

The “Litigation Hold” and Other ESI Moves: What You and Your Client Need to Know Before Stepping Into the Ring

Speakers:

Judge Nancy F. Atlas
United States District Judge
Houston, Texas

Bob Dibert, Esq
Frost Brown Todd
Louisville, Kentucky

Katie Jensen
Navigant Consulting, Inc
Chicago, Illinois

Antonio Matthews, Esq
Baker Donaldson
Memphis, Tennessee

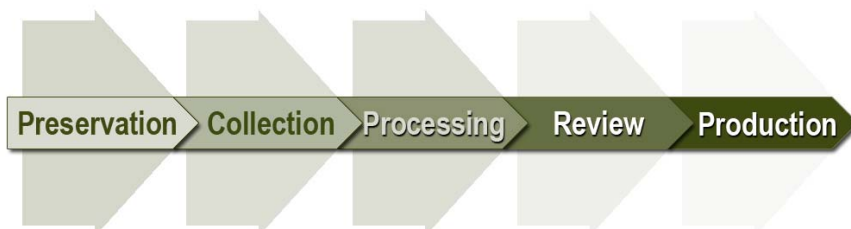
Amy L. Tenney
Jenner & Block
Washington, DC

“THE REALITY OF ELECTRONIC DISCOVERY IS IT STARTS OFF THE RESPONSIBILITY OF THOSE WHO DON’T UNDERSTAND THE TECHNOLOGY AND ENDS UP THE RESPONSIBILITY OF THOSE WHO DON’T UNDERSTAND THE LAW.” - CRAIG BALL, CORPORATE COUNSEL, “THE PERFECT PRESERVATION LETTER,” APRIL 2005.

Electronic data discovery at a high-level is composed of the following processes: (1) Preservation, (2) Collection, (3) Processing, (4) Review, and (5) Production.

Preservation Overview

Proper preservation is one the most critical aspects of eDiscovery because it feeds all the other subsequent processes. If electronically stored information (“ESI”) isn’t preserved, it is impossible to review and produce. Key elements of preservation are as follows:



- Understanding when there is a reasonable anticipation of litigation and acting upon it;
- Accurate knowledge of IT systems and processes;
 - IT systems and organization
 - Data repositories
 - Retention, destruction and recycling process
 - Up to date “data map” is crucial (think beyond email)
 - Need to be able to convey internal and external data and it’s accessibility
 - Consider data sampling on a case by case basis to validate relevancy
- Understanding business units or departments and how they interact; and
- A defensible litigation hold process which
 - Identifies key custodians
 - Must be more than a one-time communication
 - Provides detailed instructions in written form to key people
 - Communication should route through the legal team
 - Trains employees on compliance with the process and its importance.

Data Sources and Data Types

Proper ESI identification and collection is integral to a defensible litigation hold process. For an ESI data collection to be complete it must consider all relevant custodians, potentially responsive data sources, pertinent types of data, time frame(s), risks of the matter, litigation hold response plan, data collection methodology and project team communication plan.

The quantity and complexity of ESI data sources that may be potentially responsive to any given matter can be quite daunting. Utilizing an up-to-date data map or system inventory can make your job much easier. Below is a sample of data sources that should be considered:

1. Backup Tapes
 - a. Typically used for disaster recovery
 - b. Cost of data extraction for “standard” formats is declining rapidly
 - c. Difficult to search without a full restore
 - d. Not optimal for preservation efforts due to over preservation
 - e. Establish protocol to flag tapes being held for litigation hold and release tapes when no longer under hold
 - f. Not always organized or inventoried completely. Make sure you have a tape catalog or there will be extra processing requirements.
 - g. Need to understand what tapes exist and why
 - h. If potentially responsive data is on the tapes, they must be preserved unless they are excluded from preservation obligations via Rule 26(f) conference and Form 35
2. Desktops, Laptops and Data Protection Systems
 - a. Can contain millions of pages of electronic data

- b. Beware of email archives. An IT decision to limit mailbox size and promote local archives can create an unknown volume of data.
 - c. Active files are most commonly retrieved, with recovery of deleted items and full forensic analysis being less common
 - d. Documents, spreadsheets, presentations and PC based databases create unique challenges with embedded data, track changes history and complex metadata
 - e. Depending on matter, forensic imaging may be the safest approach
 - f. Shared computers create challenges in determining who the data belongs to
 - g. Never recycle computers without wiping them clean
 - h. Data protection systems create online backups of “documents” at 3rd Parties
3. File Servers, Document Repositories, SharePoint Sites, etc.
 - a. Commonly requested in nearly all matters
 - b. Need to understand access controls for shared data to help control growth and validate ownership
 - c. Home directories, departmental shares, workgroup sites
 - d. Don’t recycle network users ID’s as this will complicate “who” owns what data
 - e. Be careful with deleted data – Microsoft servers delete immediately while Novell servers can be configured to retain deleted items
 - f. Terabytes and even petabytes of data are possible. Enforce document retention policies to alleviate most volume issues.
 4. Email Servers & Email Archive Systems
 - a. Microsoft Exchange
 - OST, PST, EDB file formats
 - User archives are PST format and can be stored anywhere a file can be saved
 - Preservation from EDB may be best handled by export to PST
 - OST – offline storage file that needs to be converted to PST
 - Very few issues with accessing data, but local PST’s may be password protected
 - Most common format; many native file review tools exist that support this
 - b. Lotus Notes/Domino
 - NSF file format
 - Archives are NSF format too and can be stored anywhere a file can be saved
 - Individual mailboxes can be easily collected
 - Can be encrypted and password protected. Requires an ID file to decrypt.
 - Can contain much more than email
 - c. GroupWise
 - Server-based, “Hit the Road”, archives - need Novell server and WPDomain file
 - Less common and most difficult to process. Typically converted to PST format prior to searching.
 - Important to know versions of Novell and GroupWise is involved.
 - d. Email Archive Systems - 3rd party tools (e.g., KVS, Zantaz, Nexic, etc.) that typically preserve email data.
 5. Database Servers
 - a. Can exist in many forms, but are commonly in the form of Microsoft SQL, Oracle, Informix, DB2, and MySQL

- b. Data is in a constant state of flux.
 - c. Transaction logging may be required for ongoing preservation, but very case specific.
 - d. Some data may be exported for analysis, but typically the full system is required for queries to be comprehensible. IP disclosure may be of concern.
6. Non-Email Application Servers
- a. Accounting & Human Resource Systems - Usually proprietary software with database for storage.
 - b. Internet/Intranet Sites - Not usually requested, but may contain responsive data in program code or database system.
 - c. Instant Messaging - Corporate instant messaging systems range from no logging to complete logging with backup tape retention. Know your policy! Financial traders are required to retain this data per SEC regulations.
7. Voice Mail, Voice Recording, and Call Recording Systems
- a. Being requested more frequently.
 - b. Usually have very short retention time periods unless specific action is taken.
 - c. Data is commonly stored in a proprietary format.
 - d. Depending on the system, conversion may not be an option.
 - e. May need to collect via “in-line” recording device.
 - f. Traditionally, recordings were turned into text files; however, new tools are evolving that allow for searching with no conversion.
8. Phones, PDAs, BlackBerries, Smart Phones and Portable Storage Devices
- a. Need to understand which of these is supported and allowed, as they have the ability to hold vast amounts of data.
 - b. Portable phones, digital assistants, MP3 players, USB hard drives & “Thumb” drives
 - c. Compact Disks, DVD Disks, Floppy Disks
 - d. Qualify these devices during your custodian interviews to document the lack of, or presence of, potentially responsive data. Depending on the matter, it may not be enough to just ask, you may need to collect or sample to be sure.
9. Industry specific systems that may not store data in a centralized data store (e.g., medical devices)

Below are types of data information to be aware of:

- 1. Active Files – Word, Excel, PowerPoint, email, databases, voice recordings, temporary files
- 2. Metadata – internal and external to files
- 3. Encrypted files, password protected files & hidden files
- 4. Deleted files & file fragments within slack space and free space
- 5. Internet history, print history, USB drive usage, link files, system registry entries

Preservation/Collection Methodologies

Understanding the methods for ESI collection is critical to ensuring a proper defensible collection. There are four basic collection methodologies that can be deployed depending on the risks and needs of your matter. These are “drag & drop,” active data copy, forensic image capture, and backup tape capture.

The least desirable method is “drag & drop.” With this method, users or IT manually copy files and email to a folder or external media for further processing. This is NOT advisable as some metadata is changed during the copy process and no systematic logging of what is or isn’t copied is possible. Active data copy

is a much better approach as it preserves all the metadata and systematic logging of the process is possible. This method utilizes commercial tools (e.g., RoboCopy or Vice Versa Pro) and is usually performed by knowledgeable IT staff or consultants. Depending on your needs you may need to perform a forensic image capture. This results in a mirror image of the electronic media that captures both active and inactive (deleted or fragmented) data along with proper systematic logging and validation. The final method is backup tape capture. This is equivalent to the active data copy method, but the copied data is stored on electromagnetic tape. The problems associated with backup tape capture are that the tapes are slow, susceptible to damage, can be costly to restore, and often result in over-preservation.

Risks in the Preservation and Collection Processes

- Delay or insufficient communication in providing notice to custodians
- Lack of understanding of IT systems and organization, data repositories, and retention, destruction and recycling processes
- Over-preservation or lack of specificity of data that should be preserved
- Inadvertent destruction of documents (safe harbor?)
- “Rifle” vs. “Shotgun” approaches – not being broad enough
- Internal IT professionals vs. outside experts
 - Cost/time savings vs. risk mitigation
 - Extent of capabilities
 - Perceived bias
- Not establishing chain-of-custody
- Not following industry standards

Case Law Examples – Pitfalls of Inadequate Preservation and Collection

Qualcomm Inc. v. Broadcom Corp., Case No. 05cv1958 (BLM) (S.D. Cal. January 7, 2008)

The court ordered Qualcomm to pay all of Broadcom's litigation costs — around \$8.5 million — for "intentionally with[holding] tens of thousands of decisive documents from its opponent in an effort to win this case and gain a strategic business advantage over Broadcom." In addition, the attorneys most heavily involved were referred to the California State Bar for violations of their ethical duties.

The district court was particularly concerned with upholding the good faith standard necessitated by the discovery system and emphasized that for the system to work in a time when documents are stored electronically, "attorneys and clients must work together to ensure that both understand how and where electronic documents, records and emails are maintained and to determine how best to locate, review, and produce responsive documents."

American Express Travel Related Services Company, Inc. vs. Vinhnee (2005)

Vee Vinhnee won his case without even attending the trial. The Court refused to admit electronic evidence because American Express failed to defend the processes, people and technology used to preserve and authenticate the electronic bills in question, nor could it adequately disprove that its business records could have been altered from the time they were generated until the time of the trial.

Samsung Electronics v. Rambus, 439 F.Supp.2d 524 (E.D. Va. 2006)

Echoes the criticism of cursory compliance efforts including the misplaced reliance on custodian self-collection, stating that “[i]t is not sufficient ... for a company merely to tell employees to ‘save relevant documents’ ... this sort of token effort will hardly ever suffice.” The Court determined that the defendants’ lack of consistent systematic and effective processes to collect and preserve relevant ESI demonstrated spoliation of evidence.

NTL, Inc. Securities Litigation, 2007 WL 241344 (S.D.N.Y. Jan. 2007)

The Court imposed severe sanctions, including adverse inference instructions, attorney fees and costs upon discovering the defendant and related entity lacked a defensible process to preserve and collect ESI. Upon reviewing the steps taken to preserve and collect ESI after litigation commenced, the Court determined that the named defendant was grossly negligent because “[t]he evidence, in fact, [showed] no adequate litigation hold existed...” Although the defendant had circulated two document-hold memoranda, the Court faulted the adequacy of the overall process, noting that many employees never received the memoranda and that no concerted effort to collect the relevant ESI took place.

Wachtel v. Health Net, Inc., 2006 WL 3538935, (D.N.J. Dec. 2006)

The Court found that “Health Net’s process for responding to discovery requests was utterly inadequate . . . Health Net relied on the specified business people within the company to search and turn over whatever documents they thought were responsive, without verifying that the searches were sufficient.” The Court made clear that having a paralegal merely email preservation notifications is insufficient, noting that “Despite the document hold, thousands of employees’ emails failed to be searched.” The Court found that “even when [defendant’s] employees could search their emails, their searches were sporadic rather than systemic.” The Court, concluding that these failings constituted bad faith, imposed harsh evidentiary and monetary sanctions.

Preservation and Collection Best Practices

- Golden Rules
 - Identify your risk tolerance
 - Aim for rule of reasonableness
 - Know that data is susceptible to deletion
 - Assume email will always be targeted
 - Document communications and decisions
 - Determine in which situations it make sense to bring in a 3rd-party expert
 - Assume mistakes will happen
 - Communicate your Form 35 preservation commitments to your team and validate that they are being met
- First Steps
 - Designate an IT contact for discovery response
 - Identify sources of potentially responsive data (“the data map”) in advance of litigation
 - Establish defensible Litigation Hold procedures
 - Document and make available policies and procedures regarding document retention/destruction, data backup and tape recycling, computer usage, etc.
 - Get educated about your systems, discovery response processes, and production capabilities

Nancy F. Atlas

Nancy F. Atlas was appointed a United States District Judge for the Southern District of Texas (Houston Division) in August 1995. Before her appointment to the Federal bench, Judge Atlas was a Shareholder and Director of the law firm of Sheinfeld, Maley & Kay, P.C. in Houston, Texas, was a law clerk in the Southern District of New York, an Assistant United States Attorney in New York City, and as an associate with the New York law firm of Webster & Sheffield. Judge Atlas graduated from Tufts University (1971) magna cum laude, Phi Beta Kappa, and earned a Juris Doctor from New York University School of Law (1974). Judge Atlas serves on the Judicial Conference of the United States' Committee on Judicial Security and chairs that committee's Subcommittee on Strategic Planning. Judge Atlas chaired the Southern District of Texas Committee that drafted the Local Patent Rules. She also was instrumental in drafting the District's Alternative Dispute Resolution Program and serves as the Chair of its Standing ADR Panel of Neutrals. Judge Atlas has been active in leadership of the ABA Section of Litigation (SOL), having served on its governing Council, co-chaired its 2007 Annual Conference, co-chaired its ADR Committee, co-chaired a task force that drafted Guidelines on Multi-Jurisdictional Practice, served on a task force that worked on ABA Standards for Mediators, and as a speaker at dozens of legal education programs. Judge Atlas now is a member of the ABA's Standing Committee on Federal Judicial Improvements. Among other bar association activities, Judge Atlas has served as a Director and Treasurer of the Houston Bar Foundation, a Council Member of the State Bar of Texas's Section of Alternative Dispute Resolution, and the Co-Chair of that the Section's committee that drafted the Texas Ethical Guidelines for Mediators. Judge Atlas also co-founded, was a Director of, and served as Vice President of the Houston Chapter of the Association of Attorney-Mediators, Inc. Judge Atlas has been a member of the American Law Institute since 2001. Judge Atlas also has been active in community affairs. She served as Chair of the Texas Higher Education Coordinating Board (1992-95) (a gubernatorial appointment); a founding member of the Board of Victory, a fundraising arm of the Houston Branch of the American Cancer Society; and a Board Member, Vice President and Treasurer of the American Jewish Committee in Houston. Judge Atlas is a frequent lecturer on litigation and alternative dispute resolution topics.

Bob Dibert

Bob has litigated commercial transactions and business relationships for more than 20 years, including banking, contracts, employment terminations, joint ventures, and securities transactions. He also has litigated cases arising under federal and state civil rights laws, and both civil and criminal cases involving the federal Racketeer Influenced and Corrupt Organizations (RICO) statute. Bob also has more than 15 years' experience in the identification, preservation, production and analysis of electronically-stored information in a variety of investigative and litigation contexts.

Katie Jensen

Katie Jensen is an Associate Director in the Disputes & Investigations Practice of Navigant Consulting's Chicago office. Katie's main focus has been on assisting clients in the discovery services and data analytics litigation process. She has helped clients respond to large scale Antitrust Second Requests, SEC investigations, Class Action suits, and employment litigation. She has worked in all aspects of the discovery lifecycle for clients including, coordinating electronic document collections, data filtering and de-duplication, document processing, review, production and quality control of data sets for a significant number of productions. Katie has also done data analytics for a hedge fund bankruptcy matter, which included large data conversion and recreating report code.

Antonio Matthews

Antonio L. Matthews, of counsel in the Memphis office, concentrates his practice in the area of litigation. His primary areas of experience include business transactions and litigation, including insurance defense, contract actions, bad faith, products liability, premises liability, workers' compensation actions and employment contract disputes. Other experience includes engaging in all phases of litigation, from the inception of the case through the appellate process. Mr. Matthews drafted a winning brief in a \$1.6 million reasonable compensation case. In law school he was a member of the Moot Court Board and Black Law Students Association. He also received the Certificate of Outstanding Achievement in Appellate Argument.

Amy L. Tenney

Amy L. Tenney is a partner in the Washington, DC office of Jenner & Block LLP. Amy's litigation practice includes copyright litigation, qui tam matters, and products liability cases. For several years, she has also routinely counseled

*ABA Section of Litigation Annual Conference, April 16 – 18, 2008:
The “Litigation Hold” and Other ESI Moves*

clients on electronic discovery issues, including computer forensics and, more recently, the electronic discovery amendments to the Federal Rules of Civil Procedure. Amy's work in this area includes devising and implementing non-litigation document retention policies and data preservation plans. In addition, Amy works with vendors and clients to devise plans for the efficient collection, review, and production of electronically-stored information. Amy graduated from the University of Maryland with high honors and received her J.D., magna cum laude, from New York Law School. Following law school, she clerked for the Honorable Leonie M. Brinkema, U.S. District Court, Eastern District of Virginia (Alexandria Division), and the Honorable Frank M. Coffin, U.S. Court of Appeals, First Circuit, in Portland, Maine.