Should You Combine Your Privacy and Records Management Programs?

Compliance and Ethics

Information Governance

Law Department Management

Technology, Privacy, and eCommerce

Cheat Sheet

Two birds. While records management and privacy may have differing requirements, both programs can require many of the same capabilities.

One stone. Many companies are combining the records management and privacy functions into a single organization.

Regulatory risk. Increased privacy laws and regulations around the world are driving companies to reexamine their approach to records management and privacy.

Biggest challenge. If records management and privacy exist as separate organizations, the biggest challenge is often getting alignment between both groups.

Privacy programs and records programs share many of the same capabilities and obligations, making a merger of the two programs advantageous. Companies are increasingly coming to this conclusion, combining their privacy and records management into a single function to drive better compliance, reduce conflicts, optimize resources, and achieve synergy.

Records programs challenged by electronic information

Records management execution is a source of frustration for many companies. They find it difficult to consistently apply retention timelines, and especially proper disposition controls, to their documents and data as prescribed by their records policy and schedule. Instead, this information continues to accumulate, driving up risks and costs. Organizations often become keenly aware of gaps in the records management during eDiscovery, a regulatory inspection, or even while trying to move to a new storage system. Moreover, the drive to “save everything forever” to protect the enterprise can often put an organization at odds with the same teams designed to ensure compliance within a company.

Defensible disposition of unneeded files and emails

As the laws related to data protection expand and the privacy and data security risks are hitting companies from all sides, the interplay between records management and data protection overlap. New and expanded privacy requirements penalize companies for overretention, unlawful usage, or improper protection of privacy information. The European Union’s General Data Protection Regulation (GDPR) set clear requirements for limits on retention and purpose limitations. Now the California Consumer Privacy Act (CCPA), the California Privacy Rights Act (CPRA), and Brazil’s General Data Protection Law (LGPD) are starting a trend in the Americas of setting such strict privacy requirements as seen on the other side of the pond. With many other US states and countries worldwide posed to follow with their own legislation, implementing strict rules for management and safeguarding of personal information is a necessary requirement for all businesses.

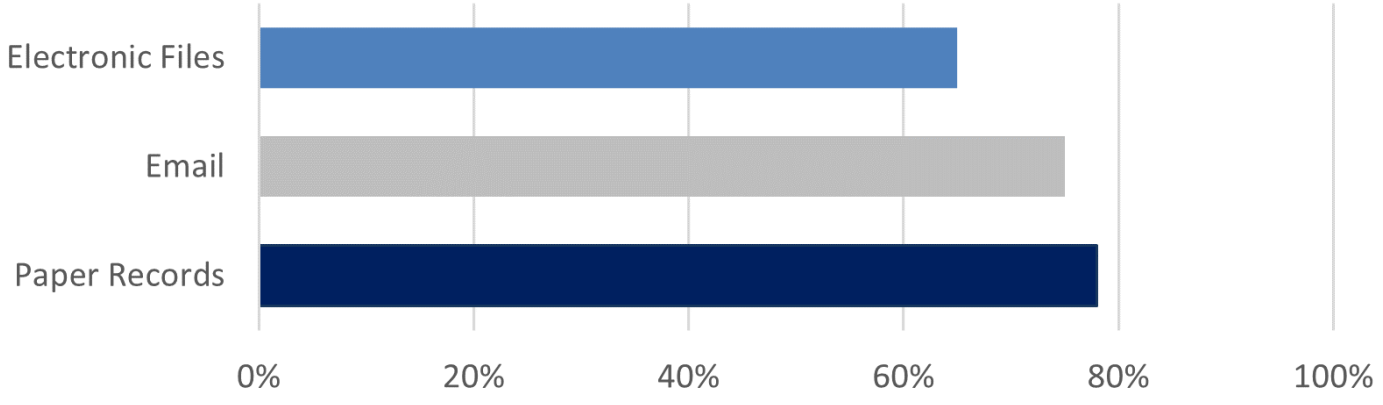

Figure 1. Average percentage of expired records and low-business-value information that can be deleted while maintaining compliance and retaining information still needed by the business. Source: Contoural

The juxtaposition of poor records management and data retention practices can run head first into these new privacy laws and regulations. Yet companies' de facto recordkeeping practices of keeping large amounts of electronic and paper information will certainly be tested under these expanding requirements. Saving large stores of old files, emails, and other electronic content that likely contain personal information is contrary to these regulatory requirements, resulting in fines and other actions as the regulators and public take notice. Furthermore, having to search through these older stores across many systems and locations will only frustrate compliance with the data subject access requests and regulatory inquires or inspections.

Many companies operate their records management and privacy as completely separate functions. One group handles retention and disposition of records, while a completely separate group manages privacy requirements. This division can surface false conflicts between these two functions, and limit the capabilities and compliance of both.

Is there an inherent conflict between records management and privacy?

On the surface, records management and privacy requirements can have conflicting interests with each other. Most records management requirements specify a minimum retention period. Airing on a false sense of caution, companies can and often do save their records for longer than the minimum, even indefinitely due to a lack of other requirements. In practice, employees retain both records and non-record electronic information without clear distinctions or retention controls. Over the years this information accumulates and multiplies across the enterprise. Companies rationalize that a "save everything forever" approach is compliant because records are kept for at least the minimum legal requirement, which often serves as the only clear guidance on appropriate retention periods.

> Airing on a false sense of caution, companies can and often do save their records for longer than the minimum, even indefinitely due to a lack of other requirements.

Privacy on the other hand is focused on lawful and limited usage, restricting the amount of time personal information can be saved beyond its purpose. Furthermore, though the GDPR's "right to be forgotten" and similar requirements under California's CCPA and Brazil's LGPD, residents and consumers can request access to or to have their personal information corrected, deleted, or sent in a portable copy through a subject access request. While some personal information may live in databases, large stores exist in the largest piles of files, emails, and other media, which makes responding to such requests complex and highly burdensome to retrieve or provide to individuals in a compliant manner.

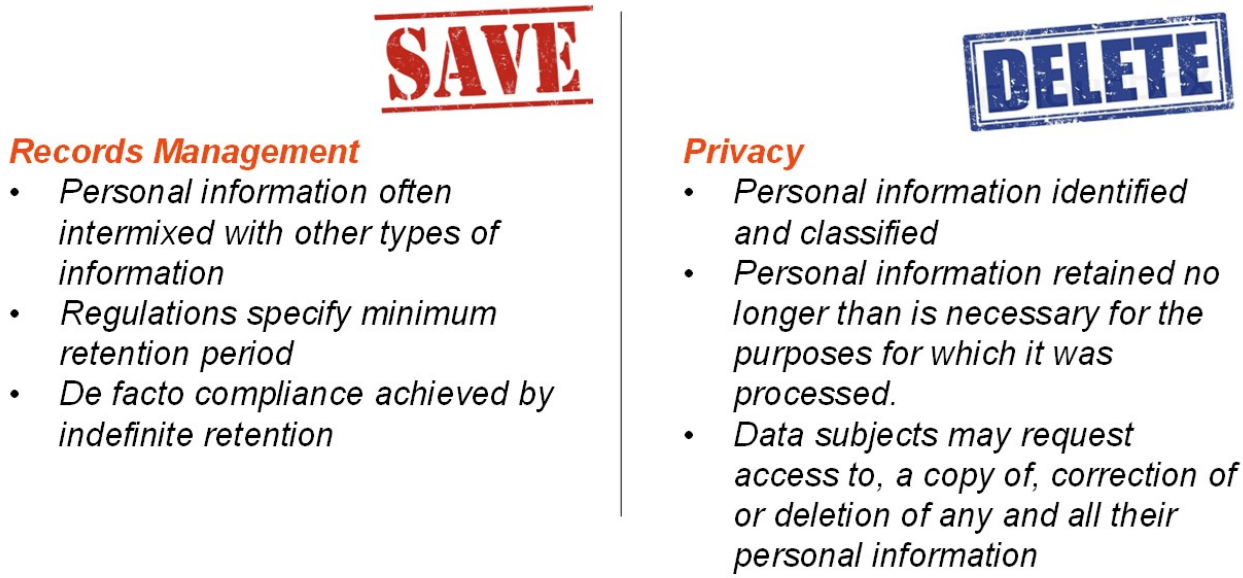

Figure 2. Records Management and Privacy programs appear to conflict.

A conflict exists in that records management compliance is often achieved by saving information longer for preservation or contingency purpose, while privacy requires disposition when the purpose for the record ends. This split is reflected not only in information management processes, but even in how companies have separate privacy and records management organizations.

Privacy and records management share many of the same information management requirements

This apparent conflict between the needs and practices of records management and privacy is false. Closer analysis reveals that privacy and records management both require a level of information management capabilities that are often duplicative or at least complementary. Furthermore, that while records management and privacy requirements come from different compliance regimes, much of the capabilities to successfully comply with both are the same. In other words, developing one common set of information management capabilities can enable companies to build compliant, effective, and harmonious records management and privacy programs.

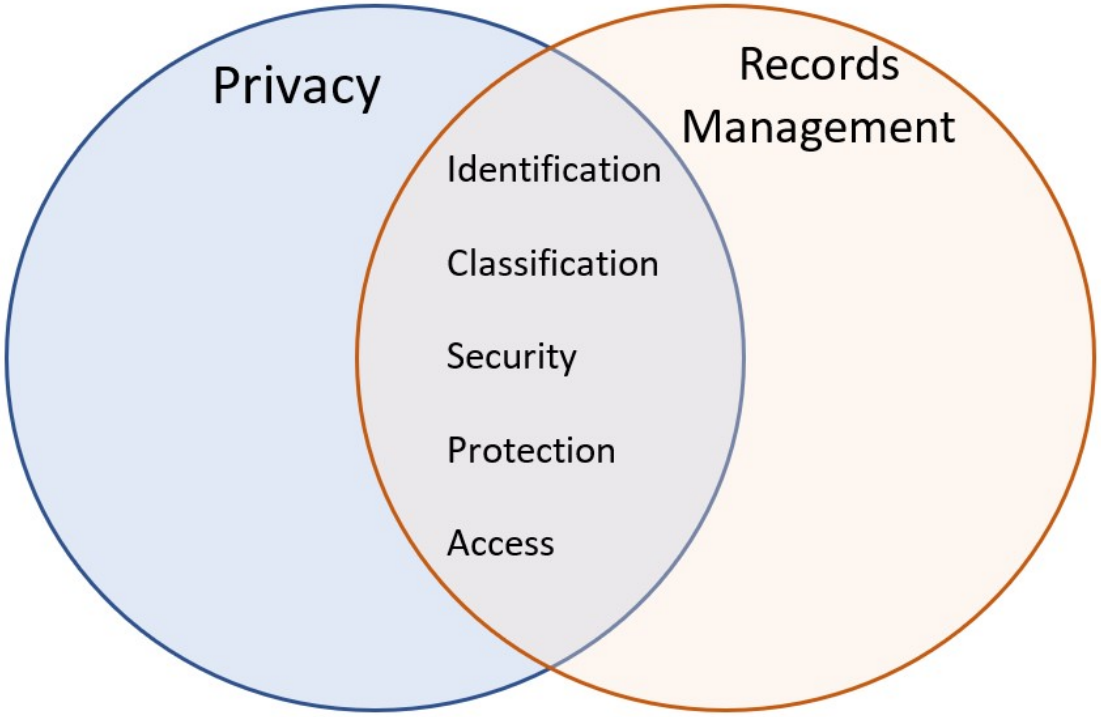

Figure 3. Overlap between privacy and records management.

These common capabilities need to address four key areas:

Identification and classification – Both records management and privacy require documents and data to be identified and classified by its content. Under GDPR and CCPA, for example, personal information is identified as whether the content can be reasonably associated with or linked to a consumer or household. Records are classified based on whether the content constitutes a record.

Security and protection – Many privacy and data protection laws require an enhanced level of security to protect against risks to individuals or the personal information, including breaches. Likewise, records management regulations require strict protection of records and other critical information. Note that files, emails, and other types of unstructured and semi-structured data in the aggregate likely contain significant amounts of personal information as well as records. Storing files, emails, and other data on ungoverned and unsecure locations such as laptops, file shares, and employee-controlled box locations is simply inviting risk.

> Storing files, emails, and other data on ungoverned and unsecure locations such as laptops, file shares, and employee-controlled box locations is simply inviting risk.

Access and retrieval – Privacy requirements dictate that a data subject has the right to know what personal information a business has collected and with whom it has been shared. Many of these laws require businesses to show individuals their actual information or at least an accounting of their information. Records management also requires that specific records be identified and produced, either to a regulator, in court or auditors. Both require the ability to search through large stores of information and selectively produce documents and data based on their content in a timely and complete/comprehensive manner.

Deletion and erasure – The commonalities between privacy and records management continues. Nearly all of the new privacy and data protection regulations limit retention of personal information past its purpose for collection, use, or processing has ceased, while others strictly mandate deletion or "erasure" when either the business purpose for which it has been collected is no longer present, or in response to a data subject's requests for deletion. There are several exemptions from erasure, including if the data still needs to be retained for legal or recordkeeping purposes. Likewise, recordkeeping best practices demand deletion for records that have met their expiration periods, except again when other or additional legal or recordkeeping purposes materialize, such as legal holds. In such cases, deletion or erasure needs to be suspended when these conditions are met and resumed when the original event has passed.

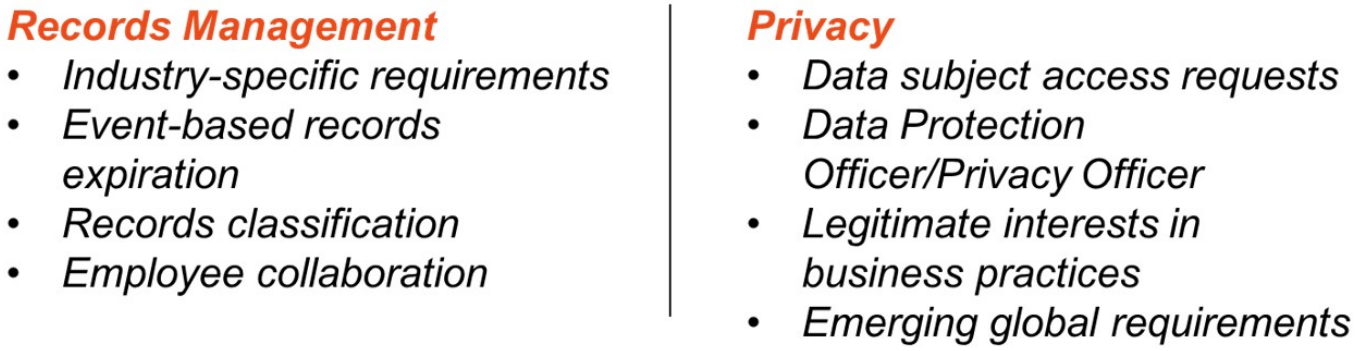

Figure 4. While records management and privacy share a number of similarities and processes, each also has its own distinct requirements.

It is true that not all privacy requirements align with records management best practices. In most privacy regimes, the period in which an individual can request his personal information is limited. Records management retention periods tend to be much longer. Nevertheless, the similarities in managing personal information for privacy and records for records management far outweigh their differences. Taking a step back, many companies are realizing that the similar needs of these programs require them to rethink their approach of two, separate programs.

Combining records management and privacy into a single program

Realizing these similarities between privacy and records management needs, many companies are taking it one step further and combining their privacy and records management program into one single team. These typically include the following steps.

Conducting enterprise-wide, combined personal information and information types inventories – Information inventories need to be created both for personal information as well as records across the document and data landscape. This includes a review of sensitive information and records across email, files, databases, and other electronic media as well as paper stores. A single repository capturing both personal information and records is easier and more cost effective to create and maintain than separate inventories for each.

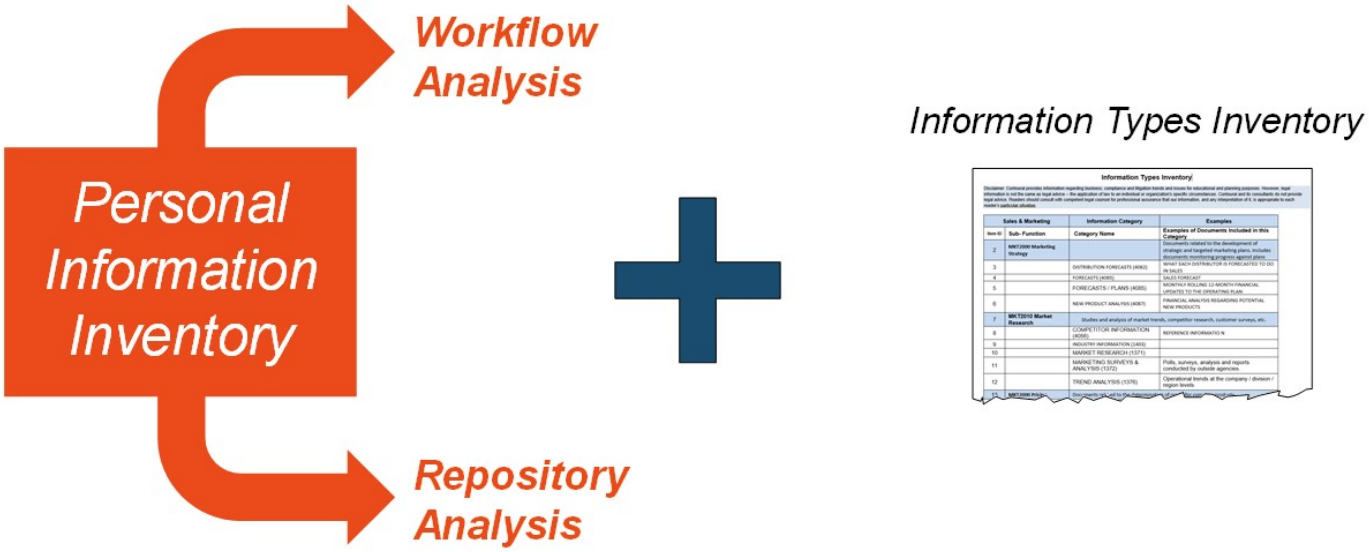

Figure 5. Information inventories can capture both personal information and records.

Developing, updating, and harmonizing privacy, data protection, and records management policies – Organizations need to develop both privacy policies that define what and how they will manage personal information as well as record retention policies and schedules that determine how long information will be maintained. Syncing or harmonizing these two policies minimizes conflicts.

Implementing and configuring information management technologies – Once policies are in place, organizations need to develop the technical capabilities of implementing these policies. This includes identification, classification, securing, managing, searching, producing, and disposing of records and information, including personal information. The same technology and process can be leveraged to address both privacy and records management needs.

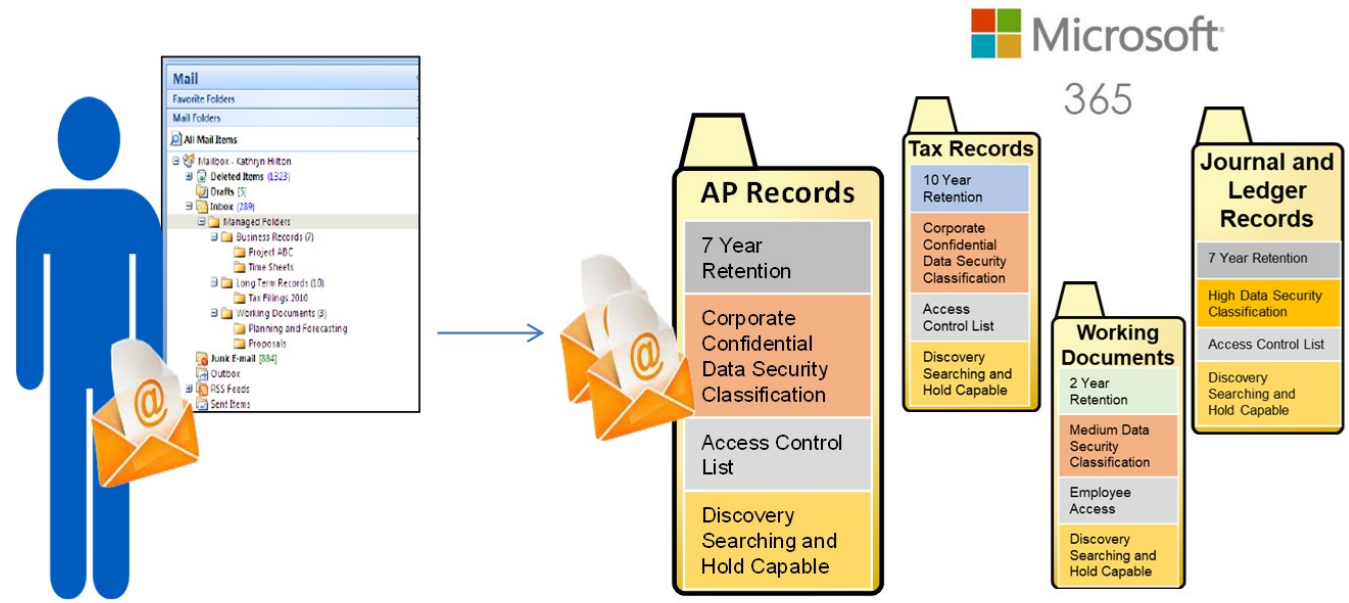

Figure 6. Information repositories such as Office 365 can be configured to apply both record retention and privacy/data security classification rules to files and emails.

Combining and building out skillsets of the new, joint team – Upon combining their privacy and records management organizations, many companies have been able to optimize their resources due

to leveraging the similar skills of the combined organization. While some skills around policy development require specific subject-matter-specific expertise, many of the responsibilities for a joint privacy-records management group require very similar skillsets. These include organizational development, training, risk management, program compliance, management and evangelism, monitoring, and audit.

Combing these programs allow for tangible benefits. First, conflicts between privacy and records management, especially in day-to-day practices are avoided. Second, managing like capabilities and processes under a single program helps create an economy of scale. This also lowers costs, as fewer resources can be deployed more efficiently. Finally, organizations that combine programs have increased compliance for both privacy and records management, as team members often support both program's goals when supporting the larger business. In summary, companies are finding it easier, less expensive, and more compliant to simply combine their privacy and records management programs.

Tactics for overcoming internal political barriers

Perhaps the largest challenge for combining records management and privacy programs are not legal or technical, but rather organizational. If records management and privacy already exist as separate organizations, it can be difficult to get both groups to agree on merging into a single organization. Key messages should be targeted separately for senior management and members of the individual teams.

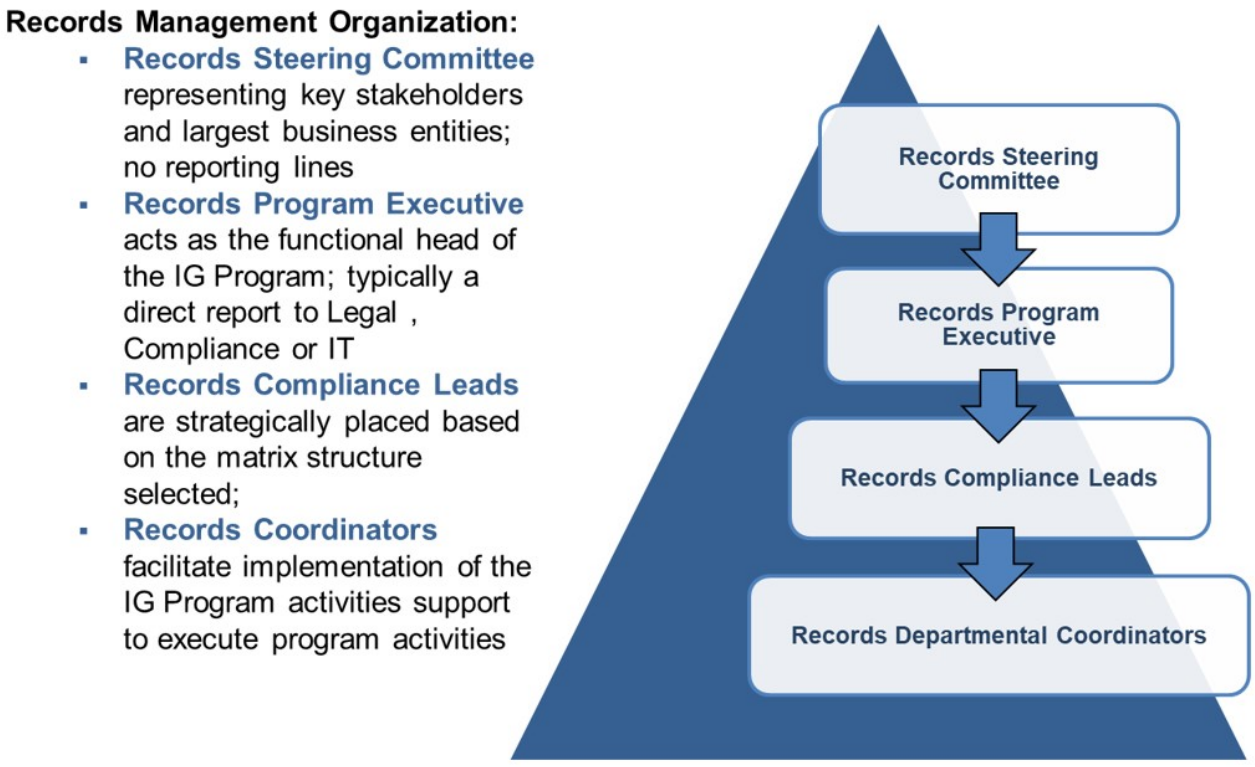

Figure 6.5

Effective messages to senior management can include:

Economy of scale cost effectiveness, cost reductions, and stronger returns on investment – Records management and privacy employ many of the same processes effectively against the same corporate information. Combing both allow an economy of scale.

Risk reductions – Misaligned record and privacy processes run the risk of deleting information that has a legal retention requirement; likewise, in order to minimize the risk of premature deletion, records may be over-retained posing a significant privacy risk. Combined or at least coordinated efforts reduce this risk through established harmonization.

Better leverage technology investments – Technology for identifying, classifying, managing, and disposing of personal information can often also be used for similar records management purposes. Taking a more holistic view can better leverage and optimize these investments.

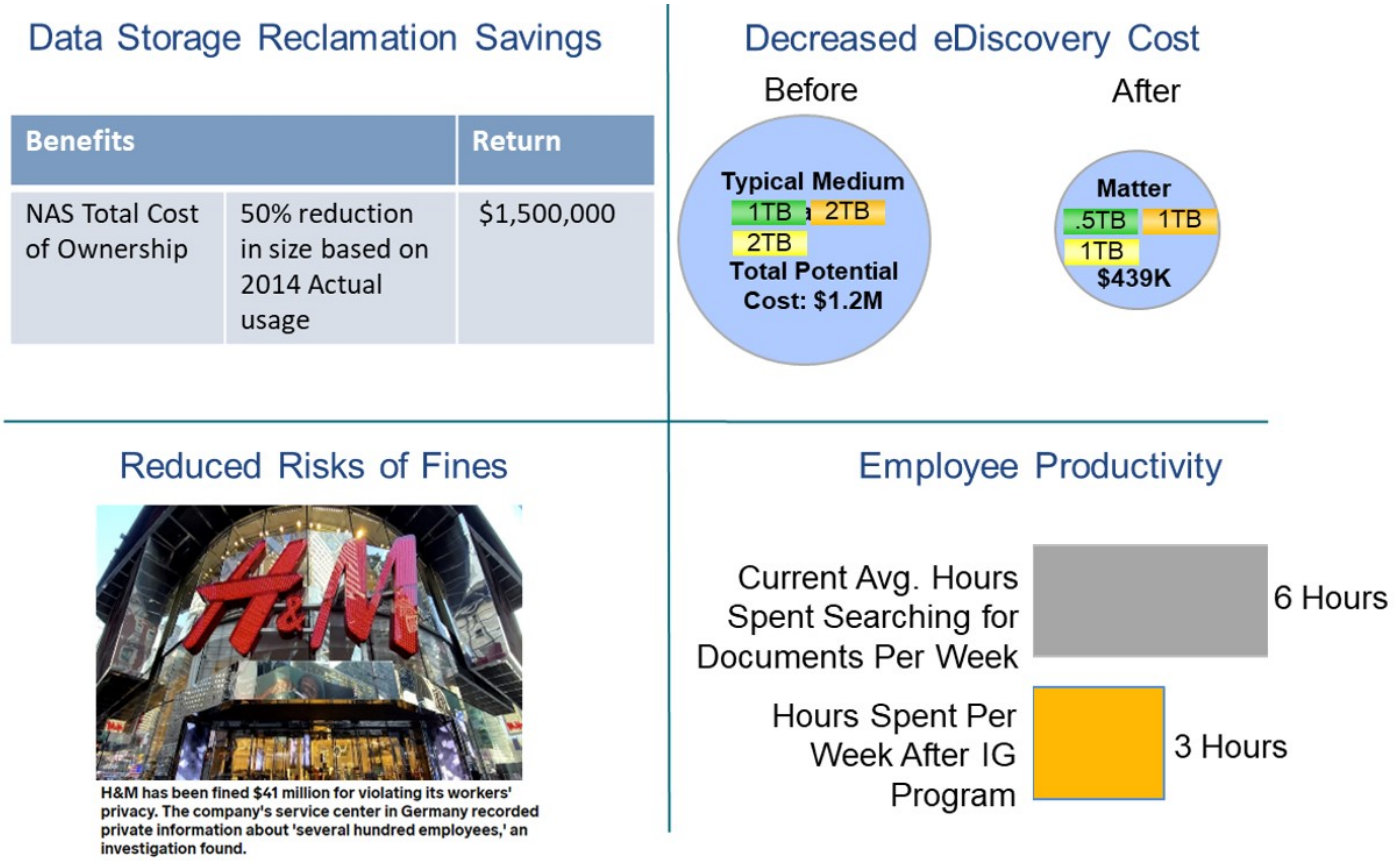

Figure 7. Robust records and privacy programs offer a variety of cost savings.

When approaching individual members of the privacy and records management groups, key messages can reduce internal resistance to combining groups.

Career growth – Combined programs offer more career growth opportunities and diversity.

Better cost sharing – Sharing costs on basic functions can allow more funding for strategic activities.

Seat at the table – A larger organization is likely to have a stronger voice in decisions, or minimally a seat at the table.

Program modernization – Privacy or records management requirements jointly can drive organizations to rethink their processes and modernize their programs.

Greater group respect – Leveraging the business value that both records management and privacy bring can increase the respect of the team across the organization.

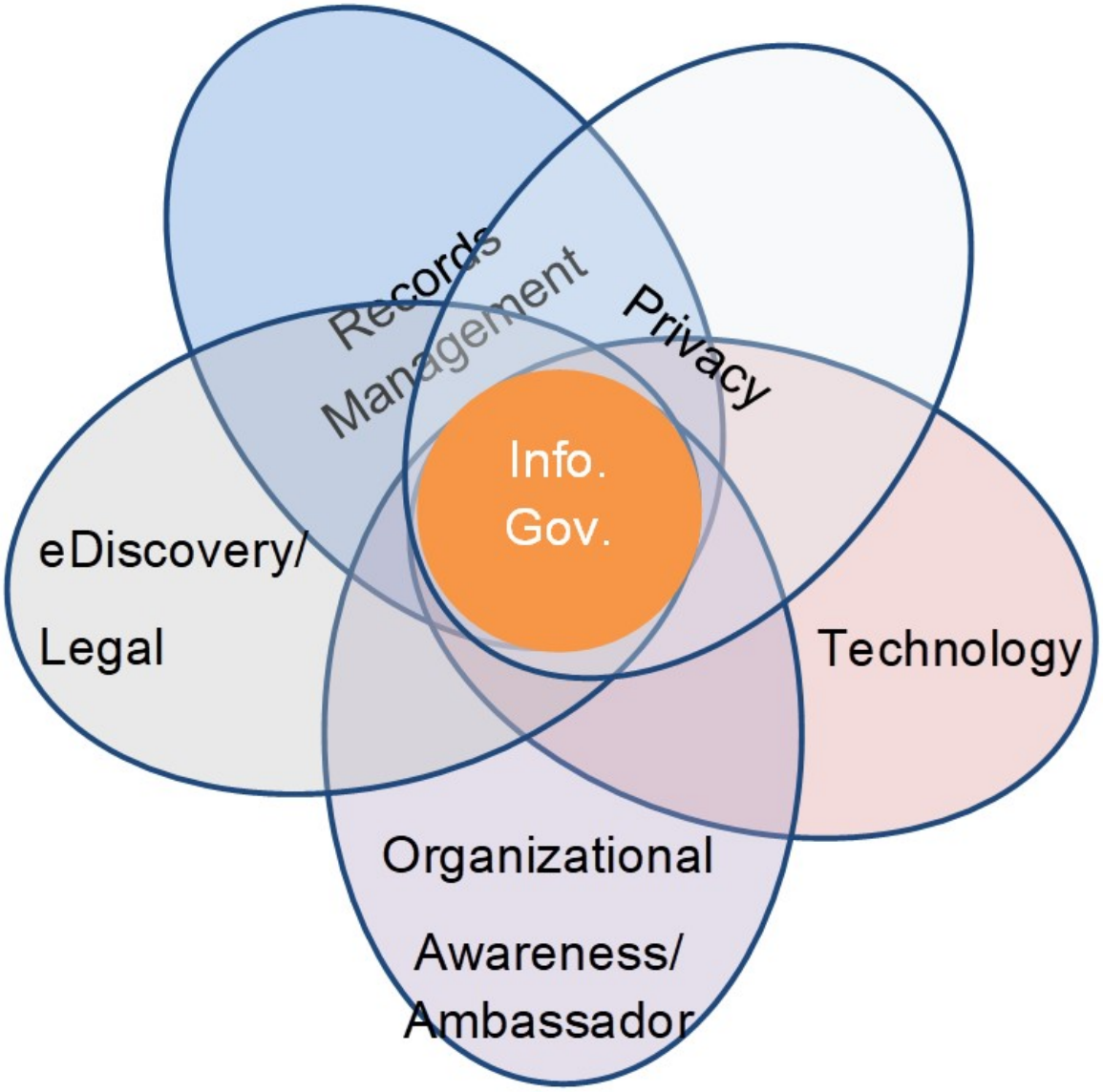

Figure 8. A combined records management and privacy organizations requires a variety of skillsets.

ACC Extras on Privacy and Records Management

ACC Guide: Automating Your Records Program

ACC Guide: Operationalizing the CA Consumer Privacy Act

ACC InfoPAK: Creating a Modern Records Retention Schedule

ACC InfoPAK: Executing Your Records Retention Schedule

Jennifer Couture

Chief Privacy Officer

Alexion Pharmaceuticals, Inc.

Jennifer Couture is chief privacy officer at Alexion Pharmaceuticals, Inc., where she is responsible for company’s global privacy program and Alexion’s records management program. Previously, she worked in a number of privacy, legal, and risk management roles.

Mark Diamond

CEO and Founder

Contoural Inc.

Mark Diamond is the CEO and founder of Contoural Inc., an independent provider of information governance consulting services. His company works with more than 30 percent of the Fortune 500, plus many mid-sized and smaller companies.