

PRIVACY HORIZONS: TERRA INCOGNITA

29th International Conference of
Data Protection and Privacy Commissioners

September 25 to 28, 2007
Montreal, Canada



LES HORIZONS DE LA PROTECTION DE LA VIE PRIVÉE : TERRA INCOGNITA

29^e Conférence internationale des commissaires
à la protection des données et de la vie privée

du 25 au 28 septembre 2007
Montréal, Canada

Generally Accepted Privacy Principles

A Global Privacy Framework

Nicholas F. Cheung, CA, CIPP/C

The Canadian Institute of Chartered Accountants

Why Is the Accounting Profession Involved with Privacy?

- Privacy is a risk management issue
 - Accountants are trusted business advisors
 - Goes “hand in glove “ with internal control assessments
- Need for external assurance regarding an organization’s privacy practices
 - CAs are recognized for their audit expertise
 - Any audit requires an examination against “suitable criteria”
- Standard setting experience
 - CICA sets accounting and assurance standards for businesses, not-for-profit organizations and government

What are Generally Accepted Privacy Principles (GAPP)?

- **A privacy framework to help both public and private entities develop and assess their privacy program and privacy risk**
- **Developed by the CICA and AICPA**
 - To create a common North American standard
 - Endorsed and supported by:
 - ISACA – Information System and Audit Control Assoc
 - IIA – The Institute of Internal Auditors

Generally Accepted Privacy Principles

- Management
- Notice
- Choice & Consent
- Collection
- Use & Retention
- Access
- Disclosure to Third Parties
- Security for Privacy
- Quality
- Monitoring & Enforcement

GAPP	Australia	Canada PIPEDA	EU Data Protection Directive	Global Privacy Standard
Management		Accountability	Notification	Accountability
Notice	Openness	Identifying Purposes, Openness	Information to be Given to the Data Subject	Purposes, Openness
Choice & Consent	Use and Disclosure	Consent	Criteria for Making Data Processing Legitimate, Data Subject's Right to Object	Consent
Collection	Collection, Sensitive Information, Anonymity	Limiting Collection	Principles Relating to Data Quality, Exemptions and Restrictions	Collection Limitation
Use and Retention	Identifiers, Use and Disclosure	Limiting Use, Disclosure, and Retention	Making Data Processing Legitimate, Special Categories of Processing, Principles Relating to Data Quality, Exemptions and Restrictions, The Data Subject's Right to Object	Use, Retention & Disclosure Limitation
Access	Access and Correction	Individual Access	The Data Subject's Right of Access to Data	Access
Disclosure	Use and Disclosure, Trans-border Data Flows	Limiting Use, Disclosure, and Retention	Transfer of Personal Data to Third Countries	Use, Retention & Disclosure Limitation
Security	Data Security	Safeguards	Confidentiality and Security of Processing	Security
Quality	Data Quality	Accuracy	Principles Relating to Data Quality	Accuracy
Monitoring & Enforcement	(Enforcement by the Office of the Privacy Commissioner)	Challenging Compliance	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	Compliance

The Benefits of GAPP

- **Comprehensive**
 - Framework of over 60 measurable and relevant criteria
 - Not just a list of principles
- **Objective**
 - Developed by the auditing profession to
 - Address international expectations
 - Create a basis for comparability
 - Universally available at no charge
- **Relevant**
 - Widespread use and recognition
 - Applicable for evaluating privacy risk enterprise-wide
- **Recognized as suitable criteria for a privacy audit**
 - Can also be the basis for an internal assessment

Example of GAPP Criteria

Ref	Security for Privacy Criteria	Illustrations and Explanations of Criteria	Additional Considerations
8.2.3	<p>Physical Access Controls</p> <p>Physical access is restricted to personal information in any form.</p>	<p>Systems and procedures are in place to:</p> <ul style="list-style-type: none"> • Manage logical and physical access to personal information, including hard copy, archival, and backup copies. • Log and monitor access to personal information. • Prevent the unauthorized or accidental destruction or loss of personal information. • Investigate breaches and attempts to gain unauthorized access. • Communicate investigation results to appropriate privacy executive. • Maintain physical control over the distribution of reports containing personal information. • Securely dispose of waste containing confidential information. 	<p>Physical safeguards may include the use of:</p> <ul style="list-style-type: none"> • locked file cabinets • Card access systems • physical keys • sign-in logs • other techniques <p>to control access to offices, data centers, and other locations in which personal information is processed or stored.</p>

External Reports for Privacy

- Benefits of third-party assurance
 - Independent
 - Objective
 - Trained in audit techniques
- Why Is This Important
 - Strengthen customer confidence
 - Provide useful reports to internal and external stakeholders
 - Required as part of a contract

Specified Procedures Engagement

- What Is It?
 - A special type of engagement where the procedures are agreed upon by the client and the public accountant
 - Accountant provides a report listing any exceptions found
 - Not an audit opinion
 - Limited distribution of report
- When Would This Be Useful?
 - Organization may not be ready for an audit, but want to provide a third-party report on privacy
 - Could use selected criteria from GAPP
 - More cost effective than an audit

External Audit

- What Is It?
 - Similar to auditor's report used for financial statements (GAPP vs. GAAP)
 - Provides reasonable assurance
 - Unlimited distribution of report
- When Would This Be Useful?
 - Provide assurance to
 - Customers and prospective customers
 - Employees / Board of Directors
 - Regulatory and government bodies
 - To obtain assurance over privacy practices of a 3rd-party vendor (outsourcing contract requirement)

Other Uses of GAPP

- Privacy Risk Assessment
 - Diagnose new or current privacy program
 - Cannot be relied upon for legal compliance
- Benchmarking
 - Against GAPP criteria or compare results against prior GAPP assessments
 - Can be used in a local, national or international context
- Privacy Notice Development

Contact Info

www.cica.ca/privacy

Nicholas F. Cheung, CA, CIPP/C
Principal, Assurance Services Development
CICA

(416) 204-3251
nicholas.cheung@cica.ca

