ. P. 26(b)(1). Rule 26(b)(2) imposes limitations upon the broad scope of discovery by permitting a court to limit discovery based upon a proportionality test that weighs the burden and expense of the proposed discovery against the expected benefit of discovery.

B. The Shift From Paper to Electronic Discovery

Paper records have traditionally been the focus of requests for the production of documents. There has been a substantial reduction in the use and prevalence of paper records over the past several years, thus significantly reducing the utility of paper document requests. As business practices continue to evolve, the volume of paper records will continue to decrease due

---

[1] 27 C.J.S. *Discovery* § 2 (2006).

to the implementation of paperless systems. Further, the widespread prevalence, acceptance, and use of electronic mail (e-mail) in conducting transactions in the normal course of business means that electronic systems are used to process and store many types of transactions (including, *inter alia*, wrongful conduct).

It has been estimated that ninety-three percent (93%) of all information generated in 1999 was generated in digital form on computers.[2] Today, it is estimated that ninety-nine percent (99%) of all documents are created and stored in electronic form, and many are never printed to hard copy.[3] Further, sixty to seventy percent (60-70%) of all corporate data resides in or is attached to e-mail messages and ninety percent (90%) of business communications are conducted by e-mail, instant messaging, and voicemail. Id. Quite simply, discovery of paper documents alone no longer achieves the objectives of the discovery process.

The process of discovering ESI for use as evidence in legal proceedings is termed "electronic discovery" or "e-discovery". Nearly all lawsuits filed today involving a commercial party involve some degree of e-discovery. While discovery devices remain the same regardless of the form in which information is created or stored, discovery of ESI presents unique challenges and issues. First, unlike paper documents which typically reside in visible physical locations, data stored in electronic format can reside in a number of inconspicuous sources, including backup media; hidden and deleted files; and metadata[4]. Second, attorneys requesting and responding to discovery must become knowledgeable of complex information systems in order to locate relevant

---

[2] *In re* Bristol Myers Squibb Sec. Litig., 2002 U.S. Dist. LEXIS 13808 (D.N.J. 2002).

[3] Stephen D. Whetstone and Michael S. Simon, *Electronic Discovery: The Stakes Have Never Been Higher*, The National Law Journal, July 17, 2006, *at* http://www.stratify.com/resources/publications/nlj_high_stakes.pdf

[4] Metadata is essentially "data about data", in that metadata describes the history, tracking, management, condition, and other characteristics of data. Certain metadata, such as file creation and modification dates, can be view by non-technical users. Other metadata fields may be embedded or hidden within an electronic file, thus requiring specialized knowledge and software to extract and view the metadata.

data sources and ensure evidence preservation duties are upheld. Third, due to the volatile nature of electronic data and the ease with which electronic data can be modified or destroyed, either intentionally or negligently, strict evidence preservation protocols and procedures must be followed to ensure evidence is retained and is original and authentic.

Electronic discovery is not a replacement for paper discovery; discovery in both formats is required to capture all potentially relevant information. For example, while an electronic file may contain metadata not present in a computer printout, the printout may contain handwritten notes not present in the electronic version. Proper discovery enables all parties to assess the relative strengths and weaknesses of each position and to reach a fair settlement without incurring the substantial expense and risks of further litigation. In practice, nearly ninety-five percent (95%) of all civil cases are settled after discovery.[5]

In order for attorneys to best serve the interests of clients by obtaining the just and speedy disposition of legal matters, it is becoming increasingly important to conduct proper e-discovery. The law governing the discovery of ESI has struggled to keep pace with the shift from predominately paper to electronic records kept in the ordinary course of business. The changing landscape of discovery law, combined with the need to understand fundamental technological concepts in order to properly apply e-discovery law, has proven a challenge for many attorneys and seasoned litigators.

1. Development of Case Law

As discussed *supra*, Rules 26 and 34 make "documents" and "things" subject to disclosure. The 1970 Advisory Committee Notes to Rule 34 made it clear that Rule 34 was to be applied to computer technology as well as paper documents. The description of "documents" was

---

[5] *See*, http://www.perkinscoie.com/area.cfm?id=220.

revised in the Advisory Committee Notes to Rule 34 to state that Rule 34 applies to "electronic data compilations"; however, the Notes were vague as to what exactly constituted an "electronic data compilation".[6] Since this revision, it has become well-settled law that electronic documents are just as discoverable as paper documents under Rules 26 and 34. *See* Anti-Monopoly, Inc. v. Hasbro, Inc., 1995 WL 649934, at *2 (S.D.N.Y. 1995) (in deciding whether to grant the plaintiff's motion to compel production of computerized data the court stated "today it is black letter law that computerized data is discoverable if relevant"); Playboy Enters., Inc. v. Welles, 60 F.Supp.2d 1050, 1053 (S.D. Cal. 1999) (in a case brought by a magazine publisher alleging various trademark and unfair competition causes of action against a former "Playmate of the Year", the court stated that by requesting documents under Rule 34 the plaintiff also implicitly requested production of information stored in electronic form); Rowe Entm't., Inc. v. The William Morris Agency, Inc., 205 F.R.D. 421, 428 (S.D.N.Y 2002) [hereinafter *Rowe*] (in a much-cited decision it was held that "electronic documents are no less subject to disclosure than paper records"); Delta Fin. Corp. v. Morrison, 819 N.Y.S.2d 908, 912 (Sup. Ct. Nassau Cty. 2006) (in an action brought by a stockholder against the defendant LLC, the Supreme Court of Nassau County relied upon *Rowe* in holding that under the New York Civil Practice Law and Rules (CPLR), like the Federal Rules, "electronic documents are no less subject to disclosure than paper records").

Further, the Southern District of New York has ruled that electronic data must be produced even if paper records of the same information have already been provided. Anti-Monopoly, Inc.,

---

[6] The Notes stated that Rule 34 applied to "electronic data compilations" from which information can be obtained only with the use of "detection devices". The Notes did not explain what "detection devices" were contemplated by the Committee, and, as the computer industry evolved this term became ambiguous and inapplicable to many forms of electronic storage systems. Further, the Advisory Committee Notes stated that in order for a party to produce information in a useable form, the producing party would need to supply a printout of computer data. As the capacity of data storage systems increased exponentially, it became increasingly burdensome and inefficient to produce electronic data in printouts.

at *1. The Eastern District of Wisconsin, however, has adopted an opposite rule whereby if a party produces electronic information in a hard copy format that "mimics" the electronic format, it is not required to produce both. India Brewing, Inc. v. Miller Brewing Co., 237 F.R.D. 190, 194 (E.D. Wis. 2006). This represents a divide in the development of electronic discovery law, but more importantly highlights a fundamental misunderstanding of paper versus electronic records. The two forms are not identical and are not mutually exclusive. For reasons discussed above, discovery of the same material in both hard copy and electronic format is required, as each format may contain information not present in the other.

Judge Shira Scheindlin of the U.S. District Court for the Southern District of New York has issued the most comprehensive and influential decisions through a series of five opinions in the Zubulake case (each discussed and cited *infra*). The Zubulake decisions have addressed, *inter alia*, issues related to the scope of electronic discovery; allocation of discovery costs; preservation of evidence; spoliation of evidence; and sanctions for spoliation.

2. Amendments to the Federal Rules of Civil Procedures

Although the FRCP contemplated the discovery of electronic information and courts have applied these rules to decide electronic discovery issues, the FRCP failed to take into consideration the significant differences between ESI and information stored on paper. Report of the Civil Rules Advisory Committee, July 25, 2005 at 10. As information technology evolved it became increasingly difficult to fit dynamic ESI, many forms of which do not resemble the fixed expression of information on paper (e.g. dynamic databases), within the definition of "documents". Amendments to Rules 16, 26, 33, 34, 37, and 45 were drafted to serve as a "comprehensive package" addressing the discovery of ESI, as well as paper records. The amended Rules became effective December 1, 2006.

Most notably, Rules 26, 34, and 45 now explicitly make "electronically stored information" discoverable. Further, the amended Rules clarify that any discovery reference to "documents" must also be understood to include ESI, unless expressly stated otherwise. The inclusion of ESI in Rules 26, 34, and 45 is intended to "confirm that discovery of electronically stored information stands on equal footing with discovery of paper documents." Advisory Committee Notes to Fed. R. Civ. P. 2006 Amendments.

The amended Rules will force attorneys to learn and embrace electronic discovery, in order to avoid running afoul of the Rules and to prevent the destruction of electronic evidence. Amended Rule 26 requires attorneys to discuss at the 26(f) conference "issues relating to the disclosure or discovery of ESI, including the form or forms in which it should be produced" and "any issues relating to claims of privilege or of protection". Fed. R. Civ. P. 26(f)(3),(4). This requires attorneys to be prepared to discuss e-discovery matters within ninety-nine (99) days of filing a lawsuit, which will often require some knowledge of a client's or adversary's information systems and data retention practices. Further, Rule 16 states that a court may include "provisions for disclosure or discovery of ESI" in it scheduling order. Fed. R. Civ. P. 16(b)(5). The impact of the FRCP amendments will be discussed throughout the remainder of this paper, as they relate to specific legal issues and doctrines.

II. THE DUTY TO PRESERVE EVIDENCE

A party to a lawsuit is required to preserve evidence that is potentially relevant to the litigation. Fujitsu Ltd. v. Fed. Express Corp., 247 F.3d 423, 436 (2d Cir. 2001). This rule does not require a party to keep or retain every document or electronic record in its possession. Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 217 (S.D.N.Y. 2003) [hereinafter *Zubulake IV*]. To require a corporation to preserve every electronic and paper record, including all e-mail and

backup tapes, would "cripple large corporations ... that are almost always involved in litigation". Id. Generally, the party need not preserve evidence that is not properly discoverable under Rules 26 and 34, however, under Rule 26(b)(2) a party is not relieved of its common law duty to preserve evidence solely because the party identifies the data as "not reasonably accessible", thus removing the data from the scope of discovery (*see infra* at p.26). A litigant is under a duty to preserve only those documents and ESI that are relevant to the litigation; are reasonably calculated to lead to the discovery of admissible evidence; are reasonably likely to be requested during discovery; or are the subject of a pending discovery request. Concord Boat Corp. v. Brunswick Corp., 1997 WL 33352759, at *4 (E.D. Ark. 1997).

Although these rules appear to place substantial limits upon the duty to preserve, in practice the duty applies broadly. For example, the duty to preserve extends to documents and ESI created by or prepared for "key players" in the litigation. Zubulake IV, 220 F.R.D. at 218. The "key players" include individuals likely to have discoverable information that any party may use to support its claims or defenses. Id. The development of an exhaustive list of all such "key players" in a particular lawsuit is a difficult task. This is particularly true where a large number of individuals have differing roles and responsibilities in the events that led to the litigation, such as in an anti-trust or unfair business practices lawsuit. In fact, it may be only after some discovery occurs that all of the key players are actually identified. At this point in the litigation, however, certain relevant data may have been destroyed, thus placing the producing party at risk of sanctions for the negligent or willful spoliation of evidence.

An even more difficult task than identifying all of the "key players" early in the litigation is identifying all of the data sources that contain the documents and ESI created by or prepared for the "key players". For example, e-mail messages and records of e-mail messages can exist in a number of data sources, including corporate e-mail servers; desktop or laptops computers used at

the workplace; home computers used to access workplace e-mail; BlackBerry and other portable e-mail devices; backup tapes; data warehousing applications; removable media; and "retired" media no longer in active use. While courts tend to underestimate the challenges involved in identifying the "key players", an even greater issue facing producing parties is that courts miss the logical extension of that requirement; that is, identifying the myriad of data sources that can exist for *each* of the "key players" and then implementing preservation efforts for each data source.

Given the variety of storage options for ESI it is likely that one document or record will exist in more than one data source. Although a party is not required to retain multiple identical copies of relevant documents (*See* Zubulake IV, 220 F.R.D. at 218), an issue exists as to whether seemingly identical documents are truly identical. For example, if an e-mail is sent to four recipients, at least five seemingly identical documents will exist (the four messages received and the one sent). If that e-mail is then forwarded by each of the four recipients, the number of seemingly identical documents can grow exponentially. These e-mail messages are not identical, however, as different metadata will attach to each. Further, if the e-mail messages are stored in more than one location (e.g. retained on corporate e-mail server, downloaded to personal computer, and stored on backup tape), different metadata will attach to each unique storage location. Courts have not addressed when this variance in metadata renders the documents identical or not identical, thus leaving open the question of precisely which data to preserve.

The practical effect of these considerations is that due to the complexities in identifying all "key players" and all of the data sources applicable to each "key player", producing parties must implement preservation efforts broadly across an organization to avoid the imposition of sanctions. The greatest risk facing a producing party is that it may learn after-the-fact that a "key player" or data source was excluded from the preservation efforts, thus giving rise to a court's power to sanction for spoliation of evidence (discussed *infra* at p.16).

A. When the Duty to Preserve Arises

Often the most difficult questions for in-house and outside counsel is when the duty to preserve attaches. This "trigger point" will determine when potentially costly and time consuming preservation efforts must be initiated. Counsel that acts too quickly to implement preservation efforts may end up wasting client resources. Conversely, counsel that reacts too slowly may open itself and its client to sanctions for the negligent destruction of evidence. To best serve the interests of clients, counsel must identify with precision when the duty to preserve is triggered. Unfortunately for attorneys and clients alike, no bright line rule exists.

The general rule is that the duty to preserve evidence arises when a party receives notice that the evidence is relevant to litigation or when a party reasonably should have known that the evidence may be relevant to pending, imminent, or reasonably foreseeable litigation. Zubulake IV, 220 F.R.D. at 216; Treppel v. Biovail Corp., 233 F.R.D. 363, 371 (S.D.N.Y. 2006); Easton Sports, Inc. v. Warrior Lacrosse, Inc., 2006 WL 2811261, at *4 (E.D. Mich. 2006); Concord Boat Corp., 1997 WL 33352759, at *4; Shaffer v. RWP Group, Inc., 169 F.R.D. 19, 24 (E.D.N.Y. 1996); Scott v. IBM Corp., 196 F.R.D. 233, 249 (D.N.J. 2000). The duty to preserve commonly arises when a complaint is filed and notice is served, however, the duty to preserve may arise even before a lawsuit is filed if a party is put on notice that litigation is likely to be commenced. Treppel, 233 F.R.D. at 371; Shaffer, 169 F.R.D. at 24.

As a practical matter, the exact moment the duty to preserve arises is not determined until long after a party has notice of litigation. As a threshold matter for determining whether sanctions should be applied for spoliation of evidence, courts look retrospectively at the facts of a case to determine when the duty to preserve actually began to run. This causes great unrest for businesses facing the risk of litigation. What actually constitutes "reasonably foreseeable litigation" is itself a heavily litigated matter. For example, is litigation reasonably foreseeable once an employee

files a personnel complaint? Given the sheer number of employee complaints that may be filed within any given large organization, the company would constantly be under a preservation duty, thus significantly reducing operational efficiencies and revenue generation. Perhaps the duty to preserve is triggered when an employee is terminated, or when an employee utters the exact words "I'm going to sue" or "I was unlawfully discriminated against". But what if the employee merely says "I probably should sue" or "if I had the money I would sue"? The questions are endless and court decisions are unpredictable; there simply is no hard and fast rule counsel can follow. *See* Concord Boat Corp., at *4 (the court found that the duty to preserve relevant e-mail began to run once the complaint was filed); Zubulake IV, 220 F.R.D. at 216-217 (in an employment discrimination and retaliation case where the plaintiff filed an EEOC complaint and was subsequently fired, the plaintiff claimed that the duty to preserve began four months before she filed the EEOC complaint because at this time certain employees titled e-mails pertaining to the plaintiff as "Attorney Client Privilege" and her termination was demanded in an e-mail. The court stated that "merely because one or two employees contemplate the possibility that a fellow employee might sue does not generally impose a firm-wide duty to preserve"; however, the court went on to find that the relevant employees at UBS anticipated litigation even before the EEOC complaint was filed. The court found that the duty to preserve began to run four months before the EEOC complaint, which was six months before the plaintiff's termination and ten months before the complaint was filed.); Treppel, 233 F.R.D. at 371 (the court found that in a case where a former employee alleged the employer of engaging in a "smear campaign" that ruined his career, the duty to preserve was not triggered because of the mere existence of a dispute between the plaintiff and defendant.); Scott v. IBM Corp., 196 F.R.D. at 249 (in an employment discrimination case, the plaintiff employee was laid off but had made previous claims of racial discrimination prior to his termination. The court found that because the defendant employer had "ample notice

that it was discharging a potentially litigious employee" the duty to preserve documents relevant to the layoff began even before the moment of actual termination.).

As demonstrated by these cases, it is difficult for counsel and clients to determine exactly when the duty to preserve arises, and therefore businesses constantly run the risk of destroying potentially relevant evidence while under a duty to preserve. Just as businesses must implement preservation efforts broader than articulated legal standards in order to compensate for the complexities in delineating preservation requirements, businesses must also err on the side of caution with respect to timing the implementation of preservation efforts in order to avoid later being found to have violated the duty to preserve.

B. Preservation Duties of Parties to Litigation

Once the duty to preserve is triggered, a party must suspend its routine document destruction policy and issue a "litigation hold" to ensure the preservation of relevant documents and ESI within the scope of discovery. Zubulake IV, 220 F.R.D. at 218. A proper "litigation hold" entails the identification of all potentially relevant data sources and the implementation of physical and technical data preservation methods. Id. Among the documents and records subject to the "litigation hold" are those generated or maintained by the "key players" in the litigation. Id. The most common method of data preservation involves the creation of one or more snapshot images[7] of potentially relevant evidence at the moment the duty to preserve is triggered, followed by the suspension of backup tape rotation and re-use procedures; the suspension of automated data destruction processes; and the on-going preservation of relevant evidence created after the image is taken. For example, if a party reasonably anticipates that its adversary will request production

---

[7] As a best practice, images should be acquired using specialized forensic software and procedures in order to preserve not only active files but also data contained in deleted files, unallocated space, swap and slack space, and other transient and hidden data sources not viewable by the "naked eye". See *infra* at p. 50.

of relevant e-mail, the party should produce an image of the e-mail server or the mailboxes of all "key players". The image will then be retained for the duration of the litigation and the e-mail server can continue to operate in its normal capacity. Compliance by employees is critical after the snapshots are taken, however, and each "key player" must be responsible for preserving relevant documents and ESI not contained in the snapshot image or captured through an enterprise data backup process.

Courts have held that parties may continue to reuse (and thus overwrite data) backup tapes maintained solely for the purpose of disaster recovery, however, backup tapes that are actively used for information retrieval must be subject to the "litigation hold" and data preservation efforts. Id. If, however, the party can identify the disaster recovery backup tapes that are the single source of particular documents created by or produced for "key players" in the litigation, those backup tapes must also be preserved. Id. The implementation of a "litigation hold" does not, in itself, satisfy the duty to preserve. The party must oversee compliance with the litigation hold by monitoring employees' efforts to retain and produce relevant evidence. Further, due to the fact that the litigation process can take several years, the litigation hold must be periodically re-communicated to the "key players" in the litigation.

C. Preservation Duties of Attorneys

The duty to preserve evidence does not fall solely on the parties to a lawsuit. Legal counsel is responsible for coordinating its clients' preservation and discovery efforts. Zubulake v. UBS Warburg LLC, 229 F.R.D. 422, 435 (S.D.N.Y. 2004) [hereinafter *Zubulake V*]. Although it is clear that both attorneys and clients have certain duties in the preservation of electronic evidence, these responsibilities frequently overlap. Often, the failure of a client to adequately preserve evidence will imply a failure of the attorney to properly oversee the client's preservation efforts. *See* Id. (after finding that employees of the defendant failed to preserve relevant e-mail

after counsel acted reasonably in directing the client to implement a litigation hold, the court stated "... UBS's counsel are not entirely blameless. While, of course, it is true that counsel need not supervise every step of the document production process and may rely upon their clients in some respects, counsel is responsible for coordinating [the] client's discovery efforts").

In *Zubulake V*, the U.S. District Court for the Southern District of New York established standards that counsel must meet in order to comply with preservation duties. First, counsel is required to locate potentially relevant information and issue a "litigation hold" at the outset of litigation. Id. at 432. In order for counsel to locate relevant information, it must first become "fully familiar" with the client's document retention policies and data retention architecture. Id.; Johnson v. Kraft Foods N. Am., Inc., 2006 WL 3302684, at *6 (D. Kan. 2006).

Second, counsel must communicate directly with the "key players" in the litigation to inform them of their duty to preserve relevant documents and ESI. Zubulake V, 229 F.R.D. at 433-434. In order for counsel to identify and locate all potentially relevant data sources, it must interview each "key player" to determine the potential sources of information created by or for each individual. Id. Further, throughout the litigation process counsel must periodically re-issue the "litigation hold", re-inventory all potentially relevant data sources, and remind the "key players" of their preservation duties. Id.

Finally, counsel must oversee the evidence preservation practices of its clients. When the duty to preserve is triggered initially, counsel must instruct all employees to produce electronic copies of relevant documents and records within their possession or control and counsel must ensure that all backup tapes subject to discovery are identified and stored in a safe place. Id. at 434. As counsel is "more conscious of the contours of the preservation obligation" that its client, the active supervision of counsel is required throughout the preservation and discovery process in order to ensure the client's compliance with preservation obligations. Id. at 433.

D. **Sanctions for the Spoliation of Evidence**

Spoliation refers to the destruction or material alteration of evidence or the failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation. Zubulake IV, 220 F.R.D. at 216. The failure to preserve evidence, once the duty to preserve has been triggered, raises issues of spoliation and the appropriate sanction, if any, for spoliation. In order to penalize the producing party for violation of the duty to preserve and to restore the requesting party to the position it would likely have been in, had the evidence been preserved and made available for inspection, courts routinely impose sanctions for spoliation of evidence. A party can only be sanctioned for the destruction of evidence if it was under a duty to preserve at the time of destruction. Id. Further, most courts will only impose sanctions upon motion by the requesting party and only if the requesting party makes a *prima facie* showing of actual harm or prejudice resulting from the spoliation. Id.

Courts have applied a broad range of sanctions for the spoliation of evidence, ranging from minor "slap on the wrist" type monetary penalties to case-determinative remedies. *See* Ball v. Versar, Inc., 2005 WL 4881102, at *5 (S.D. Ind. 2005) (the court awarded costs and fees to the plaintiff after determining that the defendant withheld discoverable information and potentially failed to preserve such information); Zubulake IV, 220 F.R.D. at 222 (the court ordered the defendant to pay the plaintiff's costs for re-deposing certain witnesses in order to gain additional information regarding the alleged destruction of evidence); Zubulake V, 229 F.R.D. at 439-440 (court granted plaintiff's motion for sanctions and ordered that an adverse inference jury instruction be given, which permitted the jury to presume that the evidence destroyed by the defendant would have been unfavorable to the defendant's position.); MasterCard Int'l., Inc. v. Mouton, 2004 WL 1393992, at *5 (S.D.N.Y. 2004) (the court refused to issue an adverse inference instruction to the jury but permitted the plaintiff to argue to the trier of fact that the

destruction of evidence warranted an inference in support of plaintiff's case); Mosaid Techs., Inc. v. Samsung Elecs. Co., LTD., 348 F.Supp.2d 332, 339-340 (D.N.J. 2004) (after the defendant failed to issue a "litigation hold" and allowed its usual e-mail destruction practices to continue after the duty to preserve was triggered, the court concluded that the imposition of an adverse jury inference and the award of monetary sanctions was a reasonable penalty); Arista Records, L.L.C. v. Tschirhart, 2006 WL 2728927, at *3-4 (W.D. Tex. 2006) (in finding that the defendant used "wiping" software to permanently erase data and then attempted to hide the use of such "wiping" software by deleting it from the computer system, the court ruled that a default judgment against the defendant was an appropriate sanction because the defendant showed "blatant contempt" for the court and a "fundamental disregard for the judicial process". In addition to the default judgment order, the court awarded costs and fees to the plaintiff.)

Courts are split as to whether the imposition of sanctions is a question of state law or federal law. The Sixth Circuit has held that the rules that apply to spoliation of evidence and the imposition of sanctions are defined by state law (*See* Easton Sports, Inc., at *4), whereas the District of Georgia has held that federal law governs the right to impose sanctions for spoliation because the issue involves an evidentiary matter (*See* Frey v. Gainey Transp. Servs., Inc., 2006 WL 2443787, at *7 (N.D. Ga. 2006). The majority rule appears to be that the right to impose sanctions for spoliation arises jointly under Rule 37 and from a court's inherent power to control the judicial process and litigation. Fujitsu Ltd., 247 F.3d at 436; Zubulake IV, 220 F.R.D. at 216; Thompson v. U.S. Dep't. of Housing and Urban Dev. (HUD), 219 F.R.D. 93, 100 (D. Md. 2003); Banco Latino, S.A.C.A. v. Gomez Lopez, 53 F.Supp.2d 1273, 1277 (S.D. Fla. 1999). Regardless of whether the power to sanction is conferred by state or federal law, the determination of an appropriate sanction for spoliation, if any, is confined to the "sound discretion of the trial judge" and is assessed on a "case-by-case basis". Fujitsu Ltd., 247 F.3d at 436. Courts have consistently

held that a sanction may be imposed regardless of whether the spoliation was the result of an intentional act or the result of negligence; however the severity of the sanction may vary based upon level of culpability. Zubulake IV, 220 F.R.D. at 220; Easton Sports, Inc., at *5.

1. Application of Sanctions Based on the Level of a Party's Culpability

Spoliation of evidence can occur as the result of negligent, grossly negligent, or intentional bad faith conduct. Thompson v. HUD, 219 F.R.D. at 101. The most severe sanctions must be reserved for the most culpable, bad faith conduct. Dismissal of a case or the imposition of a default judgment are clearly the most severe sanctions; they strike directly at the heart of a plaintiff's ability to recover. It is rare for a court to dismiss a case or enter a default judgment as a sanction for spoliation of evidence. Courts generally require that at least three elements must be established in order to dismiss a case or enter a default judgment: (1) bad faith (intentional or willful) destruction of evidence; (2) substantial prejudice to the opposing party; and (3) a finding that a less severe sanction would not avoid substantial unfairness to the opposing party. Mosaid Techs., Inc., 348 F.Supp.2d at 335; Arista Records, L.L.C., *2; Computer Assocs. Int'l., Inc. v. Am. Fundware, Inc., 133 F.R.D. 166, 169 (D. Colo. 1990).

Requesting parties more commonly move for an adverse inference jury instruction and courts have applied this sanction more liberally than dismissal or default judgment. As discussed in *Zubulake IV*, however, the practical effect of an adverse inference jury instruction is likely to be just as case determinative as dismissal or default judgment ("in practice, an adverse inference instruction often ends litigation – it is too difficult a hurdle for the spoliator to overcome. The *in terrorem* effect of an adverse inference is obvious"). Zubulake IV, 220 F.R.D. at 219. In *Zubulake V*, the jury found in favor of the plaintiff after the court gave the following instruction:

> You have heard that UBS failed to produce some of the emails sent or received by UBS personnel . . . Plaintiff has argued that this evidence was in defendant's control and would have proven facts material to the matter in controversy.

> If you find that UBS should have produced this evidence, and that the evidence was within its control, and that the evidence would have been material in deciding facts in dispute in this case, you are permitted but not required, to infer that the evidence would have been unfavorable to UBS.
>
> In deciding whether to draw this inference, you should consider whether the evidence not produced would merely have duplicated other evidence already before you. You may also consider whether you are satisfied that UBS's failure to produce this information was reasonable. Again, any inference that you decide to draw should be based on all the facts and circumstances in this case.

Courts have applied different standards for the imposition of adverse inference instructions. The U.S. District Court for the Southern District of New York requires a party seeking an adverse inference instruction to establish the following three elements: (1) that the party having control over the evidence had an obligation to preserve it at the time it was destroyed; (2) that the records were destroyed with a "culpable state of mind"; and (3) that the destroyed evidence was "relevant", such that a reasonable trier of fact could find that the evidence would support the moving party's claim or defense. Zubulake IV, 220 F.R.D. at 220. In the Second Circuit, a "culpable state of mind" includes ordinary negligence. Residential Funding Corp. v. DeGeorge Fin. Corp., 306 F.3d 99, 108 (2d Cir. 2002). Further, relevance is presumed when evidence is destroyed as the result of intentional or willful conduct, thus leaving the moving party only to show that its adversary was under a duty to preserve. Zubulake IV, 220 F.R.D. at 220. If destruction occurs through a party's negligence, however, relevance must be proven by the party seeking the sanction. Id.

The U.S. District Court for New Jersey takes a different view. In New Jersey, an adverse inference instruction is seen as a "far lesser sanction" than dismissal of a case or suppression of evidence. Mosaid Techs., Inc., 348 F.Supp.2d at 335. The standard for applying an adverse inference instruction is similar to that articulated in *Zubulake IV*, however, in practice the New Jersey rule is more stringent as it requires the moving party to show four elements: (1) that the

evidence in question was within the party's control; (2) that there was "actual suppression or withholding" of evidence; (3) that the evidence destroyed or withheld was relevant to a party's claim or defense; and (4) that it was reasonably foreseeable that the evidence would be requested in discovery. On at least one occasion the New Jersey District court has construed "actual suppression" to mean "intentional destruction". Scott v. IBM Corp., 196 F.R.D. at 248. Recent decisions, however, hold that unlike *Zubulake IV* the spoliator's culpability is irrelevant with respect to the imposition of an adverse inference instruction, whereas culpability is a consideration in the application of more severe sanctions (e.g. dismissal) in New Jersey. Mosaid Techs., Inc., 348 F.Supp.2d at 337-3338. It can be argued that culpability is also largely irrelevant in the Southern District of New York's application of adverse inference instructions, thus making no practical distinction between the two jurisdictions as to this element. Both District Courts impose an adverse inference instruction for negligent or intentional conduct and neither District will impose a sanction without finding at least negligence; there does not appear to be any strict liability standard, even in a jurisdiction where state of mind is irrelevant.

Given the same practical effect of both standards, New Jersey, which deems an adverse inference instruction less severe than the Southern District of New York, imposes a greater burden on the moving party because it must be shown that evidence was actually suppressed or withheld. This can be difficult for the requesting party to prove. If, for example, the requesting party does not receive as many e-mail messages as expected through discovery, the question raised is whether the e-mail messages were not disclosed because they were destroyed or because they never existed to begin with. The simple fact is that the evidence demanded has not been produced. The burden is placed upon the party alleging spoliation to show the evidence did exist at one time, and that it was actually suppressed or withheld. The producing party, of course, will argue that the evidence never existed and that it has superior knowledge of its information systems

and data. In order to prove spoliation the requesting party must either obtain testimony from the adverse party or conduct extensive forensic analysis of the adversary's computer systems to discover evidence of data destruction or concealment practices.

The same argument in both jurisdictions may very well lead the imposition of an adverse inference in the Southern District of New York but not in New Jersey. If, for example, a requesting party alleges spoliation because the producing party negligently failed to suspend its automated e-mail deletion process after the duty to preserve was triggered, and the likely result of this negligence was the destruction of relevant evidence, all of the elements are made out under the *Zubulake IV* rule. There is no doubt that the spoliator had exclusive control of the e-mail; that some e-mail messages were deleted; and that the spoliator was negligent. All the requesting party would need to show is that the deleted e-mail messages were *potentially* relevant to any of its claims or defenses. The same result may not be reached in New Jersey, as it will be difficult to show relevant e-mail *did* exist and was *actually* suppressed as a result of the e-mail deletion. Although the Southern District of New York gives deep consideration to the practical effect of an adverse inference instruction, especially compared to New Jersey's view, it is easier for the moving party to obtain this sanction in the Southern District of New York.

Other jurisdictions take an even more rigid approach to determining when an adverse inference instruction is appropriate as a sanction for spoliation. Many courts will only grant an adverse inference instruction if it is shown that evidence was destroyed in bad faith, either intentionally or willfully. Crandall v. The City and County of Denver, Colorado, 2006 WL 2683754, at *2 (D. Colo. 2006); Concord Boat Corp., at *6; State of Iowa v. Hartsfield, 681 N.W.2d 626, 629-630 (Iowa 2004); Banco Latino, 53 F.Supp.2d at 1277. Unlike the Southern District of New York and New Jersey, mere negligence in losing or destroying evidence does not warrant an inference that the evidence would have been detrimental to the spoliator's case.

2. Sanctions Under Amended Rule 37 (The "Safe Harbor" Rule)

Amended Rule 37 states that a court may not impose sanctions *under the Federal Rules of Civil Procedure* for the loss or destruction of ESI, provided that the loss or destruction was the result of the "routine, good-faith operation of an electronic information system". Fed. R. Civ. P. 37(f). Rule 37 does not prevent a court from imposing sanctions based upon other sources of authority, such as a court's inherent power to control the judicial process and litigation or spoliation sanctions arising under state law.

Rule 37 was amended to allow for the routine alteration and deletion of information that occurs as part of the normal operation of computer systems, with or without some level of user direction or awareness. Advisory Committee Notes to Fed. R. Civ. P. 37. This rule does not permit a party to escape its preservation duties or thwart its discovery obligations. One factor to consider in determining whether a party acted in "good faith" is whether the party implemented a "litigation hold" once the duty to preserve was trigged, and, whether pursuant to the "litigation hold" the party intervened in routine operations to modify or suspend functions and practices that could potentially destroy or modify relevant evidence. Id.

The so-called "safe harbor" provision of Rule 37 does little to change how sanctions will be applied by federal courts. First, even if evidence is lost due to the "good faith" operation of an information system, courts retain the power to sanction under authority other than the Rules, such as state law or the court's inherent ability to control the litigation process. Second, nearly every jurisdiction sanctions only negligent, grossly negligent, or bad faith spoliation. The requirement to suspend data modification and deletion practices pursuant to a "litigation hold" in order to fall under the "good faith" protection of Rule 37 means that the party must exercise due care. So long as a party exercises due care to safeguard evidence once the duty to preserve arises, the party would not ordinarily be subject to sanctions for spoliation absent Rule 37.

E. Use of Preservation Orders to Compel Preservation of ESI

Amended Rule 26 requires parities to discuss preservation issues at the 26(f) conference. The Advisory Committee was careful to note that this requirement does not imply that courts should routinely enter preservation orders. Advisory Committee Notes to Fed. R. Civ. P. 26(f). The Committee gave further guidance, stating that "a preservation order entered over objections should be narrowly tailored" and that "ex parte preservation orders should be issued only in exceptional circumstances". Id. In some circumstances a preservation order may actually benefit the producing party, however, as the court order will specifically outline the producing party's preservation duties, thus eliminating any uncertainly as to preservation requirements and spoliation sanctions.

Some courts have adopted a three-prong balancing test to determine under what circumstances a preservation order should be issued. Under this test, the court must consider the following three factors: (1) the danger of evidence destruction or loss of integrity absent a preservation order; (2) whether any irreparable harm is likely to result to the party seeking preservation of evidence absent a preservation order; and (3) the producing party's capability to preserve the evidence in its original form, considering the physical, spatial, and financial burdens created by issuing a preservation order. Capricorn Power Co., Inc. v. Siemens Westinghouse Power Corp., 220 F.R.D. 429, 433-434 (W.D. Pa. 2004); Treppel, 233 F.R.D. at 370. Other courts have held that a party seeking a preservation order must demonstrate only that the order is "necessary and not unduly burdensome". Pueblo of Laguna v. U.S., 60 Fed.Cl. 133, 136 (2004). In practice both tests place the same burden upon the party moving for a preservation order. The first two factors of the *Capricorn* test are the means through which a moving party would demonstrate whether the order is "necessary", while the third factor goes directly to whether the order would be "unduly burdensome".

III. THE SCOPE OF ELECTRONIC DISCOVERY

Generally, a party is entitled to obtain discovery of all relevant, non-privileged documents and ESI from other parties to a lawsuit, as well as from non-parties through service of a subpoena. Fed. R. Civ. P. 26(a)(1)(B), (b)(1); Fed. R. Civ. P. 45(d). Prior to the inclusion of ESI in the Rules, courts had required the production of both actively stored and deleted electronic documents. *See* Antioch Co. v. Scrapbook Borders, Inc., 210 F.R.D. 645, 652 (D. Minn. 2002) ("It is a well accepted proposition that deleted computer files, whether they be e-mails or otherwise, are discoverable"); Simon Property Group L.P. v. mySimon, Inc., 194 F.R.D. 639, 640 (S.D. Ind. 2000) ("computer records including records that have been deleted are documents discoverable under Rule 34"); Kliener v. Burns, 2000 WL 1909470 (D. Kan. 2000) ("Rule 26(a)(1)(B) requires the disclosing party to take reasonable steps to ensure that it discloses any backup copies of files or archival tapes that will provide information about any "deleted" electronic data"); Delta Fin. Corp. v. Morrison, 819 N.Y.S.2d at 912 (discovery is permissible for electronic documents currently in use, but also for documents that may have been deleted and reside only on backup tapes.) Further, requests for the discovery of electronic information that employ search terms of the e-mails and documents of key personnel have been found to be permissible. Treppel, 233 F.R.D. at 374; Kormendi v. Computer Assocs. Int'l, Inc., 2002 WL 31385832, at *7 (S.D.N.Y. 2002).

Under Rule 26 a court may limit discovery if it determines that a request is "unreasonably cumulative or duplicative, or is obtainable from some other source that is more convenient, less burdensome, or less expensive". Fed. R. Civ. P. 26(b)(2)(C). In applying this rule to the discovery of electronic documents or files, courts have been cognizant of and sympathetic to the associated expenses. *See* Zubulake v. UBS Warburg LLC, 217 F.R.D. 309, 316 (S.D.N.Y. 2003) [hereinafter *Zubulake I*] (broad scope of discovery encompassed in FRCP 26(b)(1) must be

balanced with Rule's "cost-consciousness"); Rowe Entm't., Inc., 205 F.R.D. at 423 ("too often, discovery is not just about uncovering the truth, but also about how much of the truth the parties can afford to disinter . . . discovery expenses frequently escalate when information is stored in electronic form").

A. Accessible Versus Inaccessible Data Sources

A party is not required to provide discovery of ESI from sources that the party identifies as "not reasonably accessible" because of undue burden or cost. Fed. R. Civ. P. 26(b)(2)(B). Accessible data sources typically include information systems and media from which information is retrieved and used in the normal course of business, such as server and personal computer hard drives; production-use databases; e-mail archives; and removable media readily available for use. Inaccessible data sources include electronic media retained for limited-use purposes, such as backup tapes kept solely for disaster recovery, which are not readily available or routinely used for data retrieval or use, as well as deleted, erased, corrupted, damaged, or fragmented data. In practice, data sources do not always fit neatly within the categorical designations of reasonably accessible and not reasonably accessible; the degree of accessibility flows along a continuum. For example, the greater the need to employ specialized software to access information within a particular data source (e.g. legacy systems or proprietary databases), the more inaccessible the data source is considered. Courts, therefore, must determine what constitutes an inaccessible data source. Accessible data that is relevant and non-privileged is always subject to discovery. Inaccessible data sources are not generally subject to discovery due to the burden and expense associated with the retrieval and restoration of data from these sources, unless upon motion a court finds that discovery is warranted based upon the proportionality test articulated in Rule 26(b)(2)(C).

On motion to compel discovery or for a protective order, the producing party has burden of proof to show that the requested ESI is not reasonably accessible because of undue burden or expense. Advisory Committee Notes to Fed. R. Civ. P. 26. If a *prima facie* showing is made, the burden shifts to the requesting party to show that its need for discovery outweighs the burdens and costs of locating, retrieving, and producing the information. Id. The requesting party may not know what information the data sources contain, however, so parties may need to conduct focused discovery to sample the data sources and learn more about the burdens and costs, what the information consists of, and how valuable the information is to the litigation.

Even if a producing party is able to show that the requested ESI is not reasonably accessible because of undue burden or expense, a court may nonetheless order discovery for "good cause", after consideration of limitations in Rule 26(b)(2)(C), which provides that discovery shall be limited if: (1) the discovery request is unreasonably cumulative or duplicative, or is obtainable from some other source that is more convenient, less burdensome, or less expensive; (2) the requesting party has had ample opportunity by discovery in the action to obtain the information sought; or (3) the burden or expense of the proposed discovery outweighs its likely benefit, taking into account the:

1. Needs of the case;
2. Amount in controversy;
3. Parties' resources;
4. Importance of the issues at stake in the litigation; and
5. Importance of the proposed discovery in resolving the issues.

In addition to the limitations imposed by Rule 26, in determining whether to order discovery of information designated as "not reasonably accessible" by the producing party, a court should consider the following factors enumerated in the Advisory Committee Notes to determine if "good cause" exists: (1) the specificity of the discovery request; (2) the quantity of information available from other and more easily accessed sources; (3) the failure to produce relevant

information that seems likely to have existed but is no longer available on more easily accessed sources; (4) the likelihood of finding relevant, responsive information that cannot be obtained from other, more easily accessed sources; (5) predictions as to the importance and usefulness of the further information; (6) the importance of the issues at stake in the litigation; and (7) the parties' resources. *See* Advisory Committee Notes to Fed. R. Civ. P. 26.

The use of a two-tiered approach in the production of ESI may be achieve a fair balance between the competing interests of producing and requesting parties in litigation. The parties should agree at or before the Rule 26(f) conference that relevant, non-privileged information will be produced from accessible data sources first (tier-one production). The requesting party should demand production from inaccessible data sources (tier-two production) *only if* the tier-one production does not satisfy its discovery needs. This two-tiered approach may enable the parties to avoid costly motion practice related to production from data sources not reasonably accessible. Further, if the requesting party reasonably believes that production from inaccessible sources is required, a sampling procedure may be used to form a basis for application of the Rule 26(b)(2)(C) proportionality test, which will enable courts to make better informed decisions regarding the compelled production of sources deemed not reasonably accessible (and in some cases may enable the parties to form an agreement without court intervention). Under the sampling procedure, the parties should conduct targeted discovery of a limited number of inaccessible data sources to determine (i) the likelihood that relevant information exists and (ii) the projected costs associated with complete discovery of the inaccessible sources.

B. Discovery Demands Found to be Overly Broad

Reasonably tailored requests help to ensure that the requesting party will receive the most pertinent information, but will also establish positive rapport with the court and pre-empt challenges by the producing party. Further, courts will be more likely to support future discovery

requests if it does not perceive the use of abusive "fishing expedition" tactics. In a case where customers of the Jiffy Lube franchise sued for violation of consumer protection laws, the plaintiffs requested production of "any and all information related to e-mail ... including messages". Thompson v. Jiffy Lube Int'l., Inc., 2006 WL 1174040, at *3 (D. Kan. 2006). The court rejected the plaintiff's request for the "wholesale production of all e-mail messages" as overly broad, finding that requests for the production of ESI must be "reasonably tailored" to ensure the production of information relevant to a party's claim or defense. Id. Further, Rule 34(a) requires requests for the production of documents or ESI to describe each item with "reasonable particularity". Fed. R. Civ. P. 34(b).

Similarly, in a case involving African-American concert promoters' claims of discriminatory and anti-competitive practices in the promotion of events for music groups with white members, the court characterized the following requests as "sweeping": (i) "all documents [including e-mails] concerning any communication between any defendants relating to the selection of concert promoters and bids to promote concerts"; and (ii) "all documents [including e-mails] concerning market shares, market share values, market conditions, or geographic boundaries in which any concert promoter operates." Rowe Entm't., Inc., 205 F.R.D. at 424. The plaintiffs subsequently limited the scope of their requests through date restrictions and sampling of e-mails of key personnel and were able to compel the production of e-mails. Id.

A request that a responding party "dump" their computer data (i.e. produce back-up tapes in their entirety) was found to be impermissibly overbroad as it would include "data not requested or relevant." Anti-Monopoly, Inc. v. Hasbro, Inc., 1996 WL 22976, at *2 (S.D.N.Y. 1996) (denying plaintiff's motion to compel). Requests for entire storage devices, such as hard disk drives and entire databases, as opposed to specific categories of documents, have been found to be overly broad. *See In re* Grand Jury Subpoena Duces Tecum, 846 F.Supp. 11, 13-14 (S.D.N.Y.

1994) (quashing grand jury subpoena because it sought documents irrelevant to grand jury inquiry); Jones v. Goord, 2002 U.S.Dist. LEXIS 8707, at *20 (S.D.N.Y. 2002) (denying motion to compel production of entire computerized databases where, *inter alia*, not all information contained in the requested databases was relevant to issues involved in the litigation); Quinby v. WestLB AG, 2006 WL 2597900, at *3-4 (S.D.N.Y. 2006) (order granting motion to quash two subpoenas seeking "all e-mails sent to or received by plaintiff's personal e-mail account during the period from October 2002 throughout July 2004, other than e-mails between plaintiff and her current and former counsel"). *See also* Weiller v. New York Life Ins. Co., 800 N.Y.S.2d 359 (Sup. Ct. N.Y. Cty. 2005) (finding permissible the request for specific categories of documents contained in "all databases, electronic material, tape media, electronic media, hard drives, computer disks and documents").

C. Right to Examine an Adversary's Information Systems

While the general rule is that the producing party will make reasonable efforts to comply with discovery requests, a "seed of doubt" is usually present in the requesting party's mind. Legally the producing party is required to disclose all relevant, non-privileged information, however adverse the information may be to its own claims or defenses. The only controls to enforce this obligation are spoliation sanctions and possible criminal penalties, both of which hinge upon detection of evidence tampering or destruction. The trouble with electronic evidence, at least from the requesting party's perspective, is that it can be so easily manipulated or destroyed without detection. The requesting party often seeks assurance that the producing party has captured and disclosed all available information and that the information produced is authentic and original. The best method for the requesting party to obtain this assurance is to examine the ESI itself by gaining direct access to the producing party's information systems. Direct access to an information system allows the requesting party to capture all relevant, non-privileged

information, including deleted files and traces of data manipulation and destruction. The burden and risk to the producing party is obvious; it would need to make available its information systems for inspection and risk disclosure of confidential information. By permitting direct access to information systems, courts have the power to create an incentive for producing parties to demonstrate full compliance with discovery obligations, in order to preempt demands for direct access.

Amended Rule 34 permits parties to request to "inspect, copy, test, or sample" documents and ESI. Fed. R. Civ. P. 34(a). The prior version of Rule 34 only permitted requesting parties to "inspect and copy" documents. On its face, Rule 34 appears to provide requesting parties an opportunity to gain direct access to an adversary's information systems in order to inspect, copy, test, or sample ESI, however the Advisory Committee Notes caution that Rule 34 is not meant to create a "routine right of direct access" to the responding party's information systems. Advisory Committee Notes to Fed. R. Civ. P. 34. The Committee further states that such direct access "might be justified in some circumstances", but that courts should guard against "undue intrusiveness". Id. This leaves courts to determine, in their discretion, what constitutes "undue intrusiveness" and what circumstances justify the issuance of an order granting a party direct access to its adversary's information systems.

Prior to the amendment of Rule 34 courts have tackled the issue of whether a party is entitled to gain direct access to an adversary's information systems. Several courts have permitted the requesting party, or an expert employed by the requesting party, to gain direct access to the producing party's systems. *See* Playboy Enters., Inc., 60 F.Supp.2d at 1054 (the court ordered the defendant to make her computer hard drive available for forensic examination by a third party expert employed by the plaintiff); Antioch Co., 210 F.R.D. at 653 (the court ordered the defendant to make its systems available for copying by a forensic expert employed by the plaintiff, even

before the court's scheduling order had been issued.); Simon Property Group, 194 F.R.D. at 641 (the court permitted a third party expert hired by the plaintiff to conduct forensic examination of the defendant's computer system); Tilberg v. Next Mgmt. Co., 2005 WL 2759860, at *3. (S.D.N.Y. 2005) (finding that defendants "either inadvertently or deliberately delayed and obstructed discovery in this case", the court ordered the defendants to provide the plaintiff's expert with access to their computer systems, including defendants' "central server".)

Other courts have devised rigid standards that requesting parties must meet in order to be granted direct access to the opposing party's systems. *See* Powers v. Thomas M. Cooley Law Sch., 2006 WL 2711512, at *4-5 (W.D. Mich. 2006) (in a motion for reconsideration, the plaintiff requested forensic examination of a law school's computer system in order to discover evidence allegedly withheld by the defendant. The court relied upon the proportionality test articulated in Rule 26(b)(2) to weigh the costs and burdens of the forensic examination. In denying plaintiff's motion, the court stated that it was "loathe to sanction intrusive examination of computer as a matter of course, or on the mere suspicion that the opponent may be withholding discoverable information".); *In re* Ford Motor Co., 345 F.3d 1315, 1317 (11th Cir. 2003) (the Court of Appeals for the 11th Circuit granted mandamus and vacated the trial court's order granting the plaintiff "unlimited, direct access" to the defendant's computer systems. The court found that the trial court erred by granting broad direct access without establishing any protocols for the search. The 11th Circuit left the door open on the issue of direct access, however, by stating that in certain cases a requesting party may need direct access to conduct its own search "due to improper conduct" of the producing party. The court further articulated that a requesting party is not entitled to direct access without a factual finding of the producing party's non-compliance with discovery rules."); Bethea v. Comcast, 218 F.R.D. 328, 330 (D.D.C. 2003) (in rejecting the plaintiff's motion to compel inspection of defendant's computer systems, the court ruled that the

"mere conjecture" that another party has failed to respond to document requests fully and completely does not justify compelled inspection of its computer systems. In order for the court to grant such a motion, the requesting party would need to show that (1) the information sought through direct access is relevant to the pending litigation; (2) the information sought actually exists or that the producing party unlawfully failed to produce it; and (3) the producing party's discovery efforts were inadequate in scope or duration."). It is expected that these standards will continue to be applicable to the testing and sampling of ESI under the amended Rule 34.

IV. ALLOCATION OF COSTS

Under the FRCP, the presumption is that the producing party bears the costs complying with permissible discovery requests. Oppenheimer Fund, Inc. v. Sanders, 437 U.S. 340, 358 (1978). Federal courts have discretionary power under Rule 26(c) to protect the producing party against "undue burden or expense" by ordering the requesting party to pay part or all of the costs of production. Id.; Rowe Entm't., Inc., 205 F.R.D. at 429. Understanding that electronic discovery is expensive and time consuming, courts have been cognizant of using cost shifting orders to balance the scope of discovery under Rule 26(b)(1) with the cost considerations of Rule 26(b)(2). Under Rule 26(c), such an order may be granted only upon the motion of the responding party and for "good cause shown". Further, cost shifting should be considered only when discovery imposes an "undue burden or expense" on the producing party; the issue of cost shifting does not arise merely because ESI is requested. Zubulake I, 217 F.R.D. at 317. Typically, the issue of cost shifting is raised when the requesting party demands that information be produced from data sources that the producing party deems not reasonably accessible. As discussed *supra* at p.26, the producing party is generally not required to disclose ESI that is not reasonably accessible, however, upon motion to compel the court may order discovery of any information. In

response to a court's order that information be produced from inaccessible sources, the producing party typically will file a motion for cost shifting. The producing party has the burden of proof on a motion for cost-shifting. Zubulake v. UBS Warburg LLC, 216 F.R.D. 280, 283 (S.D.N.Y. 2003) [hereinafter *Zubulake III*]; Wiginton v. CB Richard Ellis, Inc., 229 F.R.D. 568, 572 (N.D. Ill. 2004). Proof is commonly established by obtaining an affidavit from an electronic discovery expert stating the estimated costs of restoration, processing, and production.

Under the FRCP electronic discovery imposes an "undue burden or expense" when it outweighs its likely benefit, taking into account the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the litigation, and the importance of the proposed discovery in resolving the issues. Fed. R. Civ. P. 26(b)(2)(B). Some courts have relied upon this language alone in considering whether to order the requesting party to share in the costs of electronic discovery. Thompson v. HUD, 219 F.R.D. at 98; Anti-Monopoly, Inc., at *1. Other courts have described the Rule 26 approach as "crude" and have addressed the issue of cost shifting by devising common law tests for determining whether a cost-shifting order is appropriate. Zubulake I, 217 F.R.D. at 317.

A. Court-Devised Protocols for the Allocation of Discovery Costs

Courts have expounded upon the Rule 26 approach to develop a standardized framework for the allocation of costs. *See* McPeek v. Ashcroft, 202 F.R.D. 31, 34 (D.D.C. 2001) (the court adopted the economic principle of "marginal utility" as a basis for consideration of cost shifting. Under this approach the court considered not only the costs of the requested discovery but also how likely it would be that the discovery request yields relevant evidence. If the requested discovery were likely to yield critical evidence, the fairer it would be for the producing party to bear the costs of production); Rowe Entm't., Inc., 205 F.R.D. at 429 (Judge Francis employed the "marginal utility" approach to devise an eight factor test to determine whether discovery costs

should be shifted); Zubulake I, 217 F.R.D. at 321-22 (Judge Schindlen cited the *Rowe* test as the "gold standard" yet criticized the eight factor test for its tendency to favor cost shifting. In fact, in the time between *Rowe* and *Zubulake I*, all of the courts that applied the *Rowe* test ordered cost shifting. In the most influential response to the issue of cost-shifting, Judge Schindlen modified the *Rowe* test to emphasize "the extent to which the request is specifically tailored to discover relevant information and the availability of such information from other sources"); Wiginton, 229 F.R.D. at 573 (the court criticized the *Rowe* and *Zubulake* tests as not being sufficiently guided by Rule 26(b)(2)(C) and created an eight factor test that amalgamated *Rowe* and *Zubulake I* and added a new factor for consideration).

The *Rowe* 8-factor test considers the following equally-weighted factors in determining whether to shift part or all of the production costs to the requesting party:

1. the specificity of the discovery requests;
2. the likelihood of discovering critical information;
3. the availability of such information from other sources;
4. the purposes for which the responding party maintains the requested data;
5. the relative benefit to the parties of obtaining the information;
6. the total cost associated with production;
7. the relative ability of each party to control costs and its incentive to do so; and
8. the resources available to each party.

In *Rowe* the court applied the eight factor test and concluded that the requesting party would bear the costs of production. In doing so, the court specifically recognized that backup tapes "are not archives from which documents may easily be retrieved. The data on a backup tape are not organized for retrieval of individual documents or files, but for wholesale, emergency uploading onto a computer system." Rowe Entm't., Inc., 205 F.R.D. at 429. Under the language of the amended Rule 26, the court would have found that the requested information was not "reasonably accessible", thus prompting consideration of cost shifting.

In contrast to the *Rowe* test, the *Zubulake I* seven factor test conflates factors one and two, and denounces the practice of treating each factor as equally weighted. *See* Zubulake I, 217 F.R.D. at 322-23. Factors one and two of the Zubulake test comprise the "marginal utility" test established in *McPeek*. The seven factors, in descending order of importance, are:

1. the extent to which the request is specifically tailored to discover relevant information;
2. the availability of such information from other sources;
3. the total cost of production, compared to the amount in controversy;
4. the total cost of production, compared to the resources available to each party;
5. the relative ability of each party to control costs and its incentive to do so;
6. the importance of the issues at stake in the litigation; and
7. the relative benefits to the parties of obtaining the information.

In Zubulake III the court ordered the requesting party to pay for twenty-five percent (25%) of the cost of restoring the requested backup tapes. 216 F.R.D. at 280, 291. The court concluded that the proportion of costs between the requesting and producing parties was appropriate because the "success of the search is somewhat speculative", but cost allocation at a higher percentage "may chill the rights of litigants to pursue meritorious claims". Id. at 289. The court ordered cost shifting only after the producing party was ordered to bear the costs of producing and restoring a sample of five backup tapes, from which the court measured the relevancy of data contained on the requested backup tapes. In fact, many courts follow this type of "sampling" approach to determine the potential relevancy of the requested discovery prior to ordering discovery and cost allocation of the entire media. *See e.g.*, *In re* Natural Gas Commodity Litig., 235 F.R.D. 199, 220 (S.D.N.Y. 2005); J.C. Associates v. Fid. & Guar. Ins. Co., 2006 WL 1445173, at *1-2 (D.D.C. 2006).

The court in Wiginton in turn modified the *Rowe* and *Zubulake I* tests by combining the two and adding one additional factor that considers the importance of the requested discovery in

resolving the issues of the litigation, however, the majority of courts today continue to follow the *Zubulake I* approach. 235 F.R.D. at 573. The Wiginton eight factor test considers:

1. the likelihood of discovering critical information;
2. the availability of such information from other sources;
3. the amount in controversy as compared to the total cost of production;
4. the relative ability of each party to control costs and its incentive to do so;
5. the importance of the requested discovery in resolving the issues at stake in the litigation;
6. the importance of the issues at stake in the litigation;
7. the importance of the requested discovery in resolving the issues at stake in the litigation; and
8. the relative benefits to the parties of obtaining the information.

Where a court has ordered cost shifting, only the costs of restoration, processing, and searching should be shifted, in whole or in part, to the requesting party. Zubulake III, 216 F.R.D. at 291; Rowe Entm't., Inc., 205 F.R.D. at 432. The producing party must always bear the costs of production and for conducting a privilege review (*see infra* at p.44), if it so desires, prior to production. Rowe Entm't., Inc., 205 F.R.D. at 432; Zubulake III, 216 F.R.D. at 291. The rationale for this rule is that the producing party unilaterally defines the review protocol and controls the costs of the privilege review. Id. Further, the objective of cost shifting is to compensate the producing party for having to render inaccessible data accessible; once the data is converted to an accessible form the usual rules of discovery apply. *See* Id. (the court draws an analogy between data stored in inaccessible sources and paper records stored in a safe, stating "in some cases the parties should split the cost of breaking into the safe. But once the safe is opened, the production of the documents found inside is the sole responsibility of the responding party."). Several courts have cited the *Rowe* and *Zubulake* decisions as an appropriate basis for distributing costs. *See e.g.*, Gambale v. Deutsche Bank AG, 2002 U.S.Dist. LEXIS 22931, at *2 (S.D.N.Y. 2002); *In re* Livent, Inc. Noteholders Secs. Litig., 2002 U.S.Dist. LEXIS 26446, at *9 (S.D.N.Y. 2002) (citing *Rowe* with approval); Medtronic Sofamor Danek, Inc. v. Michelson, 229 F.R.D. 550,

553-554 (W.D. Tenn. 2003) (court followed the *Rowe* eight factor test and required the producing party to bear the costs of the privilege review and production); Murphy Oil USA, Inc. v. Fluor Daniel, Inc., 2002 WL 246439, at *4-6 (E.D. La. 2002) (citing *Rowe* holding that defendant shall bear the cost if it chooses to review the requested e-mails prior to production).

In Quinby the defendant moved to compel plaintiff to bear a portion of the costs for restoring and searching the requested backup tapes and other data sources not reasonably accessible. The plaintiff argued the costs should not be shifted since the defendant had a duty to preserve the requested e-mails in an accessible format. Id. at *27. In response, the defendant argued that it had a duty only to preserve the evidence; it had no duty to preserve the data in a particular format. Id. The court agreed in part, holding that a producing party does not have an explicit duty to preserve evidence in an accessible format, but that the producing party must bear the cost of producing evidence converted into an inaccessible format after litigation is reasonably anticipated. Id. at 29. This would "prevent parties from taking unfair advantage of a self-inflicted burden by shifting part of the costs of undoing the burden to an adversary." Id. at *31. Conversely, "if it is not reasonably foreseeable that the evidence at issue would have to be produced, the producing party who converts the evidence into an inaccessible format after the duty to preserve evidence arose, may still seek to shift the costs associated with restoring and searching that evidence." Id. Applying this analysis, the court determined that defendant should have reasonably anticipated the production of e-mails for all but one of the former or current employees. For that individual, the court relied on the *Zubulake I* seven factor cost shifting test and ruled the plaintiff should share thirty percent (30%) of the production costs. Ultimately, the defendant was only able to recover a little more than four hundred dollars out of the hundreds of thousands it cost to produce all of the requested ESI. Id.

B. Allocation of Costs in New York State Courts

Unlike the presumption under the FRCP that the producing party bears the costs of complying with discovery requests, New York state courts have held that under the CPLR the requesting party must incur the costs of discovery and production. Lipco Elec. Corp. v. ASG Consulting Corp., 798 N.Y.S.2d 345 (Sup. Ct. Nassau Cty. 2004). Thus, the electronic discovery analysis in New York begins and ends with the determination of whether the requested discovery is permissible under the CPLR. So long as the requesting party is willing to bear the costs of production, if the court determines that the requested discovery is "material and necessary" no further analysis or court orders are required. In Lipco, the requesting party refused to pay the costs of production and moved for a cost shifting order. The court concluded "until such time as [plaintiff] express a willingness to pay the costs to be incurred for the production of this data, the Court will not direct its production". 798 N.Y.S.2d at 348. This significant difference between the CPLR and FRCP must be considered by plaintiff's counsel when selecting a forum. Individual plaintiffs with limited resources may not be able to engage in electronic discovery in New York state courts, particularly when discovery from inaccessible sources is required, which could affect the plaintiff's ability to build a persuasive case. This could lead to the realization of the ominous warning issued by the *Zubulake* court – too high a burden may "chill the rights of litigants to pursue meritorious claims". Moreover, the choice to bring an action that is likely to involve significant electronic discovery in a New York state court could open the plaintiff's counsel to a claim of professional malpractice.

C. Cost Shifting Issues Not Yet Addressed

The cost of complying with electronic discovery obligations extends beyond just the expenses of collecting, processing, reviewing, and producing ESI. Depending upon the scope of discovery and data storage methods implemented, the producing party may incur substantial

losses through reduced operational efficiency. For example, if a business (as most do) depends upon the operation of an information system to generate revenue or to support revenue-generating business functions, and that information system must operate in a diminished capacity or be shutdown in order to facilitate the acquisition of evidence from it, the business may be forced to sacrifice revenue in order to comply with its discovery obligations. Further, what if the plaintiff and defendant are competitors and the plaintiff stands to gain at the defendant's expense? Should the costs of lost revenue, lost opportunity, and competitive advantage be factored into the cost shifting analysis? Does the "total cost of production" under the *Zubulake* test include these types of less tangible costs or is it limited only to concrete costs (e.g. fees paid to a vendor to restore and process data)? Perhaps the answer will hinge upon the reasonableness of the producing party's preparedness for electronic discovery. If, for example, the producing party has implemented redundant information systems so that critical business functions can continue at full capacity even if the primary system must be taken off-line, the court may be more sympathetic to the producing party if it is forced to incur revenue losses or a competitive disadvantage not reasonably foreseeable. To compensate the diligently-prepared producing party, courts may limit discovery or shift a greater percentage of costs to the requesting party. To the contrary, if the producing party has not diligently prepared for the possibility of electronic discovery and the resulting business impact, courts may be less sympathetic and less hesitant to shift these less tangible costs to the requesting party.

V. PROTECTION OF THE ATTORNEY-CLIENT PRIVILEGE

Attorney-client privilege protects against the disclosure of confidential communications made between a lawyer and his / her client for the purpose of obtaining or providing legal advice or services. Atronic Int'l. v. SAI Semispecialists of Am., Inc., 232 F.R.D. 160, 162 (E.D.N.Y.

2005). Parties to litigation are not required to disclose privileged documents or ESI during discovery and courts generally cannot compel a party to produce privileged communications. Rowe Entm't., Inc., 205 F.R.D. at 432. Confidentiality is the key element in creating and maintaining attorney-client privilege over a document or ESI. The *voluntary* disclosure of communications protected by attorney-client privilege generally results in the waiver of a claim of privilege. Williams v. Sprint / United Mgmt. Co., 2006 WL 1867478, at *7 (D. Kan. 2006); Atronic Int'l., 232 F.R.D at 163. A more critical issue with electronic discovery is the potential for *inadvertent* disclosure of privileged communications, which, under some circumstances may result in the waiver of privilege over those materials. With electronic information, the risk of producing privileged communications is increased because of the sheer volume of ESI subject to discovery. The risk of privilege waiver resulting from voluntary or inadvertent disclosure, and the costs necessary to avoid such waiver, add to the costs and delay of discovery.

The amended Rules require issues related to privilege and waiver to be addressed by attorneys and courts early in the litigation process. Parties must discuss any issues relating to the assertion of privilege at the 26(f) conference, including whether the parties can facilitate discovery by agreeing on procedures for asserting claims of privilege or protection after production and whether to ask a court to enter an order that includes any agreement the parties reach. Fed. R. Civ. P. 26(f)(4). Further, Rule 16(b)(6) encourages the court to include in its scheduling order any privilege and waiver agreements between the parties.

The law controlling attorney-client privilege and waiver based on voluntary or inadvertent disclosure depends upon whether the underlying cause of action arises under federal law or state law. In cases brought under federal question subject matter jurisdiction, federal privilege law controls. Atronic Int'l., 232 F.R.D at 162; Kaufman v. Sungard Inv. Sys., 2006 WL 1307882, at *2 (D.N.J. 2006). Likewise, in cases brought in federal court based upon diversity of citizenship

jurisdiction, which involve claims grounded in state law, state privilege law controls. Id. Under federal law the essential elements of attorney-client privilege are: (1) legal advice is sought; (2) from a professional legal advisor in his or her capacity as such; (3) the communications relating to that purpose; (4) made in confidence; (5) by the client; (6) are at his instance permanently protected; (7) from disclosure by himself or by the legal advisor; (8) except the protection be waived. Williams, at *5; Atronic Int'l., 232 F.R.D at 162. Nearly all states mirror or closely adhere to the federal law of when attorney-client privilege attaches.

A. Inadvertent Disclosure of Privileged Information

Generally inadvertent production of privileged information does not waive the privilege unless the producing party's conduct was so careless as to suggest that it was not concerned with the protection of the asserted privilege. Curto v. Medical World Communications, Inc., 2006 WL 1318387, at *2 (E.D.N.Y. 2006); Atronic Int'l., 232 F.R.D at 163. The vast majority of federal courts apply a five factor test, or a close derivative thereof, to determine whether the inadvertent disclosure of a document constitutes a waiver of the attorney-client privilege or of work-product protection. These five factors include: (1) the reasonableness of the precautions taken to prevent inadvertent disclosure; (2) the time taken to rectify the error; (3) the scope of discovery; (4) the extent of disclosure; and (5) the overriding issue of fairness. Williams, at *9. This test grants courts substantial discretion in determining whether waiver results from inadvertent production. Courts are generally reluctant to find waiver of privilege based upon inadvertent disclosure of ESI, reserving this consequence only for those cases where the producing party was demonstratively careless in conducting its review prior to production.

In Williams, at *9-10 the court found that inadvertently produced spreadsheets containing statistical information created at the request of the defendant's attorneys for the purpose of obtaining legal advice were protected by attorney-client privilege. In ruling the privilege had not

been waived by the defendant's inadvertent disclosure, the court applied the five factor test outlined above. To prevent inadvertent disclosure, the defendant converted the documents into TIFF images, allowed attorneys to review the images on a computer screen, and implemented document production software to label "privileged" documents for inclusion within the privilege log. Id. Citing the Advisory Committee's comments to the amendments to Rule 26(f), the court considered the added volume, expense and time required to sift through ESI in concluding that the defendant's efforts to prevent disclosure were reasonable. Id. at *9. In addition, since the defendant had immediately taken steps to secure the return of the spreadsheets after learning the documents had been inadvertently disclosed, the court ruled the privilege not waived and ordered the documents be returned to the defendant. Id. at *10.

Conversely, the court in Atronic Int'l. found that the inadvertent production of two privileged e-mails constituted a waiver of attorney-client privilege. 232 F.R.D at 166. The court found that the producing party's counsel failed in a number of ways, including: (1) counsel failed to take adequate steps to preserve the confidentiality of the e-mail in question; (2) counsel failed to label the e-mails "confidential" or "privileged"; (3) counsel failed to employ a reasonable procedure for separating privileged documents from non-privileged communications; and (4) counsel waited one full week after production to demand the return of the privileged materials. Id. at 164-166. Further, although counsel conducted a privilege review prior to production, the court found that reasonable precautions were not taken because, *inter alia*, the attorney assigned to conduct the review did not know the identity of plaintiff's legal counsel. Id. at 164. The court concluded that plaintiff's counsel exercised "inexcusable carelessness" in preventing and then attempting to remedy the inadvertent disclosure, which resulted in a waiver of privilege. Id. at 166.

To further address the issue of inadvertent waiver, the Committee on the Rules of Practice and Procedure of the Judicial Conference of the United States has proposed amending Rule 502 of the Federal Rules of Evidence. The proposed amendment explicitly provides that "inadvertent" disclosure of privileged or work-product material would not operate as a waiver in a state or federal court proceeding if the disclosure is made in connection with federal litigation or federal administrative proceedings. Further, the party asserting a claim of privilege or work product protection must have taken "reasonable precautions" to prevent disclosure and "reasonably prompt measures" to rectify the error once the party knew or should have known of the disclosure.

B. Procedures for Privilege Review and Production of ESI

Courts have employed various procedures when confronted with issues involving electronic discovery and the protection of attorney-client privilege. The most fundamental difference in each of these procedures has been whether the producing party conducts a privilege review prior to or after initial production. The rationale for conducting a privilege review after initial production is to expedite discovery, to limit the costs of review for the producing party, and to ensure that the producing party has sufficient time to review for privilege without fear of waiver. This type of disclosure is commonly referred to as "quick peek" production, whereby the requesting party is permitted to conduct an initial examination of the produced materials on an "attorneys'-eyes-only basis" to cull out relevant information upon which to base specific document and ESI requests. The producing party only needs to conduct a privilege review of the specific documents and ESI requested for final production. Most notably, the producing party does not waive any claim of privilege through the initial "quick peek" disclosure. Of course, once the opposing party has had a chance to review a privileged document, even if it must return or destroy it, that party still has knowledge of its contents. Although the privileged communication cannot be admitted as evidence, it will most certainly play into the overall litigation strategy.

Under the procedure adopted in *Rowe*, the court allowed the producing party to choose between these two types of review protocols. 205 F.R.D. at 433. The producing party could elect to produce the electronic information prior to a privilege review for initial examination by the requesting party; however, until the producing party actually performed the privilege review, the requesting party's counsel could only review the documents on an "attorneys'-eyes-only basis." Id. Further, all claims to privilege or work product were specifically reserved and a protective order was granted stating that the requesting party's review of such information did not waive attorney-client privilege or work-product protection. Id. Under the second option, the producing party could choose to conduct a review for privilege, work-product and confidentiality prior to production. If it chose to do so, it would then have to provide the opposing party with redacted copies, as well as a privilege log identifying the protected documents. Id.

The U.S. District Court for the Eastern District of Louisiana adopted a similar approach in Murphy Oil USA, Inc., at *7-8 whereby the producing party was also permitted to choose between two review protocols. Under the first option the producing party could elect to produce the requested information in hard copy and / or electronic format prior to conducting a privilege review. The court would then issue a protective order requiring the requesting party to conduct its initial examination of the evidence on an attorney's eyes only basis. The court ordered that although privileged information might be disclosed to opposing counsel during this initial production, such disclosure would not constitute a waiver. Id. at *8. The requesting party would be responsible for identifying relevant evidence and would return only responsive documents with Bates numbering to the producing party; the requesting party was ordered to destroy all non-responsive documents and electronic data. Id. The producing party would then conduct a privilege review of only the responsive documents and designate by reference to the Bates number four categories of documents in a privilege log: (1) proprietary; (2) attorney-client

communications; (3) communications that represent the work product of an attorney; and (4) discoverable documents. Id. If the requesting party agreed with the designation of a particular document as privileged or work product it was mandated by the court to destroy all hard copies and electronic copies of those documents within its possession. If the requesting party disagreed, the parties would be required to meet in order to resolve the issue, and, if resolution was not possible the parties could then present the issues to the court for determination. Id. at *9

Under the second option, the producing party could elect to conduct a privilege review prior to production. Following this approach, the producing party would be required to cull out responsive information and then apply Bates numbering to the set of documents and ESI deemed responsive. Id. By reference to the Bates numbers, the producing party could then assert claims of privilege for individual documents and e-mail. All responsive, non-privileged information would then be produced to the requesting party, along with the privilege log. The requesting party could object to any claim of privilege, and follow the procedure described in the first option to resolve issues of privilege. Under the second approach, the inadvertent production of privileged information to the requesting party could operate as a waiver of privilege, depending upon the reasonableness of the procedures employed by the producing party to identify privileged materials and the precautions taken to prevent inadvertent disclosure.

Amended Rule 26(b)(5)(B) establishes a procedure for a party to assert a claim of privilege after the production of evidence. Under this provision, if information is produced in discovery that is subject to a claim of privilege or work-product protection, the party making the claim may notify any party that received the information of the claim and the basis for it. Fed. R. Civ. P. 26(b)(5)(B). After being notified, a party must promptly return, sequester, or destroy all copies of the specified information and may not use or disclose the information until the claim is resolved. Id. The requesting party may "promptly present the information to the court under seal

for a determination of the claim." Id. If the requesting party disclosed the information to a third party prior to being notified of the claim of privilege, it must take reasonable steps to retrieve the information from such third party. Id. Further, the producing party must preserve the information subject to the privilege claim until the dispute is resolved. Id. It is important to apply this rule in the context and under the limitations intended by the drafters; the rule only establishes a procedure for the assertion of a privilege claim – it does not address whether a particular disclosure constitutes waiver of privilege. Advisory Committee Notes to Fed. R. Civ. P. 26. Pre-existing federal or state substantive law continues to control the issue of whether and under what circumsntaces inadvertent production constitutes waiver of privilege.

C. Clawback Agreements

Parties are permitted to enter into agreements that will control how issues involving privilege and waiver will be treated throughout the discovery process. The use of such agreements enables parties to manage the risks of inadvertent disclosure, and takes the "guesswork" out of whether a particular disclosure might later be found by the court to constitute a waiver. The parties may adopt a "clawback" agreement which specifies that production of privileged materials without the intent to waive such privilege will not constitute a waiver. Further, clawback agreements typically require the requesting party to return the privileged materials to the producing party. The use of a clawback agreement effectively estops the requesting party from asserting that the inadvertent disclosure of privileged material should operate as a waiver, notwithstanding considerations of the reasonableness of the producing party's efforts and overriding issues of fairness that would be applicable under federal or state common law. Courts generally will enforce clawback agreements made between parties to a lawsuit, however, there are no guarantees that such agreements will be binding upon third parties (e.g. if the requesting party, after receiving privileged communications from the producing party, re-

discloses the privileged material to a third party). Proposed Rule 502 of the Federal Rules of Evidence attempts to address this issue by requiring that clawback agreements be binding not only upon all parties having entered into the agreement, but also upon non-parties to the immediate litigation, provided that the agreement between the parties is incorporated into a federal court order.

VI. THE MECHANICS OF ELECTRONIC DISCOVERY

In order for the producing party to satisfy its discovery obligations in response to requests for ESI, it must employ several technical processes prior to actual delivery to the requesting party. In particular, responding parties must implement technical processes to: collect data sources and acquire data from each source; preserve ESI; restore data from inaccessible sources, if necessary; recover deleted, corrupted, fragmented, or hidden data, if necessary; process and search for responsive ESI; analyze ESI for responsiveness; review for privilege; and produce ESI in the agreed-upon format. Advanced computer forensic methods and techniques are typically employed to conduct many of these technical processes, however, few law firms, businesses, and government agencies employ personnel with the requisite skills, knowledge, and expertise in conducting forensic analysis. Often third party experts will be retained to provide electronic discovery and computer forensic services to the producing party. The use of third party experts in turn raises issues related to privilege, confidentiality, vendor selection, and agency relationship. Like many other areas of electronic discovery law, courts have been left to manage these issues by developing protocols for carrying out technical procedures.

A. Court Defined Protocols for the Use of Third Party Experts

The court in Playboy Enters., Inc. established one of the earliest and most-cited protocols for the use of expert electronic discovery and forensic providers. In *Playboy*, the plaintiff

petitioned the court to appoint a third party expert to conduct to conduct forensic examination of the defendant's computer hard drive after it was shown that defendant had engaged in a continuous practice of deleting potentially relevant e-mail. The court found that any burden imposed on the defendant was outweighed by the plaintiff's need for the requesting information, and that such forensic examination was necessary due to defendant's conduct of deleting e-mail without regard to the pending litigation. Playboy Enters., Inc., 60 F.Supp.2d at 1054. The plaintiff was ordered to pay for the e-mail recovery and the court first required the plaintiff to submit a declaration from an expert regarding the feasibility of recovering defendant's deleted e-mails. If the plaintiff was able to provide sufficient evidence that "recovering some deleted e-mail is just as likely as not recovering any deleted e-mail, and that no damage will result to defendant's computer", the court would direct the parties "to follow the outlined protocol." Id. at 1055.

Under the *Playboy* protocol, the court first appoints a computer expert who specializes in the field of electronic discovery. The parties are required to meet and confer to select the expert, and, if the parties cannot agree the court will appoint the expert based upon the parties' suggestions. Id. The appointed expert serves as an Officer of the Court and must sign a protective order to address the producing party's privacy and privilege concerns. Under the protective order in *Playboy*, any disclosure of privileged material to the expert would not constitute waiver and the plaintiff was barred from asserting any claim of wavier. The expert then creates a "bit stream image"[8] of the defendant's hard drive at a time and date convenient for the defendant, in the presence of only the defendant and her counsel. After the image is made, it must

---

[8] A "bit stream image" (also referred to as a "mirror image" or "forensic image") is an exact duplicate of the original computer media. Often the source drive is referred to as the "cloned" drive. The mirror imaging / bit stream backup / forensic imaging process captures all data residing on a particular storage medium, including active files easily recognized by ordinary users but also deleted, corrupted, fragmented, and hidden data.

be given to defendant's counsel, who is responsible for printing, reviewing, and producing any relevant, non-privileged documents recovered from the hard drive. All privileged documents must be listed on a privilege log. Id. The court in *Playboy* further directed that the defendant's counsel would be the sole custodian of the mirror image and that counsel must retain for the duration of the litigation the image and copies of all documents produced to the plaintiff. Id.

Another court adopted a similar approach in Simon Property Group, 194 F.R.D. at 641-42. The only differences were that the expert was required to make a report to the court describing the scope of the work performed and the volume and type of records provided to the producing party's counsel. The expert was also, to the extent possible, supposed to provide the producing party's counsel with any available information showing when any recovered "deleted" file was deleted, and the available information about the deletion and contents of any deleted file that could not be recovered. Id. at 641. Moreover, any communication between the expert and the requesting party's counsel was to be in the presence of the producing party's counsel, and the expert – rather than the producing party – was to maintain a copy of the "mirror image" until the conclusion of litigation. Id. at 642.

Yet another court fashioned an "amalgamation" of the procedures set forth in *Playboy* and *Simon*. *See* Antioch Co., 210 F.R.D. at 653. One significant difference was that the requesting party was allowed to select the computer expert to produce the bit stream image of the producing party's computer equipment. Id. The computer expert was ordered to use its best efforts to avoid unnecessarily disrupting the normal activities or business operations of the producing party while inspecting, copying, and imaging the producing party's computer equipment, up to and including the retention of the computer equipment on the producing party's premises. Id. Moreover, the only persons authorized to inspect, or otherwise handle such equipment, were employees of the

third party expert. Id. The computer expert was required to maintain all information in the strictest confidence.

Within ten days of its inspection, copying, and imaging of the producing party's computer equipment, the third party expert was required to provide the parties with a detailed report as to what computer equipment was made available by the producing party, and the actions taken by the expert with respect to each piece of computer equipment. Id. Additionally, the expert was required to document the chain of custody for any copies and images drawn from the equipment.

Subsequently, the third party expert was required to produce two copies of the resulting data. Id. One copy was to be transmitted to the court, and the other copy was to be transmitted to the producing party. Id. Thereafter, the producing party could sift through the data provided by the computer expert to locate any document responsive to the requesting party's discovery demands. Id. The responding party could then produce the documents that are "properly discoverable," as well as a privilege log. Id. At that time, the producing party also had to forward the privilege log to the court for potential in camera review. Once it has reviewed the documents produced, as well as the privilege log, the requesting party could raise a dispute as to any of the documents. Id. The court could then conduct an in camera review, limited to the issues raised.

More recently, the court in *Rowe* established a five-step protocol for the use of an expert electronic discovery provider:

1. The requesting party shall designate one or more experts who will be responsible for isolating and preparing the requested ESI for review. The producing party may object to the expert(s).

2. The producing party shall provide its discoverable hard drives and / or backup tapes to the requesting party's expert(s).

3. The requesting party's counsel shall formulate a search procedure, including any specific keyword searches. The producing party's counsel may object to any search protocols (note that the court in *Rowe* did not discuss how the parties should resolve such disputes).

4. The requesting party's expert(s), bound by applicable confidentiality orders, shall conduct the agreed upon search. The requesting party's counsel may also review the documents, but on an "attorneys'-eyes-only basis". Significantly, all claims to privilege or work product are specifically reserved and the requesting party's review of such information does not waive such privilege or work-product protection.

5. The responding party may choose to conduct a review for privilege, work-product and confidentiality prior to production. Should it choose to do so, it would then provide the opposing party with redacted copies, as well as a "privilege log" identifying the protected documents.

Rowe Entm't Inc., 205 F.R.D. at 432-33.

The Supreme Court for Nassau County, in a matrimonial action, adopted a protocol different from, but not inconsistent with, the protocols devised by federal courts. Etzion v. Etzion, 796 N.Y.S.2d 844, 847 (Sup. Ct. Nassau Cty. 2005). In Etzion, both the plaintiff and defendant retained their own computer forensic experts and the court appointed an attorney referee to supervise discovery and resolve disputes. Id. Similar to the federal court protocols, the plaintiff's expert was permitted to create a bit stream image of the defendant's hard drive, however, unlike the federal protocols the defendant's expert and the referee were ordered to accompany the plaintiff's expert. Id. Further, once the mirror images were created, the plaintiff was required to turn over the images to the referee. Id. Following the imaging process, both experts and the referee were ordered to meet in order to jointly examine the hard drives. Id. The referee was then ordered to retain possession of the cloned hard drives until conclusion of the case, at which time the cloned hard drives were returned to the defendant for disposal. Id.

B. Preservation and Collection of ESI

The use of forensic evidence acquisition procedures versus the mere copying of "active" files protects the interests of both requesting and producing parties. Forensic acquisition procedures involve not only the creation and authentication of a bit stream image through the use

of specialized software, but also the maintenance of evidence chain of custody documentation to ensure individual accountability and adequate protection of volatile ESI sources. From the producing party's perspective, the use of forensic acquisition procedures ensures that the producing party employs legally defensible evidence collection and preservation processes. As discussed *supra* at p.24, deleted data is just as discoverable as active files. Simple copying of active files does not entirely satisfy the producing party's preservation duty, as entire categories of discoverable ESI are not preserved (e.g. deleted files, hidden files, and data contained in hidden areas of a hard drive such as slack space, swap space, and unallocated space). Requesting parties may be able to leverage the limitations of non-forensic procedures to move for direct access to the producing party's systems. The use of a legally defensible protocol, based upon generally accepted forensic procedures, helps producing parties to preempt challenges and objections as to the adequacy of technical discovery processes.

The use of forensic evidence acquisition procedures also benefits the requesting party because all potentially discoverable information is captured through the bit stream imaging process, not just active files. If the producing party is employing forensic methods and procedures in the collection and preservation of evidence, the requesting party can be reasonably certain that the producing party will conduct a diligent search of all potentially responsive data sources.

C. Processing and Analysis of ESI

Several technical processes are involved in the processing and analysis of ESI in order to identify and locate evidence responsive to the requesting party's demands. In cases where data is stored on an inaccessible data source, such as a backup tape, the first step after forensic acquisition is the restoration and conversion of the data into an accessible format. Next, the producing party must recover deleted files, if demanded by the requesting party, in order to create a comprehensive source of data from which to extract relevant evidence.

Due to the sheer volume of ESI at hand in most litigation involving a commercial party, it is impractical to manually review the ESI for relevancy. Rather, specialized software applications automate the process by permitting producing parties to search for responsive evidence within voluminous data sources. Prior to conducting searches, however, the producing party should conduct a "de-duplication" process, whereby duplicate copies of electronic files are culled out. While parties are generally not required to produce more than one copy of identical ESI, documents that appear identical as displayed on a computer screen often contain different metadata. The exact content of certain metadata fields is dependant upon when certain actions were taken with each individual instance of a seemingly identical file, including creation, modification, deletion, printing, and access times and dates. The producing party must be careful to preserve and then produce identical files stored in multiple locations, if so demanded by the requesting party. After all duplicates are culled out, further data filtering should be done prior to conducting keyword and text string searches in order to maximize the efficiency and speed of the search process. For example, system-created files (e.g. files created by Microsoft Windows and other applications during software installation) should be filtered out, as these files will not contain relevant evidence. To the contrary, user-created files (e.g. word processing documents, spreadsheets, e-mail, databases, etc.) may contain evidence relevant to a claim or defense and must be searched.

After removing duplicate data files and filtering out ESI clearly irrelevant to the litigation, the producing party must identify and locate relevant evidence by conducting automated keyword searches and text string searches. Search terms should be reasonably tailored to ensure the greatest amount of relevant evidence is discovered while minimizing the number of "false positive" search hits that identify irrelevant data. Search programs used by producing parties or by experts employed by producing parties should include the capability to conduct "Boolean"

searches in order to balance these competing interests. Forensic search utilities will identify relevant evidence contained not only in active files but also relevant keywords contained in deleted files, hidden files, unallocated space, slack space, swap space, and other covert areas of electronic storage media.

D. Privilege Review

Paper documents and computer printouts have traditionally been the medium used to conduct privilege reviews. Due to the increasing volume of ESI produced through electronic discovery, it is becoming increasingly burdensome and impractical to printout all ESI for the purposes of conducting a privilege review. Keyword search programs are quickly gaining favor and acceptance for use in privilege reviews. As a matter of practice, any communication protected by attorney-client privilege will have an attorney's name or identification attached to it. Keyword search programs can be used to locate all instances of attorney names, nicknames, and e-mail addresses, thus streamlining the privilege review process. Rather than reviewing the entire body of discoverable ESI for privilege, the producing party only needs to review documents and communications containing the search results.

E. Production of ESI

Production of ESI can take one of four forms: (1) paper printouts; (2) reduction to common electronic format (e.g. quasi-paper electronic files, searchable text, etc.); (3) load files for litigation support software applications; or (4) "native"[9] electronic format. Under amended Rule 34 the requesting party may specify the form or forms for production of ESI. Fed. R. Civ. P.

---

[9] "Native" format is the file structure as created by the original application. For example, Microsoft Word documents are created and stored as .DOC files, while Microsoft Excel spreadsheets are created and stored as .XLS files. These formats (.DOC and .XLS) are "native" for the respective applications. Native format includes all associated metadata, which is ordinarily lost if the information is converted from native format. The original application (e.g. Word, Excel) is often required to view files in native format.

34(b). If the requesting party does not specify a form for production, the producing party must state the form or forms it intends to use. Id. Either the requesting party or the responding party may object to the form or forms demanded by the opposing party. If either party objects, the parties must meet and confer under Rule 37(a)(2)(B) before the requesting party can file a motion to compel. If the parties cannot reach a mutual agreement as to form or forms for production, the court can order the form or forms to be used.

If the form of production is not specified by the parties or by court order, the responding party must produce ESI either in a form or forms in which it is "ordinarily maintained" or in a form or forms that are "reasonably useable". Fed. R. Civ. P. 34(a). If the responding party ordinarily maintains information in searchable form (e.g. plaint text), the information cannot be produced in a form that removes or significantly degrades this feature (e.g. image files that are not text-searchable). Further, if necessary, the producing party must translate ESI into a reasonably useable form. Id. For example, if data is stored within a legacy information system for which specialized programs or hardware are required in order to access the data, the producing party must convert the data into a form that the requesting party can access, view, and search. Courts are cognizant of the burden and expense that a producing party may need to incur in order to translate and convert legacy or other inaccessible data. The Rule 26(b)(2)(C) proportionality test is used by courts to determine whether the producing party must convert these data to a reasonably useable form.

Absent an agreement by the parties or a court order requiring production in a particular form, courts must determine what form or forms are "reasonably useable" and what constitutes the form "ordinarily maintained". The first question raised is whether ESI should be produced in paper or electronic form. Courts will generally require parties to produce documents electronically and not in paper where the electronic data is available. For example, in Gilliam v.

Addicts Rehab. Ctr. Fund, the defendant refused to produce timekeeping and payroll contained on 148 CDs, asserting the claim that production of the CDs would reveal private employee data. 2006 WL 228874, at *1 (S.D.N.Y. 2006). Instead, defendant stated it would produce paper records containing the relevant information. Noting that paper production would comprise forty-six boxes and approximately 36,000 pages, the court stated that "there seems little doubt that the time and cost expenditure could be disproportionate to the interests sought to be protected". Id. at *2. The court contrasted this with an electronic review whereby the "plaintiffs could make duplicates of the computer discs quickly and inexpensively. These discs could then be reviewed in a more efficient manner and the sensitive information skipped by the reviewer(s)." Id. The court further assured confidentiality concerns would be handled through a protective order.

After receiving 301,539 pages of documents in response to 131 discovery requests, the plaintiff in CP Solutions PTE. Ltd. v. GE, accused the defendant of engaging in "dump truck" discovery tactics. 2006 WL 127615 (D. Conn. 2006). The plaintiff asserted the documents were not produced as maintained in the "ordinary course of business", citing e-mails that were separated from their attachments and pages containing lines of "gibberish". Id. The plaintiff sought to prohibit the defendant from using any documents not produced in their initial document disclosure; or, alternatively, to compel defendants to supplement its initial production by (1) identifying every document responsive to each of the plaintiff's requests; (2) organizing and labeling each responsive document to correspond to the categories of the plaintiff's requests; and (3) producing the documents in "native" format. Id. The court denied the plaintiff's motion for preclusion and refused to require the defendants to organize and label the produced documents as requested by the plaintiffs. Id. Further, the court declined to order the defendants to produce e-mails in their native format, as the defendants would not be able to sort out privileged files. Id. In partially granting the plaintiff's motion to compel, the court required the defendants to "re-

produce" the documents containing "gibberish" in a reasonably usable electronic format. Id. The court also required the defendants to provide the plaintiff with the information, data, or software necessary to match the e-mails with their attachments, stating, "the fact that the attachments were created with different software programs . . . does not provide [d]efendants with an excuse to produce the e-mails and attachments in a jumbled, disorganized fashion". Id. *See also* Miller v. IBM Corp., 2006 WL 995160, at *7 (N.D. Cal. 2006) (plaintiff was ordered to produce e-mails with attachments "physically attached"); Static Control Components, Inc. v. Lexmark Int'l, Inc., 2006 WL 897218, at *3-4 (E.D. Ky. 2006) (ordering defendant to produce database to plaintiff in a "reasonably usable form" over defendant's objections that software to read database was no longer available; "The Federal Rules do not permit [the defendant] to hide behind its peculiar computer system as an excuse for not producing this information to [the plaintiff]").

Production of ESI in electronic form, rather than through paper printouts, enables both the producing and requesting parties to more efficiently review, analyze, and extract information from materials provided through discovery. The producing party can take advantage of sophisticated search programs to streamline the privilege review process and minimize the risk of inadvertent disclosure. Likewise, the requesting party may also use search programs to aid in its review and trial preparation. Moreover, production in electronic format will aid requesting parties in quickly and cost-effectively reproducing and making available discoverable information to all members of the litigation team. Although most courts will require production of ESI in electronic format, it may be within the requesting party's best interest to demand both production in electronic form and production of pre-existing printouts of electronic files (as opposed to print-outs created solely for production). While the electronic files will contain information not present in print-outs, such as metadata, spreadsheet formulas, and document revisions, the pre-existing printouts may likely contain handwritten notations not present or represented in the electronic files.

A party can meet production requirements by providing the requesting party with text searchable electronic documents without reviewing the electronic documents for responsiveness. *See* Zakre v. Norddeutsche Landesbank Girozentrale, 2004 WL 764895, at *1 (S.D.N.Y. 2004) (denying plaintiff's motion to compel further discovery of two CDs containing over 200,000 e-mails, even though defendant did not review the emails for responsiveness to the plaintiff's specific document requests; defendant satisfied discovery obligation by providing all of the e-mails in a text searchable format, which allowed the plaintiff to search for single words or phrases or combinations of words or phrases). *See also* Eastman Kodak Co. v. Sony Corp., 2006 WL 2039968, at *1 (W.D.N.Y. 2006) (denying defendant's motion to compel plaintiff to "more specifically correlate information produced electronically" to discovery requests; although court recognized substantial time, effort and expense would be required to sort through produced documents, this was reasonable in light of billions of dollars at issue in case, and plaintiff was in no better position to correlate the information to defendant's discovery requests than was defendant).

1. Format for Electronic Production

As outlined above, ESI may be reduced to a common format, converted to a load file for a litigation support application, or produced in native form. The distinction between each format has significant consequences for each party. Under the first option, ESI contained in disparate file formats (e.g. Word document, Excel spreadsheets, e-mail, and databases) is reduced to a common format. Most often, ESI is reduced to either the Adobe Portable Document Format (PDF) or the Tagged Image File Format (TIFF). In essence, PDF files and TIFF images are the electronic equivalent of printed pages, thus sometimes referred to as "quasi-paper" formats. The advantage to production in PDF or TIFF format is that the requesting party does not need to use specialized software or hardware to view each individual file type; the requesting party only needs to use a

PDF reader or TIFF image viewer, both of which are readily available free programs. One significant disadvantage of reducing native files to PDF or TIFF format is that metadata, spreadsheet formulas, and document macros are not included within the PDF or TIFF file. The consequence is that the requesting party is missing potentially relevant information. For example, metadata attached to an e-mail message will disclose the dates and time the message was sent, received, read, and deleted; all carbon copy (CC) and blind carbon copy (BCC) recipients of the e-mail; and the servers the e-mail passed through along the route from source to destination. The particular metadata fields for any given file vary depending upon the file type; however, in most instances metadata contains information that can be used to stitch a cause of action together. Moreover, when dealing with Excel spreadsheets, the PDF or TIFF representation of the spreadsheet will only display the values contained in each cell, whereas the native Excel file will reveal the formulas used to derive each value. A further limitation is that TIFF images are generally not text-searchable, which precludes the requesting party from conducting automated searching and analysis of the information produced in TIFF form. Unless ESI is maintained in TIFF form or some other non-searchable format in the "usual course of business", courts will generally find that conversion of searchable documents into a non-searchable format is impermissible. *See* Hagenbuch v. 3B6 Sistemi Elettronici Industriali S.R.L., 2006 WL 665005, at *3-4 (N.D. Ill. 2006) (the court granted plaintiff's motion to compel production of electronic documents in native file format after defendant produced the requested ESI in TIFF images. The court based its decision upon finding that TIFF production did not include metadata, e-mail attachments, or all recipients, and that the ESI was not maintained in TIFF format in the "usual course of business"); OKI Am., Inc. v. Advanced Micro Devices, Inc., 2006 WL 2547464, at *4-5 (N.D. Cal. 2006) (denying defendant's motion to compel production of electronic documents in text searchable format where earlier in litigation plaintiff produced to defendant similar

information in un-searchable electronic formatting (TIFF images). The plaintiff claimed, and the court agreed, that it bore cost of converting the TIFF files into a searchable database after defendant refused to produce information in a searchable format, and that defendant should be required to do the same).

From the producing party's perspective, conversion of ESI to PDF or TIFF format requires additional time and effort. More challenging is the production of metadata to supplement the production of PDF or TIFF files; this requires the producing party to employ forensic procedures to extract metadata from various file types and assemble the metadata in a meaningful and useful format. In addition, courts may add to the complexity of the PDF or TIFF conversion by requiring the producing party to apply Bates or other identification numbers to every page of each PDF or TIFF file.

The conversion of ESI to load files for litigation support applications, such as Concordance or Summation, benefits the requesting party because information produced through discovery can be integrated into an existing, familiar information management platform. This conversion process does not capture metadata, spreadsheet formulas, or document macros, however, which results in the same limitations and challenges described above. Further, the burden is on the producing party to convert data stored in various native formats to the proprietary format employed by litigation support applications. This may require the purchase of conversion software and also adds to the cost, complexity, and time for evidence production. Few, if any, courts have required producing parties to convert native files to a load file for the litigation software used by the requesting party. Further, parties generally do not request production in this form.

Production of ESI in native format is the most efficient option for producing parties; however, the party must ensure that it reviews all metadata for privilege. Native format

production keeps all metadata in-tact, so the producing party is not required to extract and re-produce metadata. Further, native format production does not involve the complex and often costly and time-consuming conversion tasks associated with production in PDF, TIFF, or load file formats. While native format production may seem to be the best option for the requesting party because it preserves all original data and metadata, the requesting party must use the original application in order to view native files. Ordinarily this is not a problem for commonly-used applications, such as Microsoft Office applications and popular e-mail platforms, however, requesting parties may not be able to access more obscure native formats without specialized software provided by the producing party or purchased by the requesting party. The costs and complexity involved in maintaining a library of software applications in order to access a broad range of native formats may outweigh the disadvantages involved with reviewing PDF and TIFF files without in-tact metadata.

Courts have been divided in whether or not to order native format production with metadata in-tact. *See* *In re* Priceline.com Inc. Sec. Litig., 233 F.R.D. 88, 91 (D. Conn. 2005) (the court ordered production in TIFF or PDF format with Bates numbering and appropriate confidentiality designations, supplemented by the production of searchable metatdata databases. The court further ordered the producing party to maintain the original data in native format for the duration of the litigation.); Williams v. Sprint / United Mgmt. Co., 2005 U.S. Dist. LEXIS 21966 (D. Kan. 2005) (the court stated that when documents are maintained in the regular course of business in electronic form, they should be produced in that form. Moreover, when a party is ordered to produce ESI as it maintained in the ordinary course of business, it must produce the ESI with metadata in-tact, unless the producing party obtains a protective order or timely objects to production of metadata.); Wyeth v. Impax Lab., Inc., 2006 WL 3091331, at *2 (D. Del. 2006) (upon receiving production of ESI in TIFF format without metadata the plaintiff moved to compel

production in native format with metadata in-tact. The court, in denying plaintiff's motion, stated "most metadata is of limited evidentiary value, and reviewing it can waste litigation resources" and that "emerging standards of electronic discovery appear to articulate a general presumption against the production of metadata". The court carved out an exception to this general rule, however, stating that native format production with metadata is appropriate if the requesting party demonstrates a "particularized need"); *In re* NYSE Specialists Sec. Litig., 2006 WL 1704447, at *1 (S.D.N.Y. 2006) (upon motion by the plaintiffs, the U.S. District Court for the Southern District of New York ordered production of ESI in native format with all metadata in-tact. The court further ordered that the plaintiffs be provided with a copy of the software previously used by the Securities and Exchange Commission to analyze and identify allegedly illegal trades.) *In re* Verisign, Inc. Sec. Litig., U.S. Dist. LEXIS 22467 (N.D. Cal. 2004) (the court ordered production of responsive electronic documents in native form with metadata in-tact. The court order expressly stated that "production of TIFF version alone is not sufficient" and that "the electronic version must include metadata as well as be searchable".). Current best practice for the requesting party is to request certain ESI in native format, while demanding other ESI be produced in PDF or text-searchable TIFF format. Under this approach, the requesting party can demand that spreadsheet files be produced in native format so that cell formulas and other metadata are left in-tact. Other file types for which the native application is readily available, such as Microsoft Word and Outlook, should be demanded in native format as well. More obscure or less accessible file types, such as databases and files crated by legacy or proprietary applications, should be demanded in PDF or TIFF format, to be supplemented by production of metadata in a reasonably useable form. The requesting party should take advantage of Rule 34 by specifying its production format needs at or before the Rule 26(f) conference in order to preempt the producing party from selecting or beginning to use its choice of format. The requesting party can either obtain the

agreement of the producing party to bifurcate production formats for certain types of ESI or may petition the court to order such production.

VII. CONCLUSION

Although e-discovery presents many challenges, parties to litigation should be able to avoid potential pitfalls by preparing for electronic discovery even before the possibility of litigation arises. Attorneys should advise clients to prepare for e-discovery by establishing and implementing records management programs. Through proactive records management, organizations can significantly reduce the risks and costs of litigation and e-discovery. Further, the routine destruction of business records in compliance with established Records Management Policies and Procedures, coupled with a strong process to issue "litigation holds", substantially reduces the likelihood parties to a lawsuit will be subject to spoliation sanctions. Future rulings on e-discovery will flesh out the contours of the FRCP amendments and provide attorneys and their clients with additional guidance.