

Reduce the Cost of Discovery with Data Archiving

According to an ESG survey of 206 companies, 77% reported that e-mail and 50% reported that office documents had been requested as part of a legal or regulatory action.¹ This is precisely why e-mail and files are front and center for every eDiscovery discussion. This is also why organizations need a way to quickly and easily assess the risk contained in their electronically stored information before deciding if they should go to court.

There are three main schools of thought on archiving: archive everything to ensure you have it all, archive a subset of critical mailboxes, or allow end-users to select what to archive. Most organizations archive a subset of critical mailboxes or frequently litigated users, with remaining users put under quota to control storage consumption. This provides the ability to respond to discovery requests without the cost of storing unnecessary information and the risk of keeping larger amounts of data for longer periods of time. It is still a challenge, however, to find the right balance between cost, risk, and legal requirements.

In response to these challenges, and in an attempt to reduce the burdens associated with electronic discovery, the Federal Judiciary Committee amended the FRCP in December 2006. Although these changes have been in effect for two years, many organizations continue to be confused about the FRCP amendments and their impact on discovery and document production. Numerous rules were amended, but Rule 34(a) and Rule 34(b) have particular interest as they relate to the scope of discovery and the form of production.

Amendments to the Federal Rules of Civil Procedure

The amendments to Rule 34(a) create a new class of legally relevant data, ***“electronically stored information (ESI)—including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations stored in any medium...*”** Rule 34(a) also mentions the idea of testing or sampling a collection of the total dataset in an attempt to determine if additional discovery/production is required. This is done to reduce the cost and time required to review the extraordinary volumes of electronic information. The amendment to Rule 34(b) addresses the appropriate form and forms of production, defaulting the form of production to ***“a form or forms in which it is ordinarily maintained or in a form or forms that are reasonably usable.”***

In response to these rules, organizations that are faced with frequent litigation need a strategy that allows them to manage their ESI and be able to protect and produce it in its native format. CommVault® Simpana® software provides organizations with tools and techniques to collect the relevant business records, while minimizing the unnecessary growth, cost, and risk associated with keeping everything for everyone.

A Typical Discovery Scenario

Customer Challenge: A heavily litigated organization may face 7-10 lawsuits every month, plus at least that many internal audits. These incidents can range from two employees to an entire division. All of the requests require e-mail and files.

The Current Way: In response to frequent and overlapping preservation requests, the organization adopts an infinite tape retention policy, and hires a team of five consultants to retrieve tapes and restore servers. For both e-mail and files the whole server must be restored before the necessary information can be extracted because the organization uses snapshot backups to protect their environment. Once the server is restored and the necessary data is extracted, it is then searched with a desktop search engine for keywords. The results are gathered and placed into a zip or PST file for legal. The team of five continues this operation continuously, frequently having to restore the same data multiple times, as different cases need the same server, or the legal team changes the search criteria. After operating in this fashion for several years the organization has wasted both time and money and could potentially face sanctions for not having an auditable chain of custody.

The Better Way: CommVault offers a wide range of easy to implement preservation, collection and identification strategies to more effectively deal with frequent discovery requests:

- **Collect, archive and content index all journaled e-mail for a collection of users or for the entire organization**
 - CommVault software allows an authorized IT admin or legal representative to perform keyword searches directly on archive data, and to directly restore relevant messages into an audited mailbox for further processing, cutting discovery time in this example from a day or weeks with an entire team down to hours with a single user.

¹ ESG Research Report: Digital Archiving: End-User Survey & Market Forecast 2006 – 2010, March, 2006.

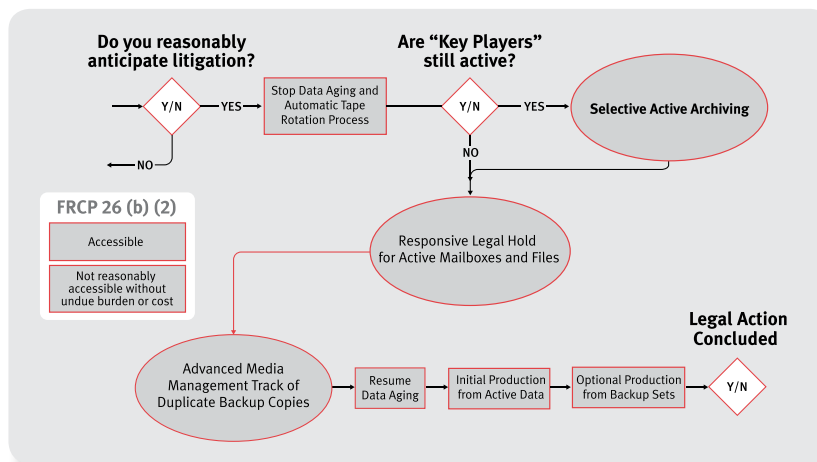


Rule 34. Production of Documents, Electronically Stored Information, and Things and Entry Upon Land for Inspection and Other Purposes

(a) Scope. Any party may serve on any other party a request (1) to produce and permit the party making the request, or someone acting on the requestor's behalf, to inspect, copy, test, or sample any designated documents or electronically stored information—including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data complications stored in any medium from which information can be obtained; translated, if necessary, by the respondent into a reasonably usable form...

(b) Procedure. The request shall set forth, either by individual item or by category, the items to be inspected, and describe each with reasonable particularity... The request may specify the form or forms in which electronically stored information is to be produced. Without leave...

(ii) if a request does not specify the form or forms for producing electronically stored information, a responding party must produce the information in a form or forms in which it is ordinarily maintained or in a form or forms that are reasonably usable; and (iii) a party need not produce the same electronically stored information in more than one form.



■ Enable employees to archive messages on their own

- CommVault software enables employees to archive their own messages through an intuitive Outlook plug-in.
- A combination of standard Exchange mailbox management rules and CommVault policies ensures that messages are collected, protected and easily accessible as part of a discovery request.
- Outlook-enabled archiving can eliminate the need to create personal PST files, and can also increase retention within employee's folders by archiving and stubbing all messages that match the defined policy.
- CommVault software can also consume and process existing PST's into the archive to clean up storage, control data growth, and bring more data under compliant retention policies.

■ Archive and content index files from a variety of locations— Linux, Unix, Windows and NetApp file systems

■ Restore e-mail and files to any location for easier production of native format documents

Now when a new lawsuit, internal audit or corporate investigation is initiated, the legal team simply executes a search against the archive and exports the results. The organization is able to find the relevant information, produce the ESI in its native format, can illustrate a consistent and repeatable process, and has a complete audit trail of its activities. The combination of solid process, and both file and e-mail archiving technology from CommVault offers companies a variety of ways to meet the expectations laid out by the amendments to Rule 34(a) and Rule 34(b) of the FRCP.

Conclusion

CommVault® Simpana® software is the only product that delivers file, e-mail and document management across replication, backup and archive data as part of a proven and unified data management solution. 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

Get the facts: http://www.uscourts.gov/rules/EDiscovery_w_Notes.pdf

This information is not intended to be legal advice; customers should consult their own attorneys for an interpretation of the rules and requirements applicable to the subject matter hereof.



commvault
solving forward®

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