Introduction

The notion of privacy transcends multiple areas of our lives: physical, informational, organizational, spiritual and intellectual. The approach to privacy and the strength of an individual’s feelings about privacy can vary across cultures and geographic areas. As a result, it is difficult to create a one-size-fits-all definition of privacy. The confluence of globalization, new information technologies, law and consumer expectations have resulted in myriad unanswered questions about what laws apply when, who owns or controls what information and when, and who should handle and what should comprise enforcement.

One of the thorniest issues in privacy is defining personal information. This term is at the heart of most privacy laws and regulations, and defining it is often the starting point for most organizations in determining how to manage and protect information. Broadly speaking, personal information is information about people. Similar, often overlapping, but not identical definitions of personal information include: “personal data,” “personally identifiable information,” “sensitive information,” “non–public personal information,” “personal health information,” “customer information,”
“employee data,” “credit reporting data” or even “PCI (payment card industry) data.” These varied definitions are one result of the different legal, societal and cultural perspectives on data privacy and response to privacy and data protection concerns. More recently, there has been a convergence of thought and definition leading to the use of “personal data,” data from, about or which can be linked to a specific individual—either through common analysis techniques or advanced analytics.

The broad definition of personal data as any information relating to an identified or identifiable individual, adopted in many international jurisdictions, originated from the OECD (Organization for Economic Cooperation and Development) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, first published in 1980. The OECD Guidelines are an extension of the widely-recognized Fair Information Practice Principles (FIPs)—developed in the early 1970s in the United States.

Many countries in the Asia Pacific Economic Cooperation (APEC) region have adopted laws or codes-of-conduct based on the APEC Privacy Principles, which are a super-regional adaptation of the OECD Guidelines. The Australia Privacy Principles (APP) and Singapore Data Protection Act (PDPA) are two examples. U.S. state, Canadian provincial and E.U. country specific laws may further define or specify the scope of personal information.

United States federal and state laws address personal information and privacy sectorally—the regulations are intended to address specific industries or types of personal data such as financial or health information, or information about children. This sectoral approach results in a variety of definitions of personal information. Generally, personal information in the United States includes name, physical and email addresses, telephone number (land or mobile) and unique information such as government issued ID number, account numbers or identity verification information (user name, password, PIN), and in some situations device ID and geo-location.

In contrast, the European Union and many other countries around the globe, define personal information (“data”) rather broadly to include any information relating to an identified or identifiable person such as identification number or one or more of the following factors: physical, physiological, mental, economic, cultural or social identity of an individual, not necessarily in combination; and may included new data derived from analytics processes.
In Canada, personal information is any information about an identifiable individual with the exception of name, title, or contact information of an employee of an organization.

Many organizations, rather than trying to determine what the definition of personal information is at a specific time and in a specific place, will choose the broadest definition: any information (or data) which can identify or be linked to an individual.

In an era of growing concern about increased, often surreptitious use of robust data analytics (aka, “big data”), data breaches and theft of trade secrets and company confidential information, many organizations focus on safeguarding customer data and fail to consider that certain privacy obligations also extend to their employees, shareholders, members, contractors, vendors, suppliers and other stakeholders.

In light of existing obligations to protect both external (customer) and internal (employee, shareholder, member, contractor, vendor, supplier and other stakeholder) information, an organization must develop a comprehensive privacy program that addresses all areas and types of data.

Creating a Privacy Program

The three great essentials to achieve anything worthwhile are: Hard work, Stick-to-itnessness, and Common sense.

—Thomas A. Edison

Creating and implementing a Privacy Program is hard work. That said, it is entirely possible to develop and implement a practical program that addresses an organization’s unique characteristics, overall strategy, customer expectations and compliance with privacy promises and obligations. But where to start? Buy-in at the top is essential, as is cross-departmental sponsorship and funding of the program. That buy-in may be easily obtained by expressing the importance of overall risk reduction through legal compliance, the increase in enforcement actions around the globe, and the enhancement of your brand and reputation by making a strong commitment to honoring privacy obligations. Once you have the commitment of the appropriate leaders and individuals in the organization, the work really begins.
Information privacy life-cycle management involves creating policies, processes and guidelines that address collection, use, management, retention, and archival or disposal of personal information in a responsible and trustworthy manner. Often, information privacy is referred to as “data protection,” “information management” or “information security;” each of these concepts is independent but connected with privacy in some way or another. This chapter focuses primarily on “information privacy,” and does not address broader privacy concepts such as anonymity or government surveillance.

Information privacy is most universally expressed in the context of Fair Information Practice Principles (FIPs). (See:) The core principles of FIPs are:

- Notice/Awareness
- Choice/Consent
- Access/Participation
- Security/Integrity
- Enforcement/Redress

Most privacy laws and regulations, throughout the globe, address each of these Principles (or their corollary found in the OECD Guidelines), and some laws and regulations include a few others. Using these Principles as a guide can assist an organization in evaluating information privacy practices and create a strong foundation for the development of a privacy program.

An effective and successful information privacy program must align with an organization’s strategy and values, and public promises, not just legal compliance. Support of the program from an organization’s executives and primary internal stakeholders is crucial to success and more easily obtained through transparency and strong communication.

Key components of a comprehensive privacy program include:

- Policies, procedures, rules and standards
- Training, communication and awareness
- Risk, impact and audit assessments and monitoring
• Alignment with overall code of conduct and ethics and enterprise risk management

• Alignment with Information Security and safeguarding programs and policies

• Consumer/user/customer education, outreach and response

• Monitoring and assessment of regulatory changes.

Some privacy programs may also include:

• Use of third party accountability agents

• Linkage with Data Governance programs and models

• Participation and contribution to public policy, legislative activity and industry best practices.

Key outcomes of a successful information privacy program include:

• Trust: customer, consumers, employees, external stakeholder trust of the organization.

• Risk Management: identifying and prioritizing the most salient areas of privacy and data protection risk.

• Setting Expectations: creating meaningful, actionable and measurable policies for employees, customers, third parties and other key stakeholders.

• Empowerment: providing employees an understanding of their role and responsibilities in managing information resources and in protecting personal information.

• Accountability: fostering a climate and culture for responsible collection, use, management, transport, retention, security and disposal of personal information.

• Operational effectiveness: the opportunity to build and implement global processes and systems that meet business, privacy, security and data governance goals and objectives.
• Brand and Reputation: enhances and preserves the organization’s reputation with stakeholders.

A comprehensive privacy program must address privacy risks and mitigation techniques to reduce an organization’s exposure to the risk potential and likely impact to the business and privacy programs outcomes described above.

A number of privacy risks, both internal and external, exist for an organization of any size. These risks include, but are not limited to: inadequate information system or security controls, misuse of personal information; failure to meet published privacy promises; failure by employees to understand or act on their obligations related to personal information or breach of confidentiality (purposeful or accidental); inability to detect breaches; failure to implement the appropriate level of security based on the type of data and its uses; technology or database malfunctions; physical loss of assets; poor data integrity and quality; third party vendor, partner or supply chain failures, and poor incident response processes. Each of these can result in reputational damage, regulatory enforcement actions, civil or criminal actions and monetary fines. While these risks cannot be entirely eliminated, many can be mitigated by employing policies and procedures that clearly articulate critical areas of exposure and assign responsibility and accountability for compliance.

The Nuts and Bolts

Start by determining what “personally identifiable information” (PII) (or personal data) means to your specific organization and how it relates to the specific products and services you provide (whether free or paid). Do you operate only in the U.S.? If so, you may choose a definition that is more specific (for example, two discrete identifiers in combination) than if you operate in the European Union, Canada, Latin America or Asia, where a broader approach to the definition of PII may be more appropriate, e.g. “personal data”. If your organization will capture PII or personal data from more than one location and transmit, store or access this data across country borders, or if you are concerned about managing a variety of data, you may choose a common definition that will transcend all jurisdictions.

Once you have determined how your organization will define PII within the given context, you should examine the who, what, when, where and why of collection, storage and use.
**Collection:** What information do you collect and from whom do you collect it? Is it employee data, customer data, vendor, supplier or agent data? Where are you collecting the information from? Is the data being transferred across borders? Why is it being collected? How is it being collected? Does the individual give the data directly to you and/or is information collected about the individuals’ behavior, activities and movements? Is this done to provide goods and services to customers or to provide employee benefits or to monitor employees? The most important question that must be answered is whether the collection is truly necessary in order to carry out the business objective and stated purposes.

**Notice and Awareness:** Have you informed individuals regarding personal information collection, use and storage? What means are used to deliver the privacy notice? Terms of Use? Online Privacy statements? Mailed statements? In-context “just-in-time” messages? Are these consistent with regulatory requirements? With customer expectations? Are the notices easy to understand?

**Storage:** Where is the information being stored, and in what form? Is it being stored by a third party (such as a “cloud” provider) or internally or both? What security measures are employed to protect the information? Are appropriate contracting terms in place? Is there a data retention and deletion policy in place?

**Use:** What will the organization use the information for? Will it be used to deliver products and services to customers? To create new products and services? To Market and sell products and services? For research? For fraud detection and prevention? To track or monitor behavior? For internal corporate administration? To share, monetize or sell to other organizations? Who has access to the information? Is the information being electronically collected, segregated, manipulated, aggregated, or otherwise “processed”?

**Choice and Consent:** Are individuals able to make a choice or consent to the collection, use or disclosure of their data? Are the consents and choices consistent with terms and notices regarding personal information collection, use and storage? What means are used to offer choice? What methods are employed to track and apply choices? Are the consents consistent with regulatory requirements? Are the methods which present choices or consents easy to find and use, and by all relevant device types or channels (web, mobile, in-person, by mail)?
Security and Integrity: Have you defined the categories and classification of personal information and data the organization has? Are adequate security levels defined for each? Are the groups responsible for privacy and security in agreement and working together to ensure the appropriate level of security is in place based on the type and sensitivity of the data? Are the groups responsible for privacy and security in agreement and working together to detect, manage and respond to incidents, including triage, correction and notifications? Are technology and business processes in place to prevent misuse, alteration or corruption of data and ensure data integrity and accuracy? Are technology and business processes in place to allow both appropriate internal and vendor access, and prevent unauthorized access to data? Are technology and business processes in place to allow both appropriate external authenticated (customer, user) access to data? Does the organization actively monitor, detect and contain intrusions? Does the organization regularly patch vulnerabilities? Does the security group actively monitor, respond to and inform internal stakeholder external changes, threats and enforcement actions in the security environment?

Enforcement and Redress: Have specific individuals been assigned responsibility for implementation of and compliance with privacy and security policies? Is there senior executive support to drive compliance and ensure governance in the organization? What mechanisms are in place to ensure employees understand their obligations related to those policies? Is there a process for your customers to submit privacy inquiries or complaints? For employees? How will the organization respond to those individuals? Has the organization evaluated what external entities (i.e., privacy regulators, government agencies, law enforcement, state Attorneys General, consumer protection groups, media) may inquire about privacy and security policies and practices? Is there a plan in place to respond to those entities?

The answers to each of these questions necessarily entail an analysis of what laws apply and when, whether certifications (U.S.-E.U./U.S.-Swiss Privacy Shield, SAS 70/SSAE 16, SOC, ISO, PCI DSS and the like) need to be examined and what organizational and/or technological security measures are employed to secure the data. However, having the answers to these questions will assist in formulating policy and procedure for how to manage privacy for your services, third party relationships and employee matters.