An Executive Overview of

GAPP

Generally Accepted Privacy Principles


Privacy

Current Environment

One of today's key business imperatives is maintaining the privacy of your customers' personal information. As business systems and processes become increasingly complex and sophisticated, growing amounts of personal information are being collected. As a result, personal information may be exposed to a variety of vulnerabilities, including loss, misuse and unauthorized access and disclosure. Those vulnerabilities raise concerns for organizations, the government and the public in general.

Maintaining the privacy and protection of customers' and employees' personal information is a risk management issue for all organizations. Research continues to show that customers have widespread distrust of many organizations' business practices, including how they collect, use and retain personal information. The increase in identity theft is a concern for all organizations. Laws and regulations continue to place requirements on businesses for the protection of personal information.

Federal legislation mandates the protection and privacy of personal information for customers, clients and patients. In the health care industry, the Health Insurance Portability and Accountability Act (HIPAA) requires covered entities to follow or address certain information security practices. The financial services industry has standards introduced by the Gramm-Leach-Bliley Act (GLBA). Individual states have also asserted their prerogatives in the absence of certain national privacy laws. For example, an issue active for several years and vastly accelerated in 2005 is regulation by states when data security breaches involve personal information. 45 states currently have security breach laws, and Congress continues to investigate. A national law has yet to evolve, with the ultimate scope of such a potential law remaining unknown.

Generally Accepted Privacy Principles (GAPP) have been developed from a business perspective, referencing some, but by no means all, significant local, national and international privacy regulations. GAPP operationalizes complex privacy requirements into a single privacy objective that is supported by 10 privacy principles. Each principle is supported by objective, measurable criteria that form the basis for effective management of privacy risk and compliance in an organization. Illustrative policy requirements, communications and controls, including monitoring controls, are provided as support for the criteria.

This document sets out to describe the privacy principles that can be used by any organization as part of its privacy program. GAPP has been developed to help management create an effective privacy program that addresses privacy risks and obligations and business opportunities.

This introduction and the set of privacy principles and related criteria will be useful to those who:

- Oversee and monitor privacy and security programs
- Implement and manage privacy in an organization
- Implement and manage security in an organization
- Oversee and manage risks and compliance in an organization
- Assess compliance and audit privacy and security programs
- Regulate privacy

What Is Privacy?

Privacy is defined in *Generally Accepted Privacy Principle*s as "the rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure and disposal of personal information."

Personal Information

Personal information (sometimes referred to as personally identifiable information) is information that is about, or can be related to, an identifiable individual. Individuals, for this purpose, include prospective, current and former customers, employees and others with whom the entity has a relationship. Most information collected by an organization about an individual is likely to be considered personal information if it can be attributed to an identified individual. Some examples of personal information are as follows:

- Name
- Home or email address
- Identification number (for example, a Social Security or Social Insurance number)
- Physical characteristics
- Consumer purchase history

Some personal information is considered sensitive. Some laws and regulations define the following to be sensitive personal information:

- Information on medical or health conditions
- Financial information
- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Sexual preferences
- Information related to offenses or criminal convictions

Sensitive personal information generally requires an extra level of protection and a higher duty of care. For example, some jurisdictions may require explicit consent rather than implicit consent for the collection and use of sensitive information.

Some information about or related to people cannot be associated with specific individuals. Such information is referred to as *nonpersonal information*. This includes statistical or summarized personal information for which the identity of the individual is unknown or linkage to the individual has been removed. In such cases, the individual's identity cannot be determined from the information that remains, because the information is deidentified or anonymized. Nonpersonal information ordinarily is not subject to privacy protection because it cannot be linked to an individual. However, some organizations may still have obligations over nonpersonal information due to other regulations and agreements (for example, clinical research and market research).

Privacy or Confidentiality?

Unlike personal information, which is often defined by law or regulation, no single definition of confidential information exists that is widely recognized. In the course of communicating and transacting business, partners often exchange information or data that one or the other party requires be maintained on a need-to-know basis. Examples of information that may be subject to a confidentiality requirement include the following:

- Transaction details
- Engineering drawings
- Business plans
- Banking information about businesses
- Inventory availability
- Bid or ask prices
- Price lists
- Legal documents
- Revenue by client and industry

Also, unlike personal information, rights of access to confidential information to ensure accuracy and completeness are not clearly defined. As a result, interpretations of what is considered confidential information can vary significantly from organization to organization and, in most cases, are driven by contractual arrangements.

Why Privacy Is a Business Issue

Good privacy is good business. Good privacy practices are a key part of corporate governance and accountability. One of today's key business imperatives is maintaining the privacy of personal information. As business systems and processes become increasingly complex and sophisticated, organizations are collecting growing amounts of personal information. As a result, personal information is vulnerable to a variety of risks, including loss, misuse, unauthorized access and unauthorized disclosure. Those vulnerabilities raise concerns for organizations, governments and the public in general.

Organizations are trying to strike a balance between proper collection and use of their customers' personal information. Governments are trying to protect the public interest and at the same time, manage their cache of personal information gathered from citizens. Consumers are very concerned about their personal information, and many believe they have lost control of it. Furthermore, the public has a significant concern about identity theft and inappropriate access to personal information, especially financial and medical records, and information about children.

Individuals expect their privacy to be respected and personal information to be protected by the organizations with which they do business. They are no longer willing to overlook an organization's failure to protect their privacy. Therefore, *all* businesses need to effectively address privacy as a risk management issue. The following are specific risks of having inadequate privacy policies and procedures:

- Damage to the organization's reputation, brand or business relationships
- Legal liability and industry or regulatory sanctions
- Charges of deceptive business practices
- Customer or employee distrust
- Denial of consent by individuals to have their personal information used for business purposes
- Lost business and consequential reduction in revenue and market share
- Disruption of international business operations
- Liability resulting from identity theft

Generally Accepted Privacy Principles

Generally Accepted Privacy Principles as developed by the AICPA and the Canadian Institute of Chartered Accountants (CICA) form a comprehensive resource providing guidance on a number of areas related to privacy. The document, which can be found at aicpa.org/privacy, offers excellent guidance on defining good privacy and security practices for personal information, organized into 10 principles.

The following are the 10 *Generally Accepted Privacy Principles*:

1. **Management.** The entity defines, documents, communicates and assigns accountability for its privacy policies and procedures.
2. **Notice.** The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained and disclosed.
3. **Choice and consent.** The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use and disclosure of personal information.
4. **Collection.** The entity collects personal information only for the purposes identified in the notice.
5. **Use, retention and disposal.** The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes or as required by law or regulation and thereafter appropriately disposes of such information.
6. **Access.** The entity provides individuals with access to their personal information for review and update.
7. **Disclosure to third parties.** The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.
8. **Security for privacy.** The entity protects personal information against unauthorized access (both physical and logical).
9. **Quality.** The entity maintains accurate, complete and relevant personal information for the purposes identified in the notice.
10. **Monitoring and enforcement.** The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related complaints and disputes.

Privacy Risk Matrix

The following table provides an overview of possible privacy risks to which your company may be exposed.

PRIVACY PRACTICE	IF	THEN
Management	If you don't effectively manage your privacy program,	… your customers will take their business elsewhere.
Notice	If you do not provide your customer with your privacy notice,	… you may be in violation of GLBA.
Choice and Consent	If you do not provide your customer with the ability to control when you collect, use and disclose their personal information,	… you may damage customer relations.
Collections	If you collect more personal information than necessary,	… you may create a greater exposure for abuse of that information.
Use, Retention and Disposal	If you use the personal information for purposes other than specified,	… you may lose customer trust.
Access	If you don't give your customers access to their personal information,	... you run the risk of not having accurate customer data.
Disclosure to Third Parties	If your third-party processor uses the personal information of your customers for purposes other than specified in your contract,	... your customer will still hold you accountable for improper use of that information.
Security for Privacy	If you don't protect your customer's personal information,	... you run the risk of a significant security breach.
Quality	If you don't maintain accurate customer data,	… your targeted marketing and sales may suffer.
Monitoring and Enforcement	If you don't effectively monitor your privacy practices,	... you may be subject to fines and penalties.

A breach occurring in any one of these 10 principles may have a detrimental effect on your bottom line. Ignoring these issues only increases the risks to your organization.

Businesses need to have sound privacy practices because they:

- Protect the entity's public image and brand
- Achieve a competitive advantage in the marketplace
- Meet the membership requirements of an industry association
- Efficiently manage personal information and, thereby, reduce administrative costs and avoid unnecessary financial costs, such as retrofitting information systems
- Enhance credibility and promote continued consumer confidence and goodwill

All these reasons have one common denominator: *Good privacy practices make good business sense. Generally Accepted Privacy Principles* are designed to assist organizations in creating an effective privacy program that addresses their privacy risks and business opportunities.

ORTHOGONAL PERSPECTIVES

Traversing the Dimensions of:

- Operations
- IT
- Finance
- Governance

Working in Partnership with
Thomas E Schmitt & Company, LLC

We help our clients develop & implement practical, holistic solutions so they can conduct their business with accountability and control

Visit us at
www.TESchmitt.com

Thomas E. Schmitt, CPA/CITP, CGMA, CISA
Managing Director

Privacy

For more information

To learn more about privacy and how implementing new privacy measures can benefit your organization, please visit **aicpa.org/privacy**

AICPA®

CA Chartered Accountants of Canada

10261-378