

Implementing an Effective Federated Legal Hold Strategy

Ensure Preservation of Information to Meet Court Requests and Reduce Risk

The Legal Hold Requirement

The US Federal Rules of Civil Procedure (FRCP) and individual global legal systems duty to preserve requirements in relation to the submission of electronic evidence in civil procedure now means that organizations faced with litigation need an efficient means of preserving all potentially relevant Electronically Stored Information (ESI) information.

In the days of paper, “legal hold” typically meant making sure that no one went through the file cabinet shredding documents. Times have changed. Organizations need to adopt new strategies to prevent the inadvertent destruction of potential ESI evidence through automatic processes such as regular tape rotation, records management disposition schedules, mailbox management processes, and PC upgrades.

An effective preservation strategy includes:

- **Awareness** of all data, processes and procedures
- **Processes** in place that can pause potentially destructive operations such as tape rotations, disposition from records systems, mailbox or message deletion, and hardware recycling
- **Technology** to collect and protect all relevant information and place it on legal hold

The Scope of Electronically Stored Information (ESI)

The management of electronic records as evidence extends beyond just simple documents and files. The term Electronically Stored Information (ESI) relates to all the electronic content and records an organization may possess in relation to a litigation including e-mail messages, instant messages, word processing files, spreadsheets, presentations, purchase orders, contracts, wiki and blog postings, files stored in collaboration systems. ESI by its very nature is harder to preserve in today’s society which by definition means that organizations have a duty to preserve it in order to maintain its integrity as evidence.

Many inherent characteristics of ESI require its legal preservation, namely, ESI is:

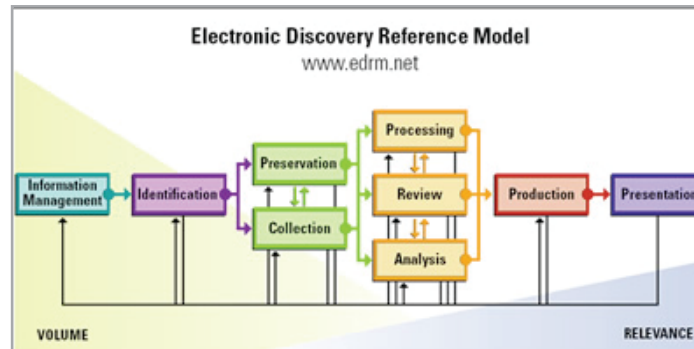
- normally stored in much greater volume than are hard copy documents.
- dynamic, in many cases modified simply by turning a computer on and off.
- incomprehensible when separated from the systems that created it.
- capturing non-apparent information, or metadata, that describes the context of the information and provides other useful and important information.

Amendments to the Federal Rules of Civil Procedures

In an effort to reduce the burden of electronic discovery on corporations, the Federal Judiciary has amended the FRCP. While many of the rules were amended, Rule 26(f) and Rule 26(b)(2)(B) have particular interest as they relate to executing an effective legal hold strategy.

The amendment to Rule 26(f) requires the discussion of issues related to preservation of discoverable information at the pre-trial conference. The amendment to Rule 26(b)(2)(B) provides organizations some relief from discovery and production of information that the “party identifies as not reasonably accessible because of undue burden or cost.” However, it does not reduce an organization’s obligation with respect to preservation as the “court may nonetheless order discovery from such sources.”

The Electronic Discovery Reference Model (EDRM)



CommVault, along with industry leading eDiscovery partners, offers a complete enterprise-wide eDiscovery solution as outlined in the Electronic Discovery Reference Model (EDRM), which is recognized as the industry standard framework for electronic discovery processes.

A Typical Discovery Scenario

Customer Challenge: A legal action involving seven employees is filed. The action includes all of the standard sources of Electronically Stored Information (ESI), such as e-mail, files, laptops and desktops, for a period of six months, containing any of fifteen search terms.

The Current Way: Legal notifies the seven employees that they are on legal hold and that they should not delete anything from the targeted period. Legal then tells IT to save the backup tapes for the six months in question. Once the data is on hold, legal asks the seven employees to search through their files and copy anything containing the search terms to the legal share. Time goes by. One of the seven employees and the backup operator leaves the company. Two employees get new laptops. Then the plaintiff adds additional search terms. The tapes are lost and three of the seven original datasets are gone. The organization now faces sanctions for spoliation (spoilage of the evidence) ranging from financial penalties to dismissal of claims or defenses.

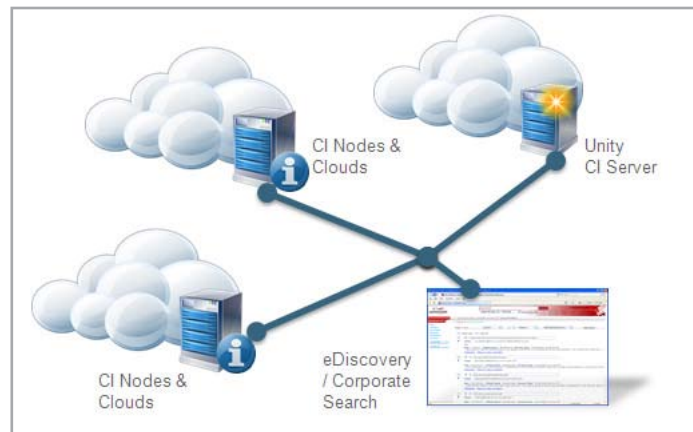
The Better Way: Legal notifies IT that they need to put seven employees' information on hold. Either IT or legal themselves define and execute search parameters that identify all the seven employees' information across backups and archives of their data. Through CommVault Simpana® software's unique eDiscovery interface, the data for the seven employees is secured and preserved regardless of location. It's as simple as that.

CommVault® Simpana® Federated Legal Hold

CommVault software's legal hold capability spans both archive and backup stores to help ensure information is preserved. By maintaining a legally defensible audit trail, these features allow customers to reduce the risks associated with non-compliance regulations such as the US Federal Rules of Civil Procedure (FRCP) for eDiscovery, as well as preserving the evidentiary integrity of content for court submission.

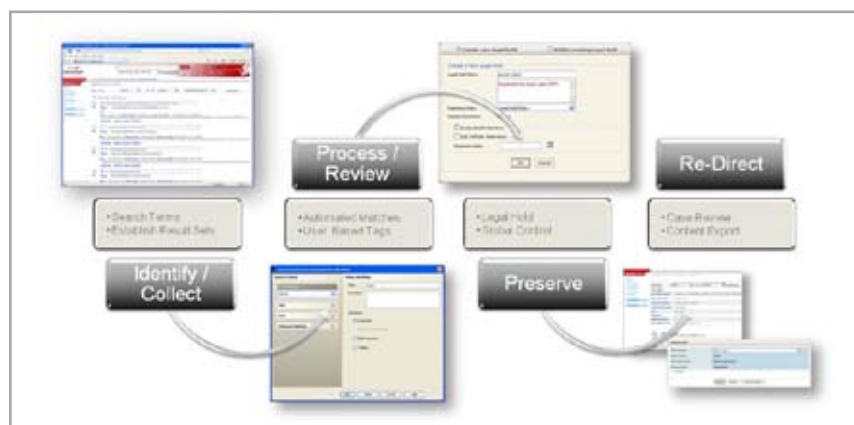
With powerful features and no need for additional licensing to enable a wide-ranging eDiscovery toolkit, the legal hold capability uses a comprehensive, automated approach to search and retrieve data from backups, archives or any Electronically Stored Information (ESI)—such as e-mails and files—and retain a subset of the data for long-term accessibility. CommVault legal hold helps customers defensibly preserve responsive information that may already be under multiple retention policies. CommVault's legal hold also embraces object level holds, beyond file-based, for a granular level of recovery for both vaulted backup sets and archives at the message or document level.

Post-hold considerations are also supported within the legal hold feature set, allowing post-hold data and content to be retained or removed as required.



All this is achieved across multiple data stores, sites and geographies. CommVault® Simpana® legal hold feature utilizes federated index and search technology that links globally to create a unique eDiscovery reference model that enables eDiscovery identification, collection and preservation from a single interface across information assets. These assets in individual sites and data stores are indexed by Simpana® nodes and the relevant nodes are linked into indexing clouds that span global configurations through a Simpana® Unity Indexing topology. The result—eDiscovery and legal hold from a single interface and legal point of interaction within an organization regardless of geographical boundary.

In addition, CommVault® Simpana® software's content workflow technology allows legal hold search patterns to be created that enable the automated promotion of relevant information content to a legal hold archive ensuring that not only existing but future risk and liability is managed again regardless of physical location.



It really doesn't get any simpler than this.

Legal Action Workflow

The illustration above highlights just how simple the CommVault® Simpana® Federated Legal Hold solution is enabling ad-hoc or pre-defined search patterns that:

1. Identify and Filter relevant results sets that highlight information assets that are both in scope of a litigation and, as a result, are at risk and need to be preserved.
2. Manage the review annotation and content classification of assets against defined legal matter categorizations.
3. Manually or automatically promote classify assets to a legal hold policy and physically secured archive that can be encrypted as required using CommVault® Simpana® encryption.
4. Re-direct held content to either CommVault® Simpana® software's review process, a specific case management technology (e.g. CaseCentral), or exported for ingestion into an in-house litigation system.

SIMPANA[®] software

CommVault[®] Simpana[®] Backup & Recovery, Archive, Replication, Resource Management and Search software is designed to work together seamlessly from the ground up, sharing a single code and common function set. This exclusive single-platform architecture enables unparalleled software efficiency, performance and reliability for unprecedented control over data growth, costs and risk.

Conclusion

CommVault[®] Simpana[®] software is one of the only true solutions to deliver federated legal hold across an organization to preserve all forms of relevant information when litigation is reasonably anticipated. Unlike traditional legal hold technologies which treat archives as a single entity and only tag messages located inside the archived storage pool, CommVault's legal hold feature searches and identifies information assets across both backups and archives, preserving data in all storage pools based on normal retention policies. Not limited to legal action, users abiding by internal governance rules can also leverage the legal hold feature set for adherence to company policies that mandate the retention and disposal of certain documents and information.

CommVault's unique Singular Information Management[®] approach to federated legal hold, specific features and benefits are made available to customers including:

- Indexing and Search technology that spans an entire organization facilitating legal hold through a single reference model and interface.
- Advanced search result views which allow users to organize and classify information, annotation and refine search results.
- Powerful filters that enable users to quickly identify and reduce the number of files and e-mail messages needed for review to make better legal decisions, meet deadlines and avoid sanctions.
- Giving users the ability to save queries and control how results are displayed. This allows relevant items to then be easily designated for legal hold where collections are defined by case-specific retention rules.
- Flexible post-hold management capabilities allowing the reclassification, consolidation and/or timely destruction of held content, regardless of infrastructure.

CommVault's unique, single architecture reduces the amount of data repositories that need to be searched in response to litigation. From a single console, meet eDiscovery and compliance challenges with powerful search, retrieval and management of all ESI.

For More Information on CommVault eDiscovery:

www.commvault.com/ediscovery



www.commvault.com ■ 888.746.3849 ■ E-mail: info@commvault.com

CommVault Worldwide Headquarters ■ 2 Crescent Place ■ Oceanport, NJ 07757 ■ 888-746-3849 ■ Fax: 732-870-4525

CommVault Regional Offices: United States ■ Europe ■ Middle East & Africa ■ Asia-Pacific ■ Latin America & Caribbean ■ Canada ■ India ■ Oceania

©1999-2009 CommVault Systems, Inc. All rights reserved. CommVault, CommVault and logo, the "CV" logo, CommVault Systems, Solving Forward, SIM, Singular Information Management, Simpana, CommVault Galaxy, Unified Data Management, QiNetix, Quick Recovery, QR, CommNet, GridStor, Vault Tracker, InnerVault, QuickSnap, QSnap, Recovery Director, CommServe, CommCell and ROMS are trademarks or registered trademarks of CommVault Systems, Inc. All other third party brands, products, service names, trademarks, or registered service marks are the property of and used to identify the products or services of their respective owners. All specifications are subject to change without notice.