Information Management

Aligning Privacy and IM Within the IG Framework

The information management (IM) and privacy functions have many interdependent activities that need to be well-aligned to enable organizations to be compliant, reduce risk, achieve efficiencies, enhance competitive advantage, and improve service. This must occur within an information governance (IG) framework in which IM and privacy are also aligned with the other IG functions: information technology, security, legal, risk/compliance, and business units.

Susan Goodman, IGP, CRM, CIP, CIPP/US, CIPM, FAI

The increasing frequency and magnitude of data breaches have brought the subject of information management (IM) – and especially privacy protection and information security – to the forefront of discussions for most organizations. Today's business environment is perfect for data breaches to occur because of the growing:

- Use of electronic systems by consumers to transact personal business
- Dependence on electronic systems to control large infrastructure systems
- Sophistication of technologies and applications
- Volume and number of data stores containing personal information (big data)
- Value of personal data being sold
- Number and brazenness of individuals who can and will execute data breaches to disrupt systems for industrial espionage, cyber warfare, and theft

Consequences of a data breach for organizations can be substantial, including regulatory investigations and sanctions, lawsuits, fraud, theft, financial loss, brand and reputational damage, and customer loss.

IG: An Umbrella to Protect Data Privacy

The data an organization maintains, and the organization itself, are at greater risk without – among other things – adequate:

- Alignment between the privacy program and other supporting functions (e.g., IM, IT)
- Identification and protection of personally identifiable information (PII)
- System security
- Staff training

Implementing an information governance (IG) framework, which has IM at its core, will not only help an organization address the issues above, it also will satisfy its other IG needs, including the need to derive value from information assets, and help ensure compliance

Other Privacy Issues That Affect Information Management (IM) and Privacy

Do not track is both a privacy advocacy initiative and a way to keep users' online behavior from being followed across the Internet by behavioral advertisers, analytics companies, and social media sites.

Privacy by design means building privacy considerations and compliance requirements into the design and development of products and services. Likewise, privacy principles and requirements should be built into the design of IG and IM programs to help protect PII and prevent breaches.

Mobile privacy includes considerations that seek to protect personally identifiable information while also transparently informing mobile device users of the privacy policies. The GSMA which represents the interests of mobile operators worldwide, has developed its own mobile privacy principles.

Data brokers are corporate entities that collect data (big data) about individuals from public records and private sources, aggregate the data to create a profile about a specific individual (age, race, height, etc.), and then sell the data to customers who use the information for such purposes as marketing or fraud detection. Data brokers in the United States are not regulated. Further, because they are not directly involved with the data subjects, they are not able to get consent for what they do with the information. Repeated attempts to regulate data brokers have failed.

The EU, in contrast, has requirements related to certain data brokers. The General Data Protection Regulation specifies that a data broker that owns the personal data of an EU resident anywhere in the world, using any equipment, is legally within the reach of EU enforcement authoriteis.

Smart cities use data collection sensors to acquire information that can help them better manage assets and resources. Data collected from citizens, devices, and assets is analyzed to monitor and manage traffic and transportation systems, for example, as well as rainfall impact, electricity provision, and more. Smart cities integrate information and communications technology and physical devices connected to the network (i.e., the Internet of Things) to optimize city operations and services and to connect to citizens.

Cities, like other entities, must perform privacy impact analyses to ensure their projects comply with legal and regulatory requirements and their commitment to specific privacy principles. Compliance includes all action on the city's part, as well as that performed by companies that supply technology, equipment, and services related to the information they collect, use, transfer, retain, and dispose. Third parties must be held accountable for satisfying the city's IM and privacy requirements (e.g., receiving informed consent, protecting collected data, disposing of data as dictated by the city's retention schedule, etc.).

Enforceable self-regulatory codes, to be promulgated and enforced by industry groups, have long been promoted by the U.S. Federal Trade Commission. The premise is that industry groups can more effectively establish requirements for their own industries. The argument against self-regulation is that an industry may not do it impartially. In either event, all self-regulatory codes must be incorporated when building the IM and privacy programs and when aligning the two.

with its legal, regulatory, and business requirements for information.

IG includes the following component functions: IM, privacy, information security, legal, risk/compliance, IT, and business units. IG integrates these elements into an overarching "umbrella" structure, enabling the success of each – and of the organization itself – because these functions are enterprise-wide and have interrelated and interdependent systems.

In an effective IG framework, the component functions apply their expertise to a strategic, multifaceted approach – at both the program and tactical levels – to satisfy the goals of all IG functions and the enterprise. From a privacy perspective, this means ensuring that the personal data the organization collects from customers and the public is secure and managed in compliance with all laws, regulations, privacy and organizational principles, and IM and business requirements.

The same is true from an IM perspective, which oversees the management of all information assets. Strengthening privacy, like strengthening IG and IM, increases organizational compliance; reduces operational, financial, reputational, and legal/regulatory risk; and increases efficiency and competitive advantage.

Definition of Privacy

Privacy at its core means the right to be left alone. *Information privacy* has a narrower scope. It is, according to the International Association of Privacy Professionals (IAPP), "the right to have some control over how your personal information is collected and used."

PII must be protected through security methods, non-disclosure practices, and tight disclosure controls. The National Institute of Standards and Technology (NIST) Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* defines PII as 1) "any information that can be used to distinguish or trace an individual's identify, such as name, Social Security number, date and place of birth, mother's maiden name or biometric methods" and 2) "any other information that is linked or linkable to an individual, such as medical, educational, financial and employment information."

So, a health record that is or can be associated with its subject's name requires protection. However, once the name and other PII linking it to its subject have been removed, resulting in anonymized data, the details do *not* require privacy protection. Increasingly, though, advanced technologies can link anonymized data in unrelated databases to re-identify a data subject. Thus, privacy protection requires controls to prevent such re-identification.

Controls to Protect Privacy

What information is considered private – and how to manage it – is typically written into law. Because the laws of various jurisdictions and regulatory authorities vary, adhering to all privacy requirements can be complex. Aligning privacy with IM within a solid IG program is essential to helping organizations comply with privacy requirements.

There are many players in the privacy space, such as federal, state, provincial, and local legislators and regulators, the executive branch, the judicial system, law enforcement agencies, and the criminal justice system. There are country-specific data protection authorities, self-regulatory certification bodies, advocacy organizations, industry groups, and professional associations. Players also include the data subjects, such as citizens, clients, customers, patients, employees, students, and more.

U.S. Controls

While the U.S. regulatory governance of privacy is "sectoral" in nature, the Federal Trade Commission (FTC) has an extremely strong privacy enforcement role nationwide as part of its consumer protection responsibilities. Its justification is that companies that violate its privacy policies are violating the FTC Act by engaging in an "unfair or deceptive act or practice."

Additionally, privacy and information security legislation promulgated by some U.S. states (Massachusetts and California, for example) requires compliance by any entity conducting business with a resident of that state, regardless of where that entity is located. Such requirements make the legislation *de-facto* national in scope.

Other Countries' Controls

Outside the United States, legislation is typically *comprehensive* rather than industry-specific. It is sometimes federally driven, as in Switzerland, and sometimes regionally driven, with individual countries establishing corresponding laws and regulations.

An example of the latter is the European Union (EU) General Data Protection Regulation (GDPR), effective May 25, which replaces the EU Data Protection Directive 95/46/EC. As described on the GDPR portal (*eugdpr.org*), it "was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens' data privacy and to reshape the way organizations across the region approach data privacy."

It also addresses the export of personal data outside the EU. Further, Article 17 of the GDPR mandates a right to erasure, commonly called "the right to be forgotten."

There are co-regulatory frameworks (e.g., Australia) where government and industry sectors collaborate on privacy regulation and oversight. There are self-regulatory frameworks in the United States and Singapore where industry groups establish, monitor, and enforce privacy requirements.

What is sensitive may also vary from location to location. For instance, in the United States property

Correlations Between the	
Generally Accepted Recordkeeping Principles®	**Generally Accepted Privacy Principles**
Accountability: A senior executive (or a person of comparable authority) shall oversee the information governance program and delegate responsibility for information management to appropriate individuals.	**Management:** Defines, documents, communicates, and assigns accountability for its privacy policies and procedures.
Integrity: An information governance program shall be constructed so the information assets generated by or managed for the organization have a reasonable guarantee of authenticity and reliability.	**Quality:** The organization maintains accurate, complete, and relevant PII that is necessary for the purposes identified.
Protection: An information governance program shall be constructed to ensure an appropriate level of protection to information assets that are private, confidential, privileged, secret, classified, essential to business continuity, or that otherwise require protection.	**Security:** PII is protected against both physical and logical unauthorized access.
Compliance: An information governance program shall be constructed to comply with applicable laws, other binding authorities, and the organization's policies.	**Monitoring and enforcement:** The organization monitors compliance with its privacy policies and procedures. It also has procedures in place to address privacy-related complaints.
Note: Even though Compliance is not cited in GAPP, compliance with privacy and information security laws and regulations is critical to an effective privacy program. IM and privacy should join forces to monitor and enforce over-lapping requirements to attain greater efficiency and compliance.	
Availability: An organization shall maintain its information assets in a manner that ensures their timely, efficient, and accurate retrieval.	**Access:** Give individuals access to their personal information for review or update.
Note: Availability and Access mean different things in this set of principles, but they correlate in that PII must be available to privacy subjects who wish to review it.	
Retention: An organization shall maintain its information assets for an appropriate time, taking into account its legal, regulatory, fiscal, operational, and historical requirements. **Disposition:** An organization shall provide secure and appropriate disposition for information assets no longer required to be maintained, in compliance with applicable laws and the organization's policies.	**Use, retention, and disposal:** Use of PII is limited to the purposes identified in the notice the individual consented to; retain PII only for as long as needed to fulfill the purposes or as required by law. Dispose appropriately after that period.
Note: There is a partial correlation between these two sets of principles. IM is responsible for issuing, monitoring, and enforcing the records retention schedule; the privacy program is therefore dependent on IM to ensure that its goals are met in those arenas. ARMA's Principles don't address agreed-upon information use as a caveat for retention, and GAPP doesn't account for legitimate operational need/business policies.	
Transparency: An organization's business processes and activities, including its information governance program, shall be documented in an open and verifiable manner, and that documentation shall be available to all personnel and appropriate, interested parties.	**Notice:** Provides notice of its policies and procedures, identifies the purposes for which PII is collected, used, and retained. **Choice and consent:** Describes the choices available to the individual; secures implicit or explicit consent regarding the collection, use, and disclosure of the personal data. **Collection:** Personal information is only collected for the purposes identified in the notice.
Note: GAPP's Choice and Consent regarding the collection, use, and disclosure of information to third parties doesn't have a counterpart in the ARMA Principles. However, IM programs are responsible for ensuring that all requirements related to information within the organization are accounted for and adhered to, and that evidence of compliance is properly documented and maintained.	

Table 1: Correlation between the Principles and GAPP

records are public, but that data is considered private in some countries. There is a broad interpretation of the term *personal information* under EU data protection law, which includes business contact information and membership in trade groups and political organizations. Salary information of most private sector employees in the United States is private, whereas in some countries it is not. Compliance with privacy and information security is especially complex for global companies, and even more so for global companies in multiple industries.

Legal cases are being adjudicated in many jurisdictions globally, setting new precedents. Added to this, all the above is evolving and shifting rapidly.

Privacy Frameworks

IG and IM professionals should be aware of these privacy frameworks:

- **U.S. FTC's Fair Information Practice Principles (FIPPs).** The principles have been incorporated into the legislation of several states and global entities.
- **Organization for Economic Co-operation and Development (OECD) privacy principles.** The OECD is a research and policy-making body that sets international standards on a wide range of issues, including communications technologies and the future of the Internet.
- **Asia Pacific Economic Cooperation (APEC) privacy framework.** It promotes a flexible approach to information privacy protection across APEC member economies, while avoiding the creation of unnecessary barriers to information flows.
- **Generally Accepted Privacy Principles (GAPP).** GAPP was developed jointly by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA).

Most privacy frameworks cover similar territory, such as opting in or out, executing and monitoring contracts with third parties that manage PII, securing PII and retaining it properly, ensuring mobile privacy, implementing privacy by design, reporting incidents, and complying with transparency requirements.

The Privacy and IM Relationship

An effective IM program must incorporate all requirements that impact the creation, management, and disposition of all organizational information, and this includes privacy requirements. Similarly, a compliant privacy function is dependent upon an effective IM program to ensure compliance with privacy requirements.

To assess this premise, it is useful to compare the Generally Accepted Recordkeeping Principles® (Principles) with privacy principles (using the GAPP as an example) because it is upon the basis of these principles that the respective programs are developed.

Although there are slight variations in the definitions and scope of the Principles and GAPP, there is a strong correlation between these sets of principles, as shown in Table 1 on page 33.

Aligning IM and Privacy

Both privacy and IM programs emphasize having, implementing, and monitoring policies and procedures; for each program to be successful, their policies and procedures must align. For instance, the privacy policy should reference the IM retention schedule, which in turn should account for privacy requirements.

Some practice areas generally are aligned between the two functions, such as the creation of inventories to identify records. IM creates records inventories to identify and document all organizational records, and privacy creates privacy inventories to identify all PII. Both identify functions and departments responsible for the information, locations, and so on.

These recommendations should help ensure greater alignment and a collaborative relationship between the two functions. IM and privacy representatives should:

- Serve on the IG team
- Work in partnership with the other IG functions
- Serve on each other's advisory committee
- Serve on many of the same committees and project teams
- Review each other's policies and procedures to ensure that all necessary requirements, references, and guidance have been included
- Align their training and communications and cross-reference the other function, as applicable

In addition, privacy should review all RIM processes and retention schedules to identify PII, and information security should provide security classifications for records listed in the retention schedules. Conversely, privacy and information security procedures should reference the records retention schedule because the schedule addresses privacy requirements and considerations.

When there are conflicts in retention requirements, privacy and IM can reach consensus about the appropriate disposition and document it for defensibility to reduce risk.

The Organizational Structure

How the functional relationship will be developed is often determined in part by the organizational structure in which IG, IM, and privacy exist. In Canadian jurisdictions, for example, the IM officer may be the chief privacy officer as well. Organizations with strong IM programs but immature privacy programs will often look to the IM director to take on the privacy function as well. Many new positions are being established that combine both functions into one role. Other organizations have placed IM and privacy under the compliance or legal functions.

Organizations are beginning to establish IG roles,

with IM and privacy reporting through them. Having them combined under the same management facilitates their alignment. Organizational management structures and reporting lines will continue to shift as IG gains a stronger foothold within organizations and as the IG, IM, and privacy functions mature. E

Read More About It

These resources provide valuable information about information governance, information management, and privacy – and about the alignment of these functions.

AICPA/CPA Generally Accepted Privacy Principles (GAPP) (*www.aicpa.org* (U.S.) and *www.cpa.com* (Canada): Search for "privacy" on each site.

AIIM (*www.aiim.org*): This organization offers publications, conferences, courses, and other resources on information management. Search for "privacy."

ARMA International *(www.arma.org):* This association serves those who manage and govern organizations' information assets, offering educational resources for IM, IG, and privacy. Learn more about the Generally Accepted Recordkeeping Principles®, the Information Governance Maturity Model and other core concepts at *http://www.arma.org/?page=CoreConceptFund* and about the Information Governance Professional certification at *www.arma.org/page/Certifications.*

ARMA International's *Secure Management of Private Information* (ARMA International 28-2015). The author of this article, Susan Goodman, contributed to this ANSI-registered technical report, which is available at *https://www.arma.org/store/ViewProduct.aspx?id=10518258.*

Asia Pacific Economic Cooperation (APEC) APEC published the *APEC Privacy Framework*, which is available at *http://publications.apec.org/publication-detail.php?-pub_id=390.*

Better Business Bureau *(www.bbb.com):* This U.S. consumer protection agency protects privacy rights and offers a self-certification program for BBB Standards for Trust that includes a privacy component.

Digital Advertising Alliance *(www.digitaladvertisingalliance.org):* This independent nonprofit organization, which is led by leading advertising and marketing trade associations, establishes and enforces responsible privacy practices across the industry for relevant digital advertising.

Electronic Frontier Foundation *(www.eff.org):* This is a leading nonprofit defending digital privacy, free speech, and innovation.

Electronic Privacy Information Center *(www.epic.org):* This is a public research center in Washington, D.C.

European Union *(www.eugdpr.org):* This site educates about the General Data Protection Regulation (GDPR).

Federal Trade Commission (FTC) *(www.ftc.gov):* Search for "privacy" and the Fair Information Practice Principles (FIPPS), which are the result of the FTC's inquiry into the way online entities collect and use personal information and safeguards to ensure that the practice is fair and provides adequate information privacy protection. (Filter by year and then document type.)

Google *(www.google.com):* Set alerts such as for "privacy" to receive messages when news items pop up for the search term you provide. (Other platforms offer similar alerts.)

Information Governance Initiative (IGI) *(www.iginitiative.com):* This is a think tank and community dedicated to advancing the adoption of information governance practices and technologies through research, events, advocacy, and peer-to-peer networking.

International Association of Privacy Professionals (IAPP) *(www.iapp.org):* This is the largest and most comprehensive global information privacy community.

Organization for Economic Co-Operation and Development (OECD) *(www.oecd.org):* The OECD published the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.*

Payment Card Industry Data Security Standard (PCI DSS) *(www.pcisecuritystandards.org)*: The PCI Security Standards Council is a global forum for the ongoing development, enhancement, storage, dissemination, and implementation of security standards for account data protection.

TrustArc (formerly TRUSTe) *(www.trustarc.com):* This organization offers privacy self-certification for firms and other privacy-related resources.

About the Author: Susan Goodman, IGP, CRM, CIP, CIPP/US, CIPM, FAI, is the CEO of Infoflo Consulting LLC, an information governance (IG), records and information management (RIM), and privacy consulting firm. She has more than 25 years of IG, RIM, and privacy leadership experience across industries and frequently speaks at conferences and contributes to professional literature. Goodman earned a bachelor of arts degree at the City University of New York-Queens College and a master's degree from the School of Information Science and Policy at the State University of New York at Albany. She has also earned the credentials of Information Governance Professional, Certified Records Manager, Certified Information Professional, and Certified Information Privacy Professional, and she was named a Fellow of ARMA International. Goodman can be contacted at *susangoodman@infofloconsulting.com*.