

# Generally Accepted Privacy Principles (GAPP) A Framework for Privacy Management

Christine Ravago, CISA, CIPP  
Privacy Risk Advisory Services, Ernst & Young, LLP



# Overview of GAPP - What Does GAPP Address?

The AICPA/CICA privacy framework contains 10 privacy principles and related criteria that are essential to the proper protection and management of personal information. These privacy principles and criteria are based on internationally known fair information practices included in many privacy laws and regulations of various jurisdictions around the world and in common and leading practices.

- ▶ Management
- ▶ Notice
- ▶ Choice and Consent
- ▶ Collection
- ▶ Use and Retention
- ▶ Access
- ▶ Disclosure
- ▶ Security
- ▶ Quality
- ▶ Monitoring and Enforcement

GAPP	US FTC FIPs	Canada PIPEDA	Australia	US Safe Harbor	EU Data Protection Directive	OECD
Management		Accountability			Notification	Accountability
Notice	Notice	Identifying Purposes, Openness	Openness	Notice	Information to be Given to the Data Subject	Purpose Specification, Openness
Choice & Consent	Choice	Consent	Use and Disclosure	Choice	Criteria for Making Data Processing Legitimate, Data Subject's Right to Object	Collection Limitation
Collection		Limiting Collection	Collection, Sensitive Information, Anonymity	Data Integrity	Principles Relating to Data Quality, Exemptions and Restrictions	Collection Limitation (including consent)
Use and Retention		Limiting Use, Disclosure, and Retention	Identifiers, Use and Disclosure	(implied but not specified)	Making Data Processing Legitimate, Special Categories of Processing, Principles Relating to Data Quality, Exemptions and Restrictions, The Data Subject's Right to Object	Use Limitation (including disclosure limitation)
Access		Individual Access	Access and Correction	Access	The Data Subject's Right of Access to Data	Individual Participation
Disclosure		Limiting Use, Disclosure, and Retention	Use and Disclosure, Trans-border Data Flows	Onward Transfer	Transfer of Personal Data to Third Countries	Use Limitation
Security	Security	Safeguards	Data Security	Security	Confidentiality and Security of Processing	Security Safeguards
Quality	Integrity	Accuracy	Data Quality	Data Integrity	Principles Relating to Data Quality	Data Quality
Monitoring & Enforcement	Enforcement	Challenging Compliance	(Enforcement by the Office of the Privacy Commissioner)	Enforcement	Judicial Remedies, Liability and Sanctions, Codes of Conduct, Supervisory Authority and Working Party on the Protection of Individuals with Regard to the Processing of Personal Data	Individual Participation



# Management

The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.

## **Policies & Communications**

- ▶ Privacy policies
- ▶ Communication to internal personnel
- ▶ Responsibility and accountability for policies

## **Procedures & Controls**

- ▶ Review and approval
- ▶ Consistency of privacy policies and procedures with laws and regulations
- ▶ Consistency of commitments with privacy policies and procedures
- ▶ Infrastructure and systems management
- ▶ Supporting resources
- ▶ Qualifications of personnel
- ▶ Changes in business and regulatory environments



# 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.

## **Policies & Communications**

- ▶ Privacy policies
- ▶ Communication to individuals

## **Procedures & Controls**

- ▶ Provision of notice
- ▶ Entities and activities covered
- ▶ Clear and conspicuous



# Choice and Consent

The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, retention, and disclosure of personal information.

## **Policies & Communications**

- ▶ Privacy policies
- ▶ Communication to individuals
- ▶ Consequences of denying or withdrawing consent

## **Procedures & Controls**

- ▶ Implicit or explicit consent
- ▶ Consent for new purposes and uses
- ▶ Explicit consent for sensitive information



# Collection

The entity collects personal information only for the purposes identified in the notice.

## **Policies & Communications**

- ▶ Privacy policies
- ▶ Communication to individuals
- ▶ Types of personal information collected and methods of collection

## **Procedures & Controls**

- ▶ Types of personal information collected and methods of collection
- ▶ Collection limited to identified purpose
- ▶ Collection by fair and lawful means
- ▶ Collection from third parties



# Use and Retention

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.

## **Policies & Communications**

- ▶ Privacy policies
- ▶ Communication to individuals

## **Procedures & Controls**

- ▶ Use of personal information
- ▶ Retention of personal information



# Access

The entity provides individuals with access to their personal information for review and update.

## **Policies & Communications**

- ▶ Privacy policies
- ▶ Communication to individuals

## **Procedures & Controls**

- ▶ Access by individuals to their personal information
- ▶ Confirmation of an individual's identity
- ▶ Understandable information, time frame, and cost
- ▶ Denial of access
- ▶ Updating or correcting personal information
- ▶ Statement of disagreement
- ▶ Escalation of complaints and disputes



# Disclosure

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.

## **Policies & Communications**

- ▶ Privacy policies
- ▶ Communication to individuals
- ▶ Communication to third parties

## **Procedures & Controls**

- ▶ Disclosure of personal information
- ▶ Protection of personal information
- ▶ New purposes and uses
- ▶ Misuse of personal information by a third party



# Security

The entity protects personal information against unauthorized access (both physical and logical).

## **Policies & Communications**

- ▶ Privacy policies
- ▶ Communication to individuals

## **Procedures & Controls**

- ▶ Information security program
- ▶ Logical access controls
- ▶ Physical access controls
- ▶ Environmental safeguards
- ▶ Transmitted personal information
- ▶ Testing security safeguards



# Quality

The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice.

## **Policies & Communications**

- ▶ Privacy policies
- ▶ Communication to individuals

## **Procedures & Controls**

- ▶ Accuracy and completeness of personal information
- ▶ Relevance of personal information



# Monitoring and Enforcement

The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related complaints and disputes.

## **Policies & Communications**

- ▶ Privacy policies
- ▶ Communication to individuals

## **Procedures & Controls**

- ▶ Complaint process
- ▶ Dispute resolution and recourse
- ▶ Compliance review
- ▶ Instances of noncompliance



# Case Study A

A health care company has implemented a new online shopping cart function that involves the collection of credit card numbers, contact information, and e-mail addresses. The e-mail addresses are collected to be shared with the fundraising department to solicit customers for fundraising drives and other donation solicitations.

**Management**

**Access**

**Notice**

**Disclosure**

**Choice and Consent**

**Quality**

**Collection**

**Security**

**Use and Retention**

**Monitoring and Enforcement**



## Case Study B

A financial institution is considering hiring a vendor to shred its hard copy documents that contain sensitive personal information.

**Management**

**Access**

**Notice**

**Disclosure**

**Choice and Consent**

**Quality**

**Collection**

**Security**

**Use and Retention**

**Monitoring and Enforcement**



# Top Privacy Issues for 2008



## Information is Power: Recognizing the Need to Classify Data

- ▶ Organizations must first inventory information and classify it based on sensitivity and impact.
- ▶ While many organizations have data classification policies in place, those may be:
  - ▶▶ Outdated (created prior to the emergence of the current privacy risks)
  - ▶▶ Overly broad (limited high level categories with only general security requirements associated with them)
  - ▶▶ Inaccurate in designating risk thresholds to certain data elements

### **Have you?**

- ▶ Inventoried your personal information across your systems, databases, and repositories of data for manual processes?
- ▶ Recently reviewed and updated your data classification policy to ensure it addresses relevant regulations risks?



## Less is More: Sanctioning the Use of Personal Information

- ▶ Limiting the collection, use, disclosure, and retention of information helps limit privacy risks to the organization
  - ▶▶ Eliminate, truncate, redact, or obfuscate
- ▶ Applications:
  - ▶▶ Data transfer (e.g. email, portable media)
  - ▶▶ To particular data elements (e.g., Social Security numbers, credit card numbers)
  - ▶▶ Disclosures to third parties

### **Have you?**

- ▶ Identified opportunities to limit the collection, use, disclosure, and retention of personal information through information minimization?
- ▶ Looked to limit personal information that is stored on portable media devices or sent via email?
- ▶ Identified specific data elements that should be minimized across the organization, and/or in communications with third parties?



## The World in Your Palm: Personal Information on Portable Devices

- ▶ Data warehouses maintain perhaps tera-bytes and peta-bytes of information about customers and employees, and similar amounts are written to disk or tape, pushed to laptop computers, and transmitted through email systems to handheld devices.
- ▶ Loss and theft of this equipment and media is the foremost trigger for security breach notification
- ▶ Need to have clear policy and procedures for:
  - ▶ Protection
  - ▶ Minimization

### **Have you?**

- ▶ Established policy or guidelines over the use of personal information with portable computing and media?
- ▶ Considered network-based back-up solutions to reduce the amount of personal information being transferred with portable media?
- ▶ Reviewed your retention policies for the consideration of portable media devices, and provided guidance to employees on how to stay on top of retention limits?



## To Decode or Not Decode: The Evolving Use of Encryption

- ▶ The practice of encrypting portable devices, portable media, and computer communications (including email messages and their attachments) are trending to become commonplace.
- ▶ For organizations already using encryption, this will mean maturing and streamlining the use of existing procedures and solutions:
  - ▶▶ Identifying specific tools and applying them consistently
  - ▶▶ Upgrading from folder-based to full-drive encryption of portable media for better coverage

### **Have you?**

- ▶ Identified encryption solutions for portable media and communications containing personal information?
- ▶ Identified opportunities to manage those solutions more effectively so encryption can be more commonly available and cost effective?



## The Three-Legged Stool: Enforcing Strict Standards With Vendors and Business Partners

- ▶ Sharing personal information with vendors and business partners is commonplace and, in fact, a necessity in today's marketplace.
- ▶ Not yet common are effective programs that consistently apply and monitor how privacy is managed once personal information leaves the organization.

### **Have you?**

- ▶ Identified personal information exchanged with third parties, and how it is secured and used by the third parties?
- ▶ Defined privacy and data protection requirements for third parties, and a process that involves periodic and ongoing assurance around the controls that the third parties have put in place over the personal information?



## On the Road Again: Personal information and the Telecommuter's Way of Life

- ▶ Whether from home, the road, or a coffee shop, more organizations support an increasing number of teleworkers, extending the enterprise to uncontrolled territory and using networks and computing devices that may not have been provided by the organization.
- ▶ Extending security to this arrangement, protecting personal information processed in these often portable devices, and training people who work in these environments in the safe handling of personal information are key challenges.

### **Have you?**

- ▶ Equipped mobile and telework devices with security features, including virus protection, spyware protection, firewalls, and encryption solutions?
- ▶ Trained mobile and teleworkers on protection of personal information in these environments?



## In Case of Emergency: Having a Plan for the Worst Case Scenario

- ▶ The need for effective and timely management of privacy events and incidents remains a critical issue for all organizations.
- ▶ Potential compromises occur frequently, even in the best run organizations, and repeatable, formal, effective processes to determine the nature of an event and the steps needed to take in response are needed.
- ▶ Maturity in this involves not just responding to events but more importantly stemming the potential damage to the organization and to potentially affected individuals.

### **Have you?**

- ▶ Established a process to manage events and incidents involving personal information?
- ▶ Tested the process and shown it to be effective?



## It's a Small World: Developing Privacy Procedures for Home and Abroad

- ▶ Business trends spread data, including personal information, seamlessly across the globe and to various parties:
  - ▶ Accelerating business models
  - ▶ Globalization of businesses, markets, and workforces
  - ▶ Harmonization of systems and processes
- ▶ Privacy regulators are more active with inquiries, audits, and enforcement activities, sometimes reactively to employee and customer complaints and sometimes proactively.

### **Have you?**

- ▶ Cataloged trans-border transfers of personal information within the corporation and among third parties?
- ▶ Addressed the legitimacy of all such transfers?



## Building a Better Mousetrap: Keeping Pace With Technology to Manage Privacy

- ▶ Any organization has some form of activity that can be considered to be monitoring adherence to policies and the effectiveness of controls.
- ▶ Monitoring now needs to be considered in the context of effectiveness of:
  - ▶▶ A privacy program
  - ▶▶ Joint or overlapping compliance activities
  - ▶▶ Balancing privacy risk and business value

### **Have you?**

- ▶ Developed a risk-based plan for monitoring the use of personal information?
- ▶ Identified gaps in capabilities for monitoring certain operations and the tools that the organization can obtain to close those gaps?
- ▶ Reviewed your monitoring activities for compliance with relevant regulations?



## The Buddy System: Including Internal Audit in Privacy Management

- ▶ Internal audit departments should reflect upon their existing expertise in with privacy.
- ▶ Leading international organizations for auditors, including those specifically serving internal audit professionals, have been developing audit criteria, guidance, and other resources that can be used both for helping organizations meet their risk and compliance needs, and for assessing them.
- ▶ Need to continuously educate internal audit and integrate it into corporate initiatives.

### **Have you?**

- ▶ Ensured internal audit has the necessary resources to assess the organization's privacy risks?



## Contact Information

**Christine Ravago, CISA, CIPP**

christine.ravago@ey.com

Privacy Risk Advisory Services,

Ernst & Young LLP

8484 Westpark Drive

McLean, VA 22102

+1-703-747-1686

[www.ey.com/privacy](http://www.ey.com/privacy)





# Questions



ERNST & YOUNG

[www.ey.com/privacy](http://www.ey.com/privacy)

© 2008 Ernst & Young.  
All Rights Reserved.  
Ernst & Young is  
a registered trademark.