MAYER·BROWN

Electronic Discovery & Records Management

Tip of the Month

Managing the Risks & Costs of Electronic Data: "Defensible Deletion"

Scenario

For years, a large company has been effectively retaining the vast majority of all electronic data generated by its systems and employees. However, the company's records retention policy was originally designed and implemented with an emphasis on hard copy records, so its electronic systems are not designed to automatically implement its record retention schedules. As a result, the company largely relies on individual employees to enforce its record retention schedules when it comes to electronic data. In addition, the company faces frequent litigation and has a large number of legal holds in effect at any given time, impacting thousands of employees. The company is now recognizing the significant risks and costs associated with retaining—and maintaining—all electronic data, but is unsure how to address the situation in a manner that is consistent with its legal and regulatory obligations and its business needs.

The Risks & Costs of Retaining All Electronic Data

In a time when fear of spoliation remains prevalent, conventional wisdom regarding electronic data and e-discovery says: "Storage is cheap. It is easier, cheaper and less risky to save all electronic data than it is to take on the challenge and risk of deleting any electronic data under any circumstances, even if you no longer need that data for business or legal purposes." However, as many organizations are now realizing, conventional wisdom is proving to be incorrect. In fact, the risks and costs of the wholesale retention of all electronic data, in a time where the volume of electronic information is exploding, may be *costlier* and *riskier* to an organization than implementing a reasonable, defensible records retention program that encompasses electronic data—*including* the defensible deletion or expiration of electronic data—and may also interfere with the organization's normal business operations. There are many arguments against such wholesale retention.

First, the reality is that data is being deleted in every organization every day, usually in an *ad hoc*, and not particularly defensible, manner. Individual employees are deleting and altering documents in the ordinary course of business; hard drives crash; emails are not properly archived due to normal error rates; systems are retired; and at least some data relating to departing employees is routinely lost. More importantly, deletions of data of this kind are done with no focus or prioritization related to legal, regulatory or business risk or value to the organization. Ignorance of this reality is not bliss—it is a ticking time bomb for legal and regulatory risks, and those risks grow as the vast amounts of data grow and become more unmanageable.

Second, contrary to popular opinion, storage is not necessarily cheap. "Storage" does not only encompass the server or drive on which the electronic data is stored: it encompasses all of the information technology infrastructure—both hardware and software—and all of the information

technology personnel required to retain, manage, protect and backup that electronic information. Often, storage includes maintaining obsolete or legacy systems that are no longer used for normal business operations simply because those systems contain unique data. Over time, and with the rapidly increasing volumes of electronic information, storage can begin to occupy a significant portion of an organization's operating expenses.

Third, the retention of electronic data that is no longer required for business or legal reasons can lead to significant unnecessary risks and costs, *to wit*, the more data that is retained, the more data that is available to be preserved, searched or collected in connection with any legal matter, and the more data that must be processed, reviewed and produced in connection with any legal matter. Considering that discovery costs can account for 75 percent or more of litigation expenses, the costs associated with retaining unnecessary data are apparent. And, in most cases, the percentage of an organization's data that truly is needed for business, legal or regulatory purposes is relatively small in comparison to the volume of data that is being retained.

Fourth, data privacy concerns may make the routine deletion of data (at least personal data) not only desirable, but legally required. The concept that for certain types of personal data, an organization should only retain such data for as long as necessary is prevalent outside the United States. However, that concept is growing in importance even here in the United States, and it is likely that some requirements of routine disposal of personal data is likely on the near horizon. Of course, to meet such requirements, such personal data needs to be properly identified and maintained in a way where proper disposal or deletion is actually effective—a significant challenge for many organizations.

Fifth, information is valuable, unless you cannot find it. Organizations are increasingly recognizing that the data within their organization can be mined for value and, more importantly, revenue. Technology and data analytics, along with the more routine identification of valuable assets such as IP, are dependant on a value-based approach to data storage. In other words, by eliminating the information with little or no value (which, in most organizations, comprises of the vast majority of information stored), organizations can start taking advantage of the new opportunities that "big data" now offer.

Considering "Defensible Deletion"

The risks and costs of retaining all electronic data gives rise to questions such as: (i) what can an organization do to manage its electronic data on a going-forward basis and (ii) what can an organization do about the terabytes and petabytes of data currently retained by the organization that are no longer needed for business purposes? However, electronic data that is no longer needed for business, legal or regulatory purposes still may be necessary for managing an ongoing business operation.

- Consider the Risks and Benefits. Most business activities involve some type of risk. It is important to recognize that a decision about how to manage an organization's electronic data, including a decision to defensibly delete or expire data that is no longer needed, is as much a business decision as it is a legal decision, and should be treated as such. In some instances, the benefits of deleting or expiring data that is no longer needed may be worth the risks involved. Not making a decision about whether to defensibly delete data is a decision to keep that data indefinitely, and that decision to maintain the status quo needs to be defensible from a legal and business perspective.
- Involve the Relevant Stakeholders. An effort to identify, categorize and manage an organization's data, including an effort to defensibly delete or expire data that is no longer needed, cannot be accomplished by legal or IT personnel alone. All of the relevant stakeholders—including senior management, IT, records management, legal, compliance and

privacy—should be involved in the process.

- Use a Targeted Approach. Rome wasn't built in a day, and the challenges associated with the management and retention of electronic data are not going to be solved overnight. Identifying priority data sources or systems and tackling those first can make manageable what seems like an insurmountable problem, and can establish a precedent for addressing other data sources or systems in a reasonable and rationale manner.
- Update Document Retention, Deletion and Archiving Policies. Many organizations have record retention policies that were created before the era of "big data." Such policies should be reconsidered in light of the current complications and challenges with managing electronic data. Among the factors to assess are: (i) how to use existing technology and tools to better manage electronic data; (ii) whether it is in the organization's best interests to acquire and implement new technologies to help manage electronic data; and (iii) developing and implementing more targeted and intensive training programs for individual employees relating to the management, retention and storage of electronic data.
- Content-Based Decisions. One way to address data retention—whether in the context of defensible deletion or going-forward management strategies—is to take a hard look at the content of the data being retained, rather than just the technical source of the data. For example, an organization may decide as a matter of policy that drafts of documents need not be retained for business purposes once the document is finalized. Or an organization may decide that any email that is considered an official record must be stored in a particular way, and that all other email is considered transitory and need not be retained for business purposes. This type of evaluation can be helpful in assessing how much data must be retained and what data can be disposed of on a regular basis.

For inquiries related to this Tip of the Month, please contact Anthony J. Diana at adiana@mayerbrown.com or Therese Craparo at tcraparo@mayerbrown.com.

Learn more about Mayer Brown's Electronic Discovery & Records Management practice or contact Anthony J. Diana at adiana@mayerbrown.com, Michael E. Lackey at mlackey@mayerbrown.com, or Ed Sautter at esautter@mayerbrown.com.

Please visit us at www.mayerbrown.com.