

Understand Legal Hold Notification Changes

The rule changes are almost here. Follow these recommendations to establish and communicate a defensible legal hold.

By Neil R. Packard, eDiligent president and CEO

E-DISCOVERY ADVISOR
Doc # 18524
2006 Issue 6
Length 4.5 pages
On page 14 of the magazine.

In an effort to clarify and combat continued electronic discovery failures, one of the Judicial Conference's Advisory Committees' amendments, deleted the term "data compilations" -- a vague term introduced to the federal rules as a means of addressing changing technology, from Rule 26(a)(1)(B) because, "The term "data compilations" is deleted as unnecessary because it is a subset of both documents and electronically stored information." The proposed Federal Rules of Civil Procedure (FRCP) Rule 34(a), lists data compilations as a subset of documents and "electronically stored information (ESI)" subject to production. "ESI" re-defines electronic evidence, encompassing computer-based information formats and incorporating flexibility for future technological changes and developments. Skirting discovery of ESI, substituting inexpensive electronic storage for Records Management, and scorched-earth retention policies are avoidance practices headed for extinction. Aspects of Discovery are evolving, however, even with the imminent implementation of the amended Federal Rules (December 1, 2006), the core-essence of discovery remains unmarred.

The catalysts of discovery's evolution stem from the ever-expanding sources, locations, and formats of discoverable material. In the past, you could control the majority of documents easily; they were stored in a few definable locations and existed in one simple format (paper).

The information technology (IT) revolution fostered the birth of electronic evidence discovery, opening document control to the masses, and scattering electronic-evidence across countless locations and diverse electronic formats. Company file storage systems expand exponentially and e-mail systems have become document repositories, a function never accounted for by their designers. Information resides in: databases, individual workstations, portable devices, and even employee home computers. Company policies do little to deter individuals from circumventing procedures. Case in point: The Veteran's Administration is mailing approximately 26.5 million letters to veterans informing them of potential identify-theft. Why? A VA employee violating Administration policy, taking home a laptop containing veterans' social security numbers and medical information, had his home burglarized and the portable device stolen, so much for policy enforcement.

Communication

Technology introduces a new, evolving, and complex level into e-discovery. Regardless, companies are responsible for communicating, coordinating, and controlling the chaos. A significant number of court opinions address the preservation and legal hold duties of a company, and recently counsel; alert every individual and entity of their preservation and retention obligations (National Ass'n of Radiation Survivors v. Turnage, 115 F.R.D. 543, 57 (N.D. Cal. 1987); Procter & Gamble v. Haugen (D. Utah 1998) 179 F.R.D. 622; Prudential Ins. Co. of America Sales Practices Litigation, supra, 169 F.R.D. at 598; Linnen v. A.H. Robins Company, Inc., supra, 10 Mass.L.Rptr. at 189; United States v. Koch Industries Inc., supra, 197 F.R.D. at 463; Old Banc One Shareholders Sec. Litig., 2005 WL 3372783 (N.D. Ill. Dec. 8, 2005)). In the prominent UBS Warburg v. Zubalake, Judge Scheindlin issued an opinion, addressing communication breakdown and compliance with discovery obligations. While her honor acknowledged UBS's counsel basically met their obligation when communicating the client's duty to preserve digital data, counsel's flaw was failing to communicate with the client's IT personnel. Additionally, she indicated a statement buried in an engagement letter might not meet counsel's duty of informing clients of preservation and retention obligations.

Direct communication with every source and custodian of relevant information is crucial and establishes a solid and defensible e-discovery foundation. Direct communication between all key players caught up in active litigation or a government investigation is not a suggestion; courts demand established preservation protocols: initializing, monitoring, and enforcing information preservation and clear legal hold

communication. (For more on pre-trial communication, see the sidebar Are You Prepared for the Pre-Trial Conference?) Most parties involved in a litigation or government investigation have experienced or read about situations where executive management insisted they have collected and provided all responsive documents (paper and ESI); only to have vital (responsive) documents materialize at a later date. Digital data intensifies this scenario a thousand-fold. Management or their agents miss responsive documents for assorted rationalizations:

1. Unaware it existed
2. Cursory searches
3. Withheld existence of the legal action from pertinent employees, in a vain attempt to cover up the issue fearing: public scrutiny, shareholder wrath, and economic impact on the company
4. Inadequate communication resulting in loss or destruction of ESI. Actions (and non-actions) negating counsels' due diligence efforts, damaging and discrediting the case in the eyes of the court

In Information Nation, Seven Keys to Information Management Compliance (Randolph A. Kahn, Esq. and Barclay T. Blair, AIIM International, March 1, 2004), the author's address Legal Hold notification:

"...organizations need a mechanism (commonly referred to as a Legal or Records Hold mechanism) to inform employees of the need to preserve information."

Some business and legal professionals, with eyes shut tight, hope the elephant leaves the room. In the movie "Jaws," Hooper's response to Mayor Vaughn's denial of a [shark] problem, "I think that I am familiar with the fact that you are going to ignore this particular problem until it swims up and bites you on the ass." This sums-up the mind-set of a large number of complex litigation and federal investigation participants.

Executing effective, reasonable, and direct communication with every individual, minimizes risk, eliminates miscommunications, and resolves perceptions of due diligence neglect. Technology-driven business environments demand that management communicate directly with custodians possibly possessing relevant information and identify their sources. Today, custodians can literally be every individual within a company with sources spread across the company's information network and geographical locations. While the global scenario is possible, identification of custodians and related sources can produce a more refined scope. However, defining the scope of relevant participants and information is dependent upon the nature of the legal action and the company's records management initiative. A generic, broad statement, broadcast throughout the company, falls short of preservation and legal hold obligations.

Technology, the enigma plaguing companies and law firms, is the cure. Turning technology on itself, while instilling a perverse sense of gratification, allows companies and counsel to:

- Promptly inform all relevant custodians and sources.
- Relay explicit preservation obligations.
- Suspend detrimental (standard) business retention and destruction policies.

Legal hold methods should blend with a company's culture and establish reasonable notification and preservation measures. Automation of legal hold notification reduces a company's cost and exposure, eliminating probable dire judicial and financial consequences associated with failing the preservation and retention of relevant information. Technology's adaptability provides the tools necessary and creates reasonable cost-effective answers with intranets, the Internet, collaboration methods, and even e-mail, offering viable delivery platforms.

Preservation and legal hold procedures

E-discovery mandates companies institute reasonable preservation and legal hold procedures. The dynamic nature of technology, coupled with the unique characteristics of legal proceedings, requires analysis and evaluation. To fine tune a legal hold notification, you must identify the extent of a matter, account for the company's needs, and balance them with the magnitude and financial impact of the legal action, basically performing legal risk management.

A legal dispute's uniqueness (every case is different), controls the scope of a company's' responsibilities. Companies must implement measures, forming a Response Plan (detailed later in this article), and account for the financial impact that includes:

- E-discovery hard-costs
- Secondary costs including: damages for non-compliance, for disregard and/or failure to preserve electronic evidence
- Soft-costs arising when complying with preservation obligations including: productivity losses and interference with a business' normal operations, intangible external costs resulting from publicity, reaction in the financial market, or retaliatory actions from share-holders.

Executive management and counsel must address these factors and assess the company's potential exposure.

Standardizing the legal hold process is not lacking issues of its own. A legal hold program must remain flexible and adapt -- dependent on the nature of the matter and the technology involved. The complex natures of technology, law, and of the utmost, human beings, makes a single boilerplate solution impracticable, and sole reliance on policies ineffective (remember the VA employee). Setting aside the different complexities involved, there are guidelines for building a practical preservation and legal hold framework. For more on preservation and legal hold procedures, see the sidebar *Be Careful What You Ask For, Because You Will Get It!*

General notification

Executive management must lead the charge, employees listen when the boss speaks. Spell out, in plain English, the employee's responsibilities, convey specifics on documents and information required, impart unique responsibilities based on the employee's role in the legal matter, and their function within the company:

- Describe the legal action's background and applicable time-frame.
- Identify information (paper and electronic) subject to preservation.
- Specify:
 1. Pertinent data-types and their associated applications
 2. Electronic and paper document preservation and retention methods
 3. Preservation (manual or automated) tools, and how to use them.
- Assign and communicate specific points-of-contact for employees who:
 1. Have questions or need additional information.
 2. Seek help with data preservation tasks.
- Inform employees of their legal obligations, including ramifications and penalties for non-compliance.

Key custodian notification

The following are categories of custodians a company might have:

- Custodians possessing or having unique knowledge and information require a more detailed assignment of tasks:

- Human Resources must identify former (potential source) employees.
- Records Management must suspend normal (standard) destruction procedures and preserve relevant documents.
- Information Technology, perhaps the most volatile area, must be informed and given clear instructions on appropriate actions. A general "save data" statement isn't enough and produces any number of "solutions," each potentially producing consequences.

Compliance

Companies should establish reasonable measures for monitoring, and following up with every key player to ensure they comply with legal holds and preservation. When designing a notification system, you should consider authenticating the steps taken by the company and validating compliance with its preservation duty, demonstrating "good faith" preservation efforts. Validation protocols include:

- Sending key players periodic reminders of their obligations
- Informing employees of additional responsibilities as the scope of the legal action changes
- Instituting tracking and audit capabilities, recording actions, and combating repudiation
- Retaining the messages or notifications sent to employees describing their legal obligations and responsibilities
- Assessing requiring relevant personnel certify preservation and retention actions

A large number of companies are unaware of the full extent of retrievable information within their possession. If the creation and implementation of a preservation and legal hold notification program falls under a company's purview, validating the program is counsel's responsibility. Counsel must authenticate a corporation's actions and ensure those actions are defensible and judicially acceptable.

The extent of counsel's duty varies, depending on facts and context of each legal action and the client's level of preservation protocols. Counsel's review of a legal hold program must be vigilant and account for legal and situational variables. The paradigm shift from paper to electronic and e-discovery's hype, may distract the plan's architects into overlooking paper. Counsel must ensure all discovery aspects are combined within one response plan. Counsel's review of procedures examines its weaknesses and strengthens the company's preservation practices. Counsel's responsibilities include initiating the business' preservation of digital data. When the duty to preserve is triggered, a subject of contention continually argued in the courts is that activating a company's preservation obligation requires the knowledge and experience of counsel, placing activation ownership on their shoulders.

Education

A communication method frequently missed is employee education. Companies, with guidance from counsel, must indoctrinate employees on their preservation and retention responsibilities, providing periodic refresher training and mandatory seminars on new or revised legal requirements. They must specifically train key departments: Records, Legal, HR, and IT personnel, on the company's legal hold policies, and their exclusive preservation and compliance responsibilities.

Party's over

When a legal action concludes, send employees a Legal Hold Termination Notice, reinstating regular retention policies and procedures. One caveat is the preserved information may be responsive to other legal matters requiring continued preservation of information. Establish methods of cross-referencing the information from a completed matter with active or potential future legal actions. While the urge to delete the information exists, don't rush the destruction of information (evidence).

Establish and validate procedures

There are a number of companies and consulting companies experienced in establishing legal hold compliance programs. Information Systems Audit and Control Association, www.isaca.org, is a valuable resource for establishing and validating procedures and protocols. Business' dependence on digital data and the legal system's increasing awareness of electronic evidence direct implementation of data preservation and legal holds. Compliance imposes specific responsibilities, compelling a joint team effort that:

- Combines the expertise and capabilities of the company
- Implements sound process and procedure
- Includes counsel's validation and continued involvement

Following these guidelines will ensure you have a reasonable legal hold program with actions that are acceptable and judicially defensible.

Are You Prepared for the Pre-Trial Conference?

A benefit of proper legal hold and preservation measures is applying the results in later stages of a legal proceeding. The pending FRCP amendments and subsequent state court adaptations, establish a link between legal holds and the pre-trial conference. Legal Professionals have a mandate -- gain an understanding of a client's systems, its strengths, weakness', flaws, and the amount and form(s) of electronic evidence. This understanding is the only way to achieve adequate representation of a client's interests. Information obtained during the legal hold and preservation phases will lay the groundwork for diligently defending the company against the opposing side's search for a chink in the armor. Absent information gained early on, proper preparation and research, potential pitfalls include: undue burden and expense on the client and counsel; sanctions, adverse judgments, etc., for misrepresentation or errors; and exposure to claims of malpractice.

Be Careful What You Ask For, Because You Will Get It!

The semantics of litigation increase exponentially, in proportion with the expanding list of custodians involved in a matter. Law and technology possess distinct terminology and rules, which when used improperly, can seriously damage the good-faith efforts of all those involved. Technicians must learn and comprehend the intricacies of evidence and the judicial system, legal professional's must learn the technical jargon, understanding exactly what they require of information technology professionals.

Ad hoc, unsupervised discovery efforts by management, IT departments, and counsel can sink a case before it even starts. This is a fact usually discovered much later, after expending significant time and money. In *Samsung Elecs. Co., Ltd. v. Rambus, Inc.*, 2006 WL 2038417 (E.D. Va. July 18, 2006), "The court found the defendant's vague litigation hold instruction to "not destroy relevant documents" did not satisfy preservation obligations," demonstrating the courts intolerance of half-measures. When requesting discovery, inaccurate or vague requests result in loss by all parties involved. On the other side, as many legal professionals have already learned; when dealing with technology, you usually get exactly what you ask for, but not what you wanted. As in law, there are terms in technology which have one specific meaning and those which have several diverse meanings, a point illustrated in the example below.

Counsel requests a "mirror image back-up" -- their intention is to preserve an exact copy (mirror image) of potentially relevant electronic information and ensure the integrity of the data. The result is a company's preservation of data being placed on backup tape media. This is an action that inevitably increases the costs of extracting responsive data, and could be argued in court as an attempt to hide evidence on inaccessible media. Why? Because when a technician hears "backup," it's a term most IT professionals associate with tape backup. In their eyes, a tape backup meets the request of "mirror image back-up."

In the same scenario, counsel notifies the IT department to preserve the companies e-mails and data for a legal matter. The IT department effort results in native files being copied (thus changing the metadata) to an external hard disk drive; the company's e-mails and databases placed on backup tape (inaccessible data) and the original data still exposed to change or deletion. In addition, the preserved data now resides on separate media formats, increasing search and retrieval costs.

A much larger group of custodians that cause concern, is a company's employees. When communicating legal hold obligations to these individuals, it must be in plain English, from both legal and technology perspectives. Sending a letter or e-mail informing staff: "Due to a suit filed by company XYZ, you are required to preserve and retain any relevant information," while short and to the point will result in a myriad of questions, responses, solutions, and of course chaos.

Resolving this issue requires efforts by all parties. Just as companies have Disaster Recovery Plans, they must design and implement a Legal Response Plan -- building the bridge before they come to it. There are a number of resources available to assist in this endeavor, and to assist counsel in drafting inclusive legal hold notifications. The Sedona Conference is expected to release a publication addressing legal holds in the near future, Michael Arkfield's Electronic Discovery and Evidence and the ABA's The Electronic Evidence and Discovery Handbook: Forms, Checklists, and Guidelines, address e-discovery topics and issues, as well as provide sample forms and letters.

Regardless of the source, the following best practices establish viable and defensible legal hold and preservation policies and procedures:

1. Execute a legal hold when the obligation to preserve is triggered.
2. Communicate directly with and clearly inform key players of their preservation obligations. Provide keyplayers with the complete picture. Explain in plain English the circumstances of the matter, facts in dispute, types of relevant information (e-mails, spreadsheets, etc.), internal and external points-of-contact, and potential repercussions for non-compliance.
3. Monitor and verify all key players are notified, understand, and acknowledge, their preservation obligations.
4. Communicate with IT personnel, gaining a sound understanding of pertinent information systems. Ensure they not only preserve data, verify they have suspended any and all automated processes which could inadvertently destroy information, until the data is collected or determined to be non-relevant. Counsel must learn how information is created, maintained, and destroyed, identify and account for accessible and inaccessible electronically stored information, and confer with technicians to devise cost effective and valid methods of data collection.
5. Communicate directly with key players ascertaining how and where they store data.
6. Become familiar with the company's record retention and destruction policies. Including determining if they were actively enforced and audited to ensure compliance, even a rock-solid policy will crumble in court if not maintained and monitored.
7. Implement "forensically sound" methods of collecting responsive data (not to be confused with computer forensics).

Remember, these are guidelines for building a solid foundation. You must tailor and expand preservation policies and procedures, addressing: applicable laws and regulations, a company's applicable industry and culture, and built-in flexibility, accounting for the changing worlds of technology and law.