

Personal Email Archives: Do They Amount to IT Malpractice?

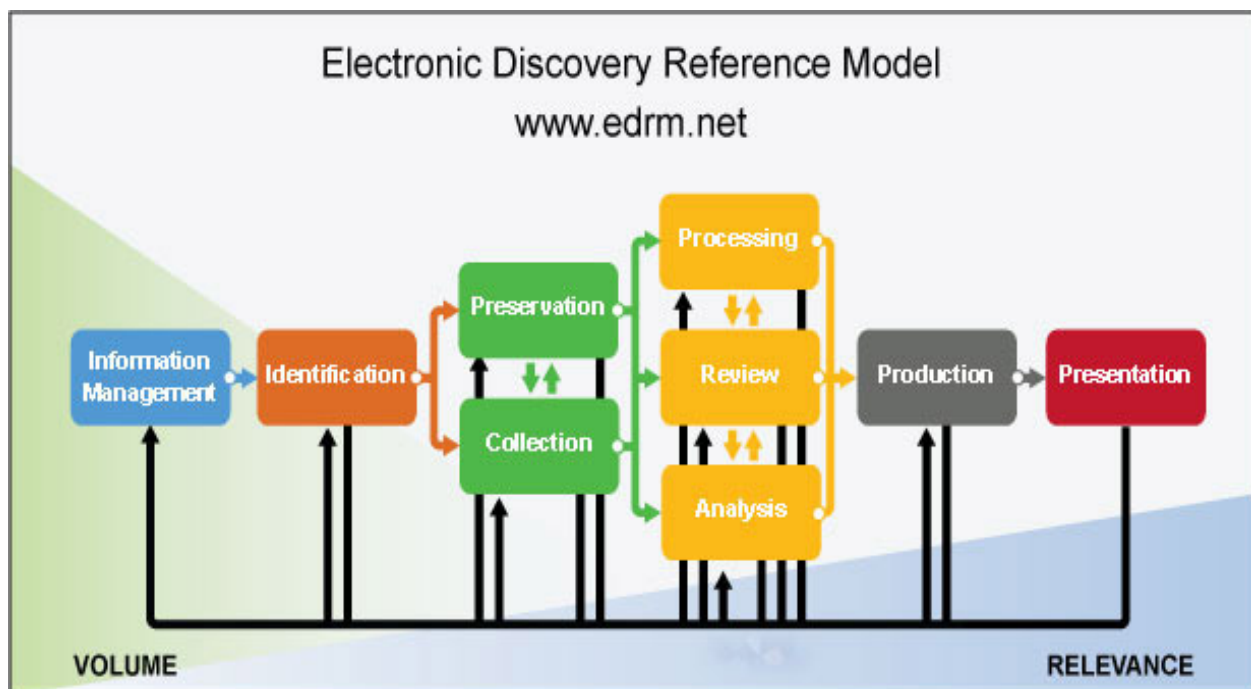
by Osman Baig, Messaging Architects

The amount of data within your messaging environment is constantly expanding as email communication continues to increase, replacing other types of communication. More messages each day, and message sizes that balloon due to large and numerous attachments. According to Gartner, the average number of email messages per user, per day has increased to over 130 messages and the average message size is over 100 KB. Many users will try to preserve between 1 and 2 GB of email data per year. In large organizations, this adds up to alarming figures for which email servers were never really designed.

In many cases, the response from IT has been to deploy complex, costly and fragmented email infrastructures just to keep up with the storage bloat. To further combat this growth, many organizations have also enforced stringent deletion rules such as 90-day retention policies. The behavioral impact resulting from these policies is often the premature deletion of potential business records or the use of personal archives to maintain data beyond the stated periods.

When personal archiving is used, it moves data off the organization's production servers and storage to a system-defined location that may include the user's local machine. The data is then no longer accessible from the corporate messaging system, resulting in idiosyncratic and highly-interpreted data retention, based on end users' perceptions of what should, or should not, be preserved. Trying to recover messages as part of an internal audit or litigation rapidly becomes a costly nightmare. All too often data simply cannot be found, or the organization runs the risk of losing critical information when PCs or laptops are refreshed.

In addition, personal archives are not storage efficient. Since they re-create copies of all attachments in each personal archive, data sizes are usually between double and triple of the original size. The increased data, combined with the inability to run centralized searches, adds stress to most discovery requests, which are typically on tight timeframes to begin with. Collecting, processing, reviewing, analyzing, and producing large sets of disparate personal archives for external parties becomes an expensive and error prone exercise in redundancy.



As part of most recent litigations, an organization's policy definition, as well as the consistency of the enforcement of this policy, is reviewed so as to identify alignment with legal requirements. When daily practices are found to be inconsistent with policies or compliance frameworks, or if relevant data is discovered in other storage locations, it rapidly opens the door to in-depth questioning of what the organization may be trying to hide, or if legal holds are being adequately respected. Attorneys are now well-versed in eDiscovery and have a very good understanding of the technology at play. Their objective will be to cast doubt on the preservation practices and the completeness of the data set provided – which if successful, can make the difference between winning a fair settlement and losing a case on technical deficiencies.

Legal Risk Exposure	
Probability	Consequences
VERY HIGH: If the data exists then it can be requested as part of the ediscovery. Federal Rule of Civil Procedure 37(d) considers it intentional obstruction of the discovery process if known and possibly relevant personal archives are not disclosed.	Financial impact of not providing access to personal archives can result in punitive fines, monetary sanctions and reimbursements **

**Reference material: GFI Acquisition, LLC vs. American Federated Title Corporation (<http://www.ediscoverylawreview.com/2010/04/articles/sanctions/obstruction-of-the-discovery-process-understanding-email/>)

This risk is compounded by the nature of the legal hold process itself. Was the hold applied when “reasonably anticipated” and were appropriate actions taken to preserve “all forms” of relevant information, which may include requests to include personal archives. Personal archives represent a subset of email that either was selectively or automatically maintained but is not necessarily captured at the time a legal hold is initiated.

Since personal archives effectively remove data from the corporate messaging system it may well also create questions about the effectiveness of the organization's legal hold process. If personal archives are part of the eDiscovery scope, this data will need to be handled appropriately. This may be stating the obvious, but in many cases the consequences and impact are not considered, and as a result fall well outside the organization's acceptable level of risk tolerance. The trend in litigation indicates a broadening definition of what is a record and what is considered relevant and discoverable. As with backup tapes, which at one

point were rarely requested as “in scope,” personal archives are now routinely considered a standard request.

Legal Risk Exposure	
Probability	Consequences
NORMAL TO HIGH: Possible that the “smoking gun” resides within personal archives. Possibility of spoliation charges.	HIGH: Risk of losing litigation based on the unknown or settlement when defensible position exists. Financial impact of not ensuring preservation of data may result in punitive fines or monetary sanctions.

Notwithstanding the philosophical debate which has been ongoing at the academic level, legal hold for email means really preserving all data from the point when “reasonably anticipated.” Thus it should include personal archives if the organization allows for this functionality to exist. Under those assumptions, the email data may be considered potential evidence and even unwillful destruction could be considered spoliation.

Technical Challenges	Comments
Requirements to maintain the growing number of personal archives	
Large personal archives run a high risk of corruption	
Collection of personal archives is a long and costly endeavor	

Things to think about:

1. Can you defend the effectiveness of your legal hold process?
2. If personal archives are requested, do you have a process to enable production?
3. For every “Send”, there is a “Receive.” What might opposing counsel have that you are not aware of?
4. Are you capable of determining if you should settle before having invested too much time?
5. Does your current setup provide the tools for effective legal strategy planning?

For your free 30-minute consultation on **Email Risk Management** and on how to attain a **Risk-Free Corporate Email Infrastructure**, call 1-866-497-0101