Analysis of Privacy Principles: Making Privacy Operational

International Security, Trust and Privacy Alliance

Version 2.0
May 2007

ISTPA
INTERNATIONAL SECURITY TRUST & PRIVACY ALLIANCE

This Page Intentionally Left Blank

Published by the International Security, Trust and Privacy Alliance (ISTPA)

ISTPA gratefully acknowledges the following authors, researchers and reviewers, as well as many external privacy experts who reviewed drafts and provided thoughtful comments and feedback.

Adriaan Veldhuisen, NCR Corporation, Principal Author
Mark Kohras, Ryerson University, Toronto, Principal Researcher
Eugene Bacic, Bell Security Solutions, Inc, Contributing Researcher
John Sabo, CA, Inc. Editor and Co-Author
Michael Willett, Seagate Technology, Chair, Framework WG and Co-Author
Scott Blackmer, Technology Law & Consulting, Co-Author
Michele Drgon, DataProbity, Co-Author
Mike Gurski, Bell Security Solutions, Inc., Co-Author
John Hopkinson, President, ISSEA, Contributing Reviewer
Kevin O'Neil, CYVA Research Corporation, Co-Author
Howard Simkevitz, Goodman, Carr, & Wakefield LLP, Contributing Reviewer
Peter Stajov, Contributing Researcher

Contents

1. AUDIENCE AND EXECUTIVE SUMMARY

Although initiated as an internal research paper, this document may also have two external audiences: privacy compliance officers and technical managers responsible for establishing privacy policies and controls in organizations. Additionally, this document can guide implementation of privacy principles and stimulate more technical specification work, especially in appropriate standards organizations. Since the document is largely self-contained, a general audience can reference the *Analysis of Privacy Principles: Making Privacy Operational* as they consider how new or revised privacy legislation and rules may impact implementation.

We wish to acknowledge the valuable contribution of external reviewers, particularly privacy officers responsible for implementing privacy policies in large organizations and ensuring privacy compliance. Because of such input, we specifically added one "regional" instrument to the analysis: the influential California Security Breach Notification Legislation, SB 1386. Although the international influence of this law and the impact of its implementation in the United States are both well established, its specific focus on a narrow component of privacy added an additional dimension to our observations regarding the Enforcement principle.

1.1. Executive Summary

The ISTPA Privacy Framework is an open, policy-configurable model consisting of 10 integrated privacy services, designed to facilitate a template for architecting and implementing privacy management solutions. Given the major changes in information privacy since the publication of the Framework in 2002, and because language and context differ across relevant legislation, directives, conventions and standards, ISTPA initiated this *Analysis of Privacy Principles: Making Privacy Operational* as a structured review of major privacy instruments to ensure that the ISTPA Framework Services in fact can be used to support all common privacy "requirements."

As a further motivation, in 2003-2004 the International Systems Security Engineering Association (ISSEA) in coordination with ISTPA submitted the Framework as a candidate ISO Publicly Available Specification. In response to this submission, the 26th International Conference of Data Protection and Privacy Commissioners in Wroclaw, Poland formally requested that ISTPA/ISSEA withdraw the Framework from the ISO balloting process, requesting that ISTPA consider certain privacy issues, including the concepts of data scarcity, minimization and anonymity, which were not explicitly addressed in the Framework. This study is an important component for addressing these issues.

A key consideration reflected in this *Analysis* is the recognition that language and context differ across international legislation, directives, conventions and standards. Therefore, the study's approach is to provide a *structured* review of major, representative international privacy instruments. The twelve instruments selected for detailed evaluation include, in chronological order:

- The Privacy Act of 1974 (U.S.)
- OECD Privacy Guidelines
- UN Guidelines Concerning Personalized Computer Files

- EU Data Protection Directive 95/46/EC
- Health Insurance Portability and Accountability Act (HIPAA) Privacy Regulations
- Canadian Standards Association Model Code (incorporated in the Personal Information Protection and Electronic Documents Act [PIPEDA])
- US FTC statement of Fair Information Practice Principles
- US-EU Safe Harbor Privacy Principles
- Australian Privacy Act – National Privacy Principles
- California Senate Bill SB 1386, "Security Breach Notification"
- Japan Personal Information Protection Act
- APEC (Asia-Pacific Economic Cooperation) Privacy Framework

The study methodology includes the use of a working set of privacy principles in order to facilitate cross-instrument mapping while also accommodating their many variations in the twelve instruments. These privacy principles are Accountability, Notice, Consent, Collection Limitation, Use Limitation, Disclosure, Access and Correction, Security/Safeguards, Data Quality, Enforcement, and Openness.

Using direct references extracted from each instrument, mapped against these terms in tabular format, the *Analysis* compares and correlates the language in each instrument associated with these key principles and identifies in nine instances where a particular principle is composed of additional, definable components. For purposes of this study, we use the term "requirements" to characterize these more detailed components.

For example, Notice, as defined and expressed in the twelve instruments, is more accurately understood as a set of five related but discrete requirements (Notice of Collection, Policy Notification, Changes in Policy or Data Use, Language and Timing of Notification).

Other principles having sub-components include

- Consent (Sensitive Information, Informed Consent, Change of Use Consent, and Consequences of Consent Denial)
- Collection Limitation (Limitation of Consent, and Fair and Lawful Means)
- Use Limitation (Acceptable Uses and Data Retention)
- Disclosure (Third Party Disclosure, Third Party Policy Requirements, and Disclosure for Legal and Health Reasons)
- Access and Correction (Access to Information, Proof of Identity, Provision of Data, Denial of Access, and Correcting Information)
- Security/Safeguards (Safeguards and Destruction of Data)
- Enforcement (Ensuring Compliance, Handling Complaints, and Sanctions)
- Openness (Public Policies and Establishing Existence of Personal Data)

The Study also determined that three additional privacy requirements are expressed in these international privacy instruments: anonymity, data flow and data sensitivity.

As a consequence of this analysis and findings, the study provides a set of composite, operational definition for each principle. These operational definitions include the sub-components described above.

In summary, this *Analysis* is a practical first step in framing the huge variations in language and the differing placement of many principles/practices in international privacy law, regulations and directives. It enables ISTPA to test the ISTPA Privacy Framework's completeness and to identify areas for Framework revision reflecting the inherent complexity and interdependence of privacy and data protection laws, directives and policies as well as the evolution of privacy requirements and expectations since the

Framework's first publication in 2002. The *Analysis* may also be useful to external audiences: the privacy officer, those persons responsible for establishing privacy policies and controls in organizations, and standards bodies having an interest in privacy.

2. ISTPA INTRODUCTION

2.1. Overview of the ISTPA Organization

Founded in 1999, the International Security, Trust, and Privacy Alliance (ISTPA) is a global alliance of companies, institutions, and expert practitioners working together to address evolving issues related to privacy from an implementation perspective. Our goal is to develop and maintain a Framework for the protection of personal data, which defines security, trust, and privacy Services and Functions, and their inter-relationships.

The ISTPA Privacy Framework is an open, policy-configurable model consisting of 10 integrated privacy services, designed to facilitate a template for architecting and implementing solutions to meet privacy management requirements internationally.

ISTPA Projects

- **Analysis of Privacy Principles**

Assessing the development and evaluation of privacy and data protection regulations, this detailed Analysis proposes a common basis for understanding core components of operational privacy.

- **Improve and Revise the ISTPA Privacy Framework**

With input from the practical application of the Framework through the Analysis, the ISTPA Privacy Framework is being revised and updated to improve its usefulness in solving real-world privacy management requirements.

- **ISTPA-ISSEA Project: Map Security Safeguards to ISTPA Privacy Framework**

Using the International Systems Security Engineering Association (ISSEA) Maturity Model for Information Security, information security controls will be mapped to the ISTPA Privacy Framework services.

- **Master Tool Set for Privacy**

Given any set of privacy principles or practices (input requirements), the ISTPA Tool Set will enable conversion or mapping of these requirements into detailed actions under each Privacy Framework Service. The ISTPA Tool Set will be available for piloting against actual requirements. An automation tool for the Tool Set exercise is also being explored.

2.2. Motivation for the Analysis of Privacy Instruments

The ISTPA Privacy Framework, or any operational privacy framework, must support all core privacy principles and their functional implementation. Because language and context differ across relevant legislation, directives, conventions and standards, a key objective for ISTPA was to conduct a structured review of major, representative international privacy instruments to ensure that the ISTPA Framework Services in fact support common “requirements” derived from a review of these instruments. (Recognizing that the breadth of international, national, and regional laws and standards

makes a comprehensive analysis of all such instruments out of scope for this project, ISTPA nevertheless believes that the methodology used for this study may form the basis for additional research.)

Additionally, our review was undertaken as a consequence of the submission of the ISTPA Privacy Framework in 2003 by ISSEA as a candidate ISO Publicly Available Specification (PAS) *(ISO/IEC (PAS) DIS 20886).* In response to this submission, the 26th International Conference of Data Protection and Privacy Commissioners in Wroclaw, Poland formally requested in 2004 that ISTPA/ISSEA withdraw the Framework from the ISO balloting process to work on certain issues that they considered important to the international data protection community, in particular:

- development of a privacy technology standard that would support the implementation of legal rules on privacy and data protection where they exist and the formulation of such rules where they are still lacking, and
- development of an international privacy standard based on the fair information practices as well as the concepts of data scarcity, minimization and anonymity.

It is our belief that the research and analysis represented in this document provide a basis for ISTPA to address these two issues. The Analysis will be used to test the ISTPA Privacy Framework's completeness and as a basis for a major revision of the Framework.

2.3. Overview of the ISTPA Framework

We recognize information privacy as being the proper collection, management, use and destruction of personal information throughout its life cycle, consistent with data protection principles and the preferences of the subject, and as defined by laws and regulations. We use the term Personal Information to denote any data related to an individual[1] regardless of whether the subject of the personal information is identifiable. Worldwide, especially with the rapid onset of web-based and networked e-business and e-government programs, systems and applications, privacy concerns have intensified. Legislation has been enacted to establish ground rules for handling certain kinds of personal information as well as to address specific issues associated with privacy, such as notifying data subjects following a breach of data security. With this heightened focus on privacy, a policy-configurable framework is valuable, as it will enable particular jurisdictional requirements to serve as input parameters to govern the behavior of the framework components.

(Note: By policy-configurable, we mean that business process and information technology-based system parameters can be set and business operations executed based on objective policy statements derived from any set of laws, regulations or policies.)

For more than 30 years, a set of privacy principles defining Fair Information Practices (FIP) have been evolving in the business and government sectors for the handling of personal information. In the ISTPA Privacy Framework v1.1, ISTPA views FIP as representing definable actions that are necessary to support privacy principles:

- Notice and Awareness
- Choice and Consent
- Access (by the Subject of the Personal Information)

[1] Although some data protection laws protect juridical as well as natural persons, for purposes of this document we have limited our review and analysis to natural persons.

- Information Quality and Integrity
- Update and Correction
- Enforcement and Recourse

The ISTPA Privacy Framework provides a complete template for an implementation of these practices by including operational elements that were missing from the various privacy principles. The Framework however does not specify particular technologies or business processes to be used for the various functions it defines. These choices must be made by implementers, as they deem appropriate for particular environments.

Although in the Framework analysis, the FIP were viewed as fundamental and, at times, static components, they are now understood as more complex and interactive. The FIP serve as high-level guidelines for human, business process, IT system and network behavior toward personal information; however, their operational specifications are in fact typically incomplete and left to the implementer to decipher. We also learned that even the core FIP did not incorporate essential components routinely used in business and IT systems - such as subject agent, interfaces, policy control, and secure repository. These components are also necessary to support a technical, programmatic implementation.

The ISTPA Privacy Framework addresses these missing components and relationships and provides a path and linkage between privacy principles and fair information practices with a more granular embodiment of functionality made possible by a discrete set of services. (In the Framework, a "service" is a collection of related functions and mechanisms that operate for a specified purpose.) In this way, business process and IT architectures, as well as specific implementation mechanisms, can be identified, developed and integrated in business processes and underlying information technology systems.

The ISTPA Privacy Framework also serves as a template for designing privacy management systems and as an analytic tool for assessing privacy solutions. The ISTPA Framework Services, when combined with existing, industry-standard security architectures, creates a robust information privacy management and compliance methodology that can be used within and across jurisdictions.

2.4. ISTPA Privacy Framework Services

As noted above, in the Framework, a "service" is a collection of related functions and mechanisms that operate for a specified purpose. **The following 10 operational services constitute the current ISTPA Framework:**

- The **Audit Service** handles the recording and maintenance of service events from other services. It captures, into privileged audit logs, necessary audit data to ascertain compliance with governing policies and procedures derived from agreements, an organization's internal policies, and any applicable law or regulation.

- The **Certification Service** supports the management and affirmation of credentials of any responsible party or service involved in processing Personal Information. Security, in terms of Authentication and Authorization, and trust necessitate services that certify or attest to an actor's or system component's compliance and trustworthiness.

- The **Control Service** encompasses the functions that work together to ensure that the Fair Information Practices operate according to prescribed privacy policy on

Personal Information. These functions are maintained and manipulated primarily by data collection controllers or data processing entities.

- The **Enforcement Service** initiates response actions when a data collection or data processing entity does not conform to the terms or policies of an agreement or the applicable regulations. Enforcement also includes recourse for data subjects when their Personal Information is being used differently from the original agreement.

- The **Interaction Service** facilitates a generalized interface as required for raw information presentation and handoff. The concepts are not expressly related to privacy but emphasize the wide range of interactions between the Framework and all entities outside the Framework. The Interaction Service, nevertheless, encompasses such principles as notice and awareness, and choice and consent.

- The **Negotiation Service** provides an individual, about whom Personal Information is collected, an understanding of the purposes for which the data will be used and an opportunity to provide or deny consent or optionally conduct a negotiation.

- The **Validation Service** evaluates data quality in terms of accuracy, completeness and timeliness of Personal Information. Relevance is also included under data quality.

- The **Access Service** ensures that data subjects have access to any Personal Information that a data controller or processor has collected about them. A subject should have the ability to provide changes to that Personal Information as appropriate.

- The **Agent Service** is a software process that acts on behalf of a data subject or a requestor in order to support one or more of the services defined in this Framework. Agent also refers to the data subject in the case of a manual process.

- The **Usage Service** ensures that the active use of Personal Information that is outside the direct control of the subject complies with the terms and policies of any agreement and applicable regulation. It assumes the role of “processing monitor” including linking, integration, inference transfer, derivation, aggregation, and pseudo-anonymization.

2.5. Organization of this Document

We provide the following information to ensure clarity and consistent interpretation of terms used in this requirements specification.

Chapter 1 – **Audience and Executive Summary** - identifies the expected external audience for this Analysis and provides an Executive Summary

Chapter 2 - **ISTPA Introduction** – provides background on the organization, the ISTPA Privacy Framework and the Motivation for this study

Chapter 3 - **Study Introduction** – sets out the process and limitations that evolved as we progressed through this work

Chapter 4 - **Background and Considerations** – examines the elements of privacy and security with a brief historic perspective of the concept of principles as it applies to privacy regulation

Chapter 5 - **Scope and Synopsis of Research Instruments** - provides the title, web link for (English) text, practices and principles that we found within the scope that we set out for our Analysis

Chapter 6 – **Requirements Correlation and Observations –** Detailed research - comparison tables for privacy instruments examined for relationship to the requirements - requirement sources references, study observations, and a resulting requirements definition

Chapter 7 - **General Findings and Conclusions** – analysis and observations for the findings, terminology used and discussion

Chapter 8 – **Appendices** – contains additional information and discussion items related to the Analysis, Sources and Glossary

3. STUDY INTRODUCTION

The ISTPA Privacy Framework is an operational framework for implementing information privacy requirements imposed by law, contract or internal policy. To be useful, this operational framework must (a) reflect all widely accepted fair information practices and principles, as reflected in modern personal data protection laws, directives, conventions, and standards and (b) facilitate their functional implementation.

In this *Analysis of Privacy Principles: Making Privacy Operational*, we publish our detailed analysis of major, representative information privacy instruments. We parsed their expressed requirements into a set of consistent privacy categories and then cross-mapped their essential requirements. Because the terms and context differ among these instruments, a key purpose of this approach was to ensure that the ISTPA Framework Services in fact support common "requirements" derived from a review of these instruments. For purposes of this study, we use the term "requirements" to characterize expressed components of privacy principles. In our view, this exercise was necessary to test the ISTPA Privacy Framework's completeness and to identify areas for possible revision based on the evolution of privacy and data protection law and practice since the Framework's first publication in 2002.

This study neither attempts to select the "ideal" set of privacy requirements nor to suggest that one legislative or policy approach to privacy has precedence over another. Those who control the collection, use or disclosure of personal data must make their own determination as to which laws, regulations and policies apply to them and which policies should be looked upon as models. We have conducted what is essentially a descriptive and analytical exercise and have attempted to harmonize disparate language, definitions and expressed requirements in order to provide a common basis for a true operational privacy framework. To ensure that this work was manageable, we:

- selected a set of twelve influential privacy instruments
- illustrated selected subsets of their stated requirements, recognizing that there are many more available for analysis and that in a few instances certain requirements might fit into more than one category
- verified that the more recent sets of information privacy principles are broadly similar to older ones, although we found a few requirements that only appear in newer regulations, such as specific types of data sensitivity
- limited our research to those documents published in English
- analyzed the requirements for commonalities and differences
- used the results of analysis to prepare findings usable for the ISTPA Privacy Framework revision and additional work

4. BACKGROUND AND CONSIDERATIONS

4.1. Background

The *Analysis of Privacy Principles: Making Privacy Operational* provides a template for analysis of privacy and data protection laws and directives around the world, evaluating similarities, dissimilarities and providing analysis regarding their manageability. This section introduces the analysis of privacy principles and the FIP that serve as the design requirements for an operational privacy framework. The effective definition of privacy, as reflected in the practices across the life cycle of Personal Information, motivates the set of privacy services in the ISTPA Privacy Framework.

4.2. Security Components of Privacy

The ISTPA Privacy Framework treats security as integral to all Framework services but intentionally does not specifically address security controls with respect to each service. In the following research and analysis, ISTPA is addressing security more directly.

The concept of security to protect personal data, systems and networks is well-accepted, and most of the statements of the FIP include the principle of information security (sometimes called safeguards), but usually with very little substantive guidance. Although Safeguards is one of the privacy principles included in this study, ISTPA recognizes that information security is a well-understood discipline and has an extensive body of knowledge, including theory, standards, practices, models, services and mechanisms. ISTPA also recognizes that security controls are applicable to all other privacy principles in some manner. However, for purposes of this study we do not explore security/safeguards in depth.

The EU Data Protection Directive has much to say on this subject, and some of the Member States (notably Austria, Belgium, France, Italy, and Spain, in addition to Norway among the EEA countries) have adopted more detailed regulations on securing personal data, especially the more sensitive categories of personal data (typically including health and financial data). Valuable national and international standards and recommendations that are directly relevant to securing personal data in the context of information privacy are:

- *OECD Information Security Guidelines* [2002]
- ISO 17799 [2000 and 2005 versions] and BS 7799 [1999, with Part B]
- ISO 15408 Common Criteria
- NIST publications such as *FIPS 201, Personal Identity Verification of Federal Employees and Contractors and its Computer Security Incident Handling Guide*
- *TechNet Corporate Information Security Evaluation for CEOs*
- *Federal Information Security Management Act of 2002 (FISMA)* includes a mandate to NIST to develop information security standards for controls over federal information assets, which include massive amounts of personal data)
- Payment Card Industry (PCI) Data Security Standard for securing credit and debit card information and transactions (2005)
- TRUSTe checklist of security measures to protect personal information online
- U.S. GLBA and HIPAA security rules to protect personal financial and medical information, respectively
- FTC consent decrees defining security measures to protect consumer data

- ISSEA SSE-CCM
- COSO and COBIT IT control frameworks, used by many US companies to assess their information security in connection with Sarbanes-Oxley compliance
- *Institute of Internal Auditors 2005 GTAG (Global Technology Audit Guide)*, "Information Technology Controls" (which expressly refers to privacy requirements)

4.3. Privacy Principles

Privacy principles are design points in the ISTPA Framework describing proper handling of Personal Information - see http://www.istpa.org/pdfs/ISTPAPrivacyFrameworkV1.1.pdf

Origin of Privacy Principles

The United States Department of Health, Education and Welfare Advisory Committee on Automated Personal Data Systems submitted an early formulation of information privacy principles as a list in its report, *Records, Computers and the Rights of Citizens* (July 1973). See http://www.epic.org/privacy/hew1973report . The Committee was asked to analyze and make recommendations about:

- *Harmful consequences that may result from using automated personal data systems*
- *Safeguards that might protect against potentially harmful consequences*
- *Measures that might afford redress for any harmful consequences*
- *Policy and practice relating to the issuance and use of Social Security numbers*

The Committee provided two sets of Privacy Principles, one set being the Safeguards for Personal Privacy based on the concept of certain fundamental principles of the FIP:

- *There must be no personal-data record-keeping systems whose very existence is secret.*
- *There must be a way for an individual to find out what information about him is in a record and how it is used.*
- *There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.*
- *There must be a way for an individual to correct or amend a record of identifiable information about him.*
- *Any organization creating, maintaining, using or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.*

  These principles should govern the conduct of all personal-data record-keeping systems. Deviations from them should be permitted only if it is clear that some significant interest of the individual data subject will be served or if some paramount societal interest can be clearly demonstrated; no deviation should be permitted except as specifically provided by law.

The second set was Recommended Safeguards for Administrative Personal Data Systems:

- *Any organization maintaining a record of individually identifiable personal data, which it does not maintain as part of an administrative automated*

> *personal data system, shall make no transfer of any such data to another organization without the prior informed consent of the individual to whom the data pertain, if, as a consequence of the transfer, such data will become part of an administrative automated personal data system that is not subject to these safeguard requirements.*

Note that this speaks in general terms of the need for a "personal data system," but these principles, if properly implemented, require administrative and legal as well as technical resources.

The HEW report became the foundation for the Privacy Act of 1974 (US), which regulates the handling of personal data in US federal government databases. Similar principles are found in the early data protection acts adopted in the 1970s in Hesse, Sweden, and France. These principles are also reflected in international guidelines or conventions later promulgated by the OECD, the Council of Europe, the International Labour Organization, the United Nations, the European Union and APEC.

The Legal Privacy Landscape

Commonly accepted principles of the FIP are incorporated in the more recent comprehensive data protection laws enacted in Europe, Canada, Japan, Australia and several other jurisdictions. The most common model is the EU Data Protection Directive (95/46/EC). In addition to the 25 European Union countries and three additional EEA countries, nine other European countries or dependencies have enacted laws to date based on the EU Data Protection Directive. Eight other countries and the Hong Kong SAR have enacted comprehensive data protection laws in other regions of the world and there are similar laws (with somewhat narrower scope) in the Canadian provinces and territories and some of the Australian states. There is also proposed legislation in at least a dozen other countries. Clearly, researching and analyzing language and intent of global privacy is a moving target.

Likewise, concepts of the FIP are also found in sectoral legislation in countries without comprehensive data protection statutes. Leading examples in the United States include the Fair Credit Reporting Act and FACTA amendments; the GLB Financial Modernization Act (GLBA); privacy regulations under HIPAA for health records; the Children's Online Privacy Protection Act; the CAN-SPAM Act; the 23 state acts (as of September 2006) requiring notice of security breaches (including California SB 1386); California's AB 1950 (2004) on personal information security and its new online privacy act; and the privacy and freedom of information acts around the world that concentrate on government data holdings, financial services, credit reporting, medical records, telecoms privacy, and online transactions. Again, these sectoral acts are numerous and typically less comprehensive in their treatment of the FIP and principles.

Selecting Representative Sets of Privacy Practices and Principles for Analysis

Sets of privacy practices/principles have proliferated and now appear in a number of forms, including legislation. Those selected for analysis have approximately similar concepts and terminology (often with nuanced differences in their use and definitions), but each typically introduces unique terms or requirements that do not appear in other lists; these unique privacy practices and principles often reflect expected behavior unique to a given jurisdiction. As an example, the EU Data Protection Directive includes specific guidance on the use of automated decision-making (such as credit scoring or job application screening) that is not found on other privacy practices and principles lists.

In undertaking the Analysis, we considered formal privacy practices and principles instruments that we found to be particularly influential on legislation and practice. In chronological order, these are:

- The Privacy Act of 1974 (U.S.)
- Council of Europe Convention 108
- OECD Privacy Guidelines
- UN Guidelines Concerning Personalized Computer Files
- Hong Kong Personal Data (Privacy) Ordinance
- EU Data Protection Directive 95/46/EC
- Health Insurance Portability and Accountability Act (HIPAA) Privacy Regulations
- Canadian Standards Association Model Code (incorporated in the Personal Information Protection and Electronic Documents Act [PIPEDA])
- International Labour Organization (ILO) Code of Practice on the Protection of Workers' Personal Data
- US FTC statement of Fair Information Practice Principles
- US-EU Safe Harbor Privacy Principles
- Ontario Privacy Diagnostic Tool
- Australian Privacy Act – National Privacy Principles
- California Senate Bill 1386, "Security Breach Notification"
- AICPA/CICA Privacy Framework
- Japan Personal Information Protection Act
- APEC (Asia-Pacific Economic Cooperation) Privacy Framework

Using a Selected Set

From this group of 17 instruments we selected twelve for additional research and analysis, and by carefully reviewing their provisions, identified the privacy principles and practices that are common to all; that is, privacy principles and practices that are represented in each source document. We also harmonized terminology and definitions, where necessary, in order to achieve useful review and analysis, recognizing that some nuances may be lost in that translation. Additionally, we also identified a number of privacy principles and practices that were relatively unique. The resulting set of privacy principles and practices was then analyzed, comparisons made, and conclusions drawn, as reflected in this Analysis. In Chapter 5 of this Analysis, we reference the outline of each of these instruments to illustrate their principal privacy components and their terminology.

Chapter 6 of this Analysis includes the research findings and analysis for this selected set of privacy practices/principles sources.

This *Analysis* can be updated in the future, using additional source laws and other instruments, further-refined privacy practices/principles sets, and new methodologies as needed to update and refine the study.

5. SCOPE AND SYNOPSIS OF RESEARCH INSTRUMENTS

As noted above, ISTPA selected the following privacy instruments as representative of the broad range of privacy regulations worldwide. We further analyzed these regulations with respect to the variations in meaning of the common privacy terminology. The instruments are listed in order of enactment or publication. Following is the title of each instrument, an abstract describing the instrument and a list of the practices or principles that were found in the instrument. See also Appendix C: Other Instruments.

5.1. The Privacy Act of 1974

The Privacy Act of 1974 (U.S.) was created in response to concerns about how the creation and use of computerized government databases (defined as systems of records) might impact individuals' privacy rights. It safeguards privacy through creating four procedural and substantive rights in personal data. First, it requires government agencies to show an individual any records kept on him or her (subject to certain exceptions). Second, it requires agencies to observe specific practices when gathering and handling personal data. Third, it places restrictions on how agencies can share an individual's data with other persons and agencies. Fourth, it provides individuals a right of action in the courts to compel the government to conform to these requirements and to compensate individuals for violations.

http://www.usdoj.gov/oip/privstat.htm

1. Openness
2. Individual Participation
3. Collection Limitation and Consent
4. Data Quality and Correction
5. Reliability and Use Limitation

5.2. OECD Privacy Guidelines

The OECD Privacy Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980, motivated by the global development of automated data processing in business and government, consider privacy protection in relation to the automated processing and storage of personal data. The Guidelines were designed to help member countries prepare national legislation and other measures to ensure the protection of privacy as a fundamental human right, with sufficiently similar legal approaches to ensure the free movement of information across borders for legitimate purposes.

http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_119820_1_1_1,00.html

1. Collection Limitation

2. Data Quality
3. Purpose Specification
4. Use Limitation
5. Security Safeguards
6. Openness
7. Individual Participation
8. Accountability

5.3. UN Guidelines Concerning Computerized Personal Data Files

The United Nations Guidelines concerning Computerized Personal Data Files, ("UN Guidelines") adopted by the General Assembly on 14 December 1990, are designed as guidance for nations in adopting legal measures to protect personal data and as guidance for UN agencies and other international organizations in developing their own privacy policies.

http://ec.europa.eu/justice_home/fsj/privacy/instruments/un_en.htm

1. Lawfulness and Fairness
2. Accuracy
3. Purpose Specification
4. Interested-Person Access
5. Non-Discrimination
6. Power to Make Exceptions
7. Security
8. Supervision and Sanctions
9. Transborder Data Flow

5.4. Directive 95/46/EC of the European Parliament

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 (commonly termed the "EU Data Protection Directive") directs the EU Member States to adopt harmonized legal measures to protect individuals with regard to the processing of personal data; the Directive thereby ensures the free movement of personal data within the EU and (subject to similar protections) abroad. The principles embodied in the Directive apply to information in structured paper files as well as electronic databases. The Directive requires the Member States to establish a system of official notification and supervision by an independent Data Protection Authority (DPA), as well as recourse to the courts.

http://europa.eu/scadplus/leg/en/lvb/l14012.htm
(Also http://www.cdt.org/privacy/eudirective/EU_Directive_.html#HD_NM_1)

1. Collection Limitation
2. Purpose Limitation
3. Data Quality & Proportionality
4. Use Limitation
5. Special Categories (sensitive information)
6. Security Safeguards
7. Transparency (Notice)
8. Individual Participation

9. Supervision and Sanctions
10. Transborder Data Flows

5.5. CSA Model Code for the Protection of Personal Information

The CSA Standard CAN/CSA-Q830, Model Code for the Protection of Personal Information is a National Standard of Canada prepared by the Canadian Standards Association and published under the authority of the Standards Council of Canada. The standard was published in May 1996. It addresses concerns about the protection of privacy rights and the individual's right to control the use and exchange of personal information. The standards has since been given the force of law within the scope of the federal Personal Information Protection and Electronic Documents Act (PIPEDA) (2001), and similar provincial statutes, which incorporate the CSA privacy principles.

http://www.apec.org/apec/apec_groups/som_special_task_groups/electronic_commerce.html

1. Preventing Harm
2. Notice
3. Collection Limitations
4. Uses of Personal Information
5. Choice
6. Integrity of Personal Information
7. Security Safeguards
8. Access and Correction
9. Accountability

5.6. Health Insurance Portability and Accountability Act

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) amends the Internal Revenue Code of 1986. HIPAA was designed to improve the portability and continuity of health insurance coverage and reduce the cost of administering health insurance. Because of the anticipated migration of medical records and insurance claims to electronic databases, the US Congress directed the Department of Health and Human Services (HHS) to promulgate privacy regulations. We used the HHS Privacy Rule (45 CFR Parts 160 & 164) (as amended through February 2006) as the source document for this Analysis

http://www.hhs.gov/ocr/combinedregtext.pdf

1. Permitted Use and Disclosure
2. Minimum Necessary Standards
3. Patient Authorization
4. Notice of Privacy Practices
5. De-Identification
6. Limited Data Sets
7. Role-Based Access
8. Training
9. Individuals' Rights

5.7. Safe Harbor Privacy Principles

The EU Data Protection Directive prohibits the transfer of personal data outside the EU and EEA unless there are safeguards (by law, contract, bilateral agreement or otherwise) that "adequately" protect the data. The United States defined a sectoral approach in 2004 that relies on a mix of legislation, regulation, and self-regulation, rather than a comprehensive data protection law on the EU model. In order to bridge these different privacy approaches, the US Department of Commerce and the European Commission developed in 2000 a set of "Safe Harbor Privacy Principles." US companies that certify compliance with these principles are permitted to transfer personal data from Europe to the US, subject to enforcement (in most instances) by the US Federal Trade Commission.

http://www.export.gov/safeharbor/SHPRINCIPLESFINAL.htm

1. Notice
2. Choice
3. Onward Transfer
4. Security
5. Data Integrity
6. Access
7. Enforcement

5.8. Federal Trade Commission Fair Information Practice Principles

The US Federal Trade Commission has taken enforcement action against numerous companies for privacy abuses deemed "unfair or deceptive practices" under section 5 of the Federal Trade Act. To guide businesses in this area, the FTC published its version of "Fair Information Practice Principles" in 2000.

http://www.ftc.gov/reports/privacy3/fairinfo.htm

1. Notice and Awareness
2. Choice and Consent
3. Access and Participation
4. Integrity and Security
5. Enforcement and Redress
    a. Self-Regulation
    b. Private Remedies
    c. Government Enforcement

5.9. Australian National Privacy Principles

The Privacy Amendment (Private Sector) Act 2000 amended the federal Privacy Act and listed ten National Privacy Principles, effective in December 2001, that apply to much of the private sector as well as to the public sector in Australia.

http://www.privacy.gov.au/publications/npps01.html

1. Collection
2. Use and Disclosure
3. Data Quality
4. Data Security
5. Openness
6. Access and Correction
7. Identifiers
8. Anonymity
9. Transborder Data Flows
10. Sensitive Information

5.10. California SB 1386 "Security Breach Notification"

This law, which became effective on July 1, 2003, requires businesses and government agencies to notify California residents with regard to a security breach of certain kinds of unencrypted personal information in a computer database. It is designed to address the crime of identity theft. The California law has become the model for similar laws in more than 35 other US jurisdictions and proposed federal legislation.

http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html

1. Accountability
2. Data Security
3. Notice of Security Breach
4. Enforcement: Fines, Civil Action

5.11. Japan Personal Information Protection Act

Japan Personal Information Protection Act of 2005 is designed to protect individuals' rights and welfare while preserving the usefulness of Personal Information in the public and private sectors.

http://www.ecom.jp/ecom_e/home/research_file/20011119recenttrend.pdf#search=%22Japan%20Personal%20Information%20%20Principles%22

1. Basic Principles
    a. Restrictions according to usage
    b. Appropriate acquisition
    c. Ensuring correctness
    d. Ensuring security
    e. Ensuring clarity
2. Provisions of Obligations
    a. Restrictions according to usage and appropriate acquisition of data
    b. Achieving proper management of data
    c. Restrictions on provision of data to third parties
    d. Publication
    e. Disclosure
    f. Revision
    g. Suspension of Data
    h. Handling complaints
    i. Approval of complaint-handling entities

5.12. APEC Privacy Framework

The guidelines for privacy laws and practices were adopted in 2005 by the 21 members of the intergovernmental Asia-Pacific Economic Cooperation group. The APEC Privacy Framework is expressly intended to be consistent with the "core values" of the OECD Privacy Guidelines, while providing somewhat more detailed guidance based on developments since 1980 and introducing the principle of "preventing harm."

http://www.apec.org/apec/apec_groups/som_special_task_groups/electronic_commerce.html

1. Preventing Harm
2. Notice
3. Collection Limitation
4. Uses of Personal Information
5. Choice
6. Integrity of Personal Information
7. Security Safeguards
8. Access and Correction
9. Accountability

5.13. Privacy Requirements Restructuring Summary

The translation from the above twelve lists of Privacy Practice/Principles into a set of requirements is difficult, to say the least. "Composite Requirements" in Section 2.3 are:

- Notice and Awareness
- Choice and Consent
- Access (by the Subject of the Personal Information)
- Information Quality and Integrity
- Update and Correction
- Enforcement and Recourse

We observed that there is a different set of Principles that is often expressed as common terminology. In trying to adapt the study to this observation we found it necessary to split some Composite Requirements into multiple Restructured Requirements, e.g. Notice and Awareness, and to merge others into one Structured Requirement, e.g. Access *and* Correction. For the basis of the Analysis in Chapter 6, we chose eleven Restructured Requirements, as mapped out in the following table:

Composite Requirement	Restructured Requirement
Notice and Awareness	Openness
	Disclosure
	Notice
Choice and Consent	Collection Limitations
	Use Limitations
	Consent
	Accountability
Access (by the Subject)	Access (not Correction)

Information Quality	Data Quality
	Security/Safeguards
Update and Correction	Correction (not Access)
Enforcement and Recourse	Enforcement

6. REQUIREMENTS CORRELATION AND OBSERVATIONS

What follows is our effort to compare and correlate the key principles found in the leading international privacy instruments, ending in each case with a composite, *operational* definition.

Please note that a major intent of this analysis is to determine the common elements in a group of representative, global privacy instruments and to assess whether it is possible to derive a set of "core" principles. Such a set of core principles would enable ISTPA to:

- ensure that the ISTPA Privacy Framework will in fact reflect all core privacy principles;
- develop usable tools to make the Framework more accessible to practitioners; and
- develop a core set of operational components for use in modeling, IT architecture deign, and taxonomies.

ISTPA recognizes that the following comparative charts, analysis, and general observations are not exhaustive. ***Their primary purpose is to provide a reasonable basis for identifying common elements and exceptions with respect to internationally recognized privacy principles to meet ISTPA objectives and serve as a basis for Framework updates and improvements.*** However, they may also be of use to practitioners seeking to understand in general terms some of the similarities and differences of major international laws and directives.

The table below lists the instruments that we selected for Analysis, in ascending chronological order, and the label that we use to identify the Source References in the following sections of this chapter.

Table of Instruments Selected for Analysis

Instrument	Year	Label
The Privacy Act of 1974	1974	US
OECD Privacy Guidelines	1980	OECD
UN Guidelines Concerning Computerized Personal Data Files	1990	UN
Directive 95/46/EC of the European Parliament	1995	EU
CSA Model Code for the Protection of Personal Information	1996	CSA
Health Insurance Portability and Accountability Act	1996	HIPAA
Safe Harbor Privacy Principles	2000	SH
Federal Trade Commission Fair Information Practice Principles	2000	FTC
Australian National Privacy Principles	2001	ANPP
California SB 1386	2003	CAL
Japan Personal Information Protection Act	2005	JPIPA
APEC Privacy Framework	2005	APEC

6.1. Accountability

Privacy Instruments examined for relationship to Accountability:

- **APEC Privacy Framework** under "Accountability" (Section IX)
- **OECD Guidelines** under "Accountability" (Paragraph 14)
- **EU Data Protection Directive** under "Judicial Remedies, Liability and Sanctions" (Chapter III) and "Supervisory Authority (Chapter VI)
- **CSA Model Code** under "Accountability" (Clause 4.1-4.1.4)
- **California SB 1386** under Section 4.

Accountability Source References:

1. **Accountability**

An organization should be held accountable for Personal Information under its control and complying with applicable privacy policies associated with it.

APEC	"A personal information controller should be accountable for complying with measures that give effect to the Principles stated above." (Paragraph 26)
OECD	"A data controller should be accountable for complying with measures which give effect to the principles stated above." (Paragraph 14)
EU	"The Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive." (Article 24)
CSA	"An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles." (Clause 4.1)
CAL	"Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system" … to any resident of California whose unencrypted personal information was …acquired by an unauthorized person. (e) For purposes of this section, "personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social security number. (2) Driver's license number or California Identification Card number. (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. f) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records".

General Study Observations:

- Accountability clearly must be managed in the implementation of privacy
- Other instruments support accountability (that is, "accountability" is inferred), but do not explicitly use the term; the term 'responsibility' is used in some instances
- Accountability is focused on both individuals and organizations, depending on the particular instrument where it is referenced, and both therefore must be managed
- Accountability must be linked to collecting and auditing privacy actions
- Sanctions must be addressed; sanctions are not defined in the principles themselves, and so would need to be linked
- Privacy Rights Expression Language and taxonomies would be useful, given the general references to "measures" in the source instruments
- For accountability to function effectively, carefully defined Personal Information, and defined operations on Personal Information, are necessary

Composite Operational Definition:

Accountability: Reporting made by the business process and technical systems which implement privacy policies to the individual or entity accountable for ensuring compliance with those policies, with optional linkages to sanctions.

6.2. Notice

Privacy Instruments examined for relationship to Notice:

- **APEC Privacy Framework** under "Notice" (Section II)
- **OECD Privacy Guidelines** under "Purpose Specification" (Paragraph 9, 54)
- **EU Data Protection Directive** under "Information Given to the Data Subject" (Section IV)*
- **Safe Harbor Principles** under "Notice"
- **Health Insurance Portability and Accountability Act (HIPAA)** under "Notice of privacy practices for protected health information" (§ 164.520)
- **UN Guidelines Concerning Computerized Personal Data Files** under "Purpose-Specification" (Paragraph 3)
- **US FTC Fair Information Practices** under "Notice/Awareness" (Section 1)
- **Japan Personal Information Protection Act** under "Notice of Purpose of Use at the Time of Acquisition" (Article 18)
- **Australian National Privacy Principles** under "Collection" (Sub clause 1.3)
- **US Privacy Act** under "Agency Requirements" (Subsection e)
- **CSA Model Code** under "Identifying Purposes" (Clause 4.2-4.2.6)
- **California SB 1386** under Section 4

*It should be noted that the **EU Data Protection Directive** Section IX entitled "Notification" refers to notification of a supervisory authority and *not* to the notification of the Data Subject.

Notice Source References:

1. **<u>Notice of Collection</u>**

Notice must be provided to the Data Subject of the purpose for collecting personal information and the type of data collected.

APEC	"Personal information controllers should provide clear and easily accessible statements about their practices and policies with respect to personal information that should include: b) the purposes for which personal information is collected;" (Paragraph 15)
OECD	"The purposes for which personal data are collected should be specified not later than at the time of data collection…" (Paragraph 9)
EU	"Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it: (b) the purposes of the processing for which the data are intended;" (Article 10)
SH	"An organization must inform individuals about the purposes for which it collects and uses information about them"
HIPAA	"…an individual has a right to adequate notice of the uses and disclosures of protected health information that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to protected health information." [§ 164.520(a)(1)]

UN	"The purpose which a file is to serve and its utilization in terms of that purpose should be specified, legitimate and, when it is established, receive a certain amount of publicity or be brought to the attention of the person concerned…" (Paragraph 3)
FTC	"While the scope and content of notice will depend on the entity's substantive information practices, notice of some or all of the following have been recognized as essential to ensuring that consumers are properly informed before divulging personal information: • identification of the uses to which the data will be put;" (Section 1)
JPIPA	"When having acquired personal information, an entity handling personal information must, except in cases in which the Purpose of Use has already been publicly announced, promptly notify the person of the Purpose of Use or publicly announce the Purpose of Use." (Article 18, Paragraph 1)
ANPP	"At or before the time (or, if that is not practicable, as soon as practicable after) an organization collects personal information about an individual from the individual, the must take reasonable steps to ensure that the individual is aware of: (c) the purposes for which the information is collected;" (Sub clause 1.3)
US	"Each agency that maintains a system of records shall— (3) inform each individual whom it asks to supply information, on the form which it uses to collect the information or on a separate form that can be retained by the individual-- (B) the principal purpose or purposes for which the information is intended to be used;" [Subsection (e)(3)(B)]
CSA	"The identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected." (Clause 4.2.3)

2. <u>Policy Notification</u>

Data Subject must be notified of the applicable policies in terms of Consent, Access and Disclosure.

APEC	"Personal information controllers should provide clear and easily accessible statements about their practices and policies with respect to personal information that should include: e) the choices and means the personal information controller offers individuals for limiting use and disclosure of, and for accessing and correcting, their personal information." (Paragraph 15)
EU	"Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it:

	(c) any further information such as • the recipients or categories of recipients of the data, • whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply, • the existence of the right of access to and the right to rectify the data concerning him" (Article 10)
SH	"An organization must inform individuals about… the choices and means the organization offers individuals for limiting its use and disclosure."
HIPAA	"The notice must contain: (A) A statement that the covered entity is required by law to maintain the privacy of protected health information and to provide individuals with notice of its legal duties and privacy practices with respect to protected health information" [§ 164.520(b)(v)(A)]
FTC	"…the notice should also identify any available consumer rights, including: any choice respecting the use of the data; whether the consumer has been given a right of access to the data; the ability of the consumer to contest inaccuracies; the availability of redress for violations of the practice code; and how such rights can be exercised." (Section 1)
ANPP	"At or before the time (or, if that is not practicable, as soon as practicable after) an organization collects personal information about an individual from the individual, the organization must take reasonable steps to ensure that the individual is aware of: (a) the identity of the organization and how to contact it; and (b) the fact that he or she is able to gain access to the information; and (d) the organizations (or the types of organizations) to which the organization usually discloses information of that kind; and (e) any law that requires the particular information to be collected;" (Sub clause 1.3)
US	"Each agency that maintains a system of records shall— (4) …publish in the Federal Register upon establishment or revision a notice of the existence and character of the system of records, which notice shall include— (E) the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records;" [Subsection (e)(4)(E)]

3. Changes in Policy or Data Use

Notice must be provided if and when any changes are made to the applicable privacy policies or in the event that the information collected is used for any reason other than the originally stated purpose.

OECD	"before, and in any case not later than at the time data collection it

	should be possible to identify the purposes for which these data are to be used, and that later changes of purposes should likewise be specified." (Paragraph 54)
SH	"This notice must be provided… in any event before the organization uses such information for a purpose other than that for which it was originally collected"
HIPAA	"The covered entity must promptly revise and distribute its notice whenever there is a material change to the uses or disclosures, the individual's rights, the covered entity's legal duties, or other privacy practices stated in the notice. Except when required by law, a material change to any term of the notice may not be implemented prior to the effective date of the notice in which such material change is reflected." [§ 164.520(b)(3)]
JPIPA	"When an entity handling personal information has changed the Purpose of Use, the entity must notify the person of the changed Purpose of Use or publicly announce it." (Article 18, Paragraph 3)
US	"Each agency that maintains a system of records shall— (11) at least 30 days prior to publication of information… publish in the Federal Register notice of any new use or intended use of the information in the system, and provide an opportunity for interested persons to submit written data, views, or arguments to the agency;" [Subsection (e)(11)]
CSA	"When personal information that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified prior to use." (Clause 4.2.4)
CAL	(g) "For purposes of this section, "notice" may be provided by one of the following methods: (1) Written notice. (2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code. (3) Substitute notice, if the agency demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the agency does not have sufficient contact information. Substitute notice shall consist of all of the following: (A) E-mail notice when the agency has an e-mail address for the subject persons. (B) Conspicuous posting of the notice on the agency's Web site page, if the agency maintains one. Notification to major statewide media"

4. <u>Language</u>

Notice must be provided in clear and conspicuous language.

SH	"This notice must be provided in clear and conspicuous language…"
HIPAA	"The covered entity must provide a notice that is written in plain language…" [§ 164.520(b)(1)]

5. Timing of Notification

There are two dominant positions on WHEN the Data Subject should be notified. The EU, HIPAA and UN do not state when notification should be sent. The APEC and Safe Harbor state that notification may be sent at the time of collection, before the time of collection *or reasonably thereafter*. However, the OECD, CSA and JPIPA state that Notification must be provided *by the time of collection* and no later. CAL requires specific notification practices following a security breach.

APEC	"All reasonably practicable steps shall be taken to ensure that such notice is provided either before or at the time of collection of personal information. Otherwise, such notice should be provided **as soon after as is practicable.**" (Paragraph 16)
OECD	"The purposes for which personal data are collected should be specified **not later than at the time of data collection**" (Paragraph 9)
SH	"This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or **as soon thereafter as is practicable**"
FTC	"Consumers should be given notice of an entity's information practices **before** any personal information is collected from them." (section 1)
JPIPA	"…when an entity handling personal information acquires such personal information on a person as is written in an agreement or other document (including a record made by an electronic method, a magnetic method, or any other method not recognizable to human senses. Hereinafter this applies in this paragraph.) as a result of concluding an agreement with the person or acquires such personal information on a person as is written in a document directly from the person, the entity must expressly show the Purpose of Use **in advance**." (Article 18, Paragraph 2)
CSA	"The identified purposes should be specified **at or before the time of collection** to the individual from whom the personal information is collected." (Clause 4.2.3)
CAL	"The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data The notification required in this section may be delayed if a Law enforcement agency determines that notification will impede a criminal investigation"

General Study Observations:

- Notice is one of the Privacy requirements that is referenced in all instruments, whether explicitly stated or implied
- Notice incorporates at least five major components
- There are exceptional notice conditions and qualifiers, and these require notice management capabilities long after the initial collection
- Notice (based on ISTPA analysis) can be understood as having a unique set of characteristics outside of specific content of the notification. Notice is a vehicle that can have many types of content. This content can be notification on terms of collection and

use, notification of breaches, notification of change in privacy policies. Notice is analogous to communications, that is, a vessel or process that can be filled with various content messages

- Legal sufficiency of notice is not the same as use of plain language in providing notification
- Timing of notification (that is: before, during or after data transaction) has not coalesced to an accepted norm across legislative instruments
- Notice, whether for initial collection and use, or change in use, reflects the need for maintaining a relationship between an organization and the individual at different points in the Personal Information lifecycle process
- An optional path confirming that the notice has been received by the data subject (and responded to) should be considered
- Change in an organization's Privacy policy should cause a notice action; mechanisms for new notice are triggered and executed
- A change in policy, by a subsequent holder of data, impacts the notice requirement for the organization that has the initial relationship with the data subject
- Notice and response should "travel" (i.e., be linkable in some manner) with the data throughout its lifecycle
- Usability (readability, navigation) of notices and unambiguous and granular tracking are needed
- Notice is an action that has both time and content components

Composite Operational Definition:

Notice: Information regarding an entity's privacy policies and practices including: definition of the personal information collected; its use (purpose specification); its disclosure to parties within or external to the entity; practices associated with the maintenance and protection of the information; options available to the data subject regarding the collector's privacy practices; changes made to policies or practices; and information provided to data subject at designated times and under designated circumstances.

6.3. Consent

Privacy Instruments examined for relationship to Consent:

- **APEC Privacy Framework** under "Choice" (Section V)
- **OECD Guidelines** under "Collection Limitation" (Paragraph 7, 52)
- **EU Data Protection Directive** under "Criteria for Making Data Processing Legitimate" (Section II)
- **Safe Harbor Principles** under "Choice"
- **Health Insurance Portability and Accountability Act (HIPAA)** under "Uses and disclosures requiring an opportunity for the individual to agree or to object" (§ 164.510)
- **US FTC Fair Information Practices** under "Choice/Consent" (Section 2)
- **Japan Personal Information Protection Act** under "Prior consent" (Section 16)
- **Australian National Privacy Principles** under "Collection" (Sub clause 1.3)
- **The Privacy Act of 1974 (US)** under "Conditions of disclosure" (Subsection b)
- **CSA Model Code** under "Consent" (Clause 4.3-4.3.8)

Consent Source References:

1. **Sensitive Information**
   While there is general agreement on the principle, there are potentially major differences. For example, the EU limits the collection and use of sensitive information by force of law, while others use potentially ambiguous language.

   Data Subjects must be informed of, and explicitly consent to, the collection, use and disclosure of sensitive information (i.e. medical or health conditions, racial or ethnic origins, political views, religious or philosophical beliefs, trade union membership or information regarding sex life) unless a law or regulation specifically requires otherwise.

EU	"1) Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life. 2) Paragraph 1 shall not apply where: (a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent; or (b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or (c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or

	legally incapable of giving his consent; or (d) processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or (e) the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defense of legal claims." (Article 8)
SH	"For sensitive information (i.e. personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual), they must be given affirmative or explicit (opt in) choice if the information is to be disclosed to a third party or used for a purpose other than those for which it was originally collected or subsequently authorized by the individual through the exercise of opt in choice."
HIPAA	"A covered entity may use or disclose protected health information without the written consent or authorization of the individual… provided that the individual is informed in advance of the use or disclosure and has the opportunity to agree to or prohibit or restrict the disclosure in accordance with the applicable requirements of this section. The covered entity may orally inform the individual of and obtain the individual's oral agreement or objection to a use or disclosure permitted by this section." (§ 164.510)
JPIPA	"An entity handling personal information must not handle personal information about a person, without obtaining the prior consent of the person, beyond the scope necessary for the achievement of the Purpose of Use specified under the preceding article." (Article 16, Paragraph 1)
ANPP	"An organization must not collect sensitive information about an individual unless: (a) the individual has consented; or (b) the collection is required by law; or (c) the collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual, where the individual whom the information concerns: (i) is physically or legally incapable of giving consent to the collection; or (ii) physically cannot communicate consent to the collection; or (d) if the information is collected in the course of the activities of a non-profit organization, the following conditions are satisfied:

	(i) the information relates solely to the members of the organization or to individuals who have regular contact with it in connection with its activities; (ii) at or before the time of collecting the information, the organization undertakes to the individual whom the information concerns that the organization will not disclose the information without the individual's consent; or (e) the collection is necessary for the establishment, exercise or defense of a legal or equitable claim. 10.2 Despite sub clause 10.1, an organization may collect health information about an individual if: (a) the information is necessary to provide a health service to the individual; and (b) the information is collected: (i) as required by law (other than this Act); or (ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organization. 10.3 Despite sub clause 10.1, an organization may collect health information about an individual if: (a) the collection is necessary for any of the following purposes: (i) research relevant to public health or public safety; (ii) the compilation or analysis of statistics relevant to public health or public safety; (iii) the management, funding or monitoring of a health service; and (b) that purpose cannot be served by the collection of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained; and (c) it is impracticable for the organization to seek the individual's consent to the collection; and (d) the information is collected: (i) as required by law (other than this Act); or (ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional

	confidentiality which bind the organization; or (iii) in accordance with guidelines approved by the Commissioner under section 95A for the purposes of this subparagraph. 10.4 If an organization collects health information about an individual in accordance with sub clause 10.3, the organization must take reasonable steps to permanently de-identify the information before the organization discloses it." (Sub clause 10)
US	(b) Conditions of disclosure "No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains" (Subsection b)
CSA	"The way in which an organization seeks consent may vary, depending on the circumstances and the type of information collected. An organization should generally seek express consent when the information is likely to be considered sensitive." (4.3.6)

2. Informed Consent

The Data Subject must provide *informed* consent to the collection of personal information unless a law or regulation specifically requires otherwise.

APEC	"Where appropriate, individuals should be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information." (Paragraph 20)
OECD	"There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject." (Paragraph 7)
EU	"Member States shall provide that personal data may be processed only if: (a) the data subject has unambiguously given his consent; or (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or (c) processing is necessary for compliance with a legal obligation to which the controller is subject; or (d) processing is necessary in order to protect the vital interests of the data subject;" (Article 10)
SH	"Individuals must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice."
HIPAA	"A covered health care provider must inform an individual of the protected health information that it may include in a directory and the persons to whom it may disclose such information (including disclosures to clergy of information regarding religious affiliation) and provide the individual with the opportunity to restrict or prohibit some or all of the uses or disclosures permitted…" [§ 164.510(a)(2)]

FTC	"…choice means giving consumers options as to how any personal information collected from them may be used. Specifically, choice relates to secondary uses of information -- *i.e*., uses beyond those necessary to complete the contemplated transaction." (Section 2)
CSA	"Consent is required for the collection of personal information and the subsequent use or disclosure of this information." (Clause 4.3.1)

3. Change of Use Consent
Consent must be acquired from the Data Subject to use personal information for purposes other than those originally stated at time of collection.

OECD	"Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 *[In other words, those stated in original notice. Note: see notice comparison for paragraph 9]* except: a) with the consent of the data subject; or b) by the authority of law." (Paragraph 10)
SH	"An organization must offer individuals the opportunity to choose (opt out) whether their personal information is: (b) to be used for a purpose that is incompatible with the purpose(s) for which it was originally collected or subsequently authorized by the individual."
CSA	"In certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before use (for example, when an organization wants to use information for a purpose not previously identified)." (Clause 4.3.1)

4. Consequences of Consent Denial
Data Subjects must be made aware of the consequences of denying consent.

EU	"Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it: c) any further information such as • whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply" (Article 10)
ANPP	"At or before the time (or, if that is not practicable, as soon as practicable after) an organization collects personal information about an individual from the individual, the organization must take reasonable steps to ensure that the individual is aware of: (f) the main consequences (if any) for the individual if all or part of the information is not provided." (Sub clause 1.3)
CSA	"An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The organization should inform the individual of the implications of such withdrawal." (Clause 4.3.8)

General Study Observations:

- Notice is given and consent is requested, but the notion of consent does not always extend to the consequences of use
- Individual Participation falls within Consent
- Choice is part of consent, as expressed in HIPAA, FTC, and APEC
- Sensitivity levels of information are covered under consent; one needs to make sure that sensitivity classification of data is facilitated
- There is a lack of explicit consent in some legislation; and, consent appears in many forms
- Consent is one of the Privacy requirements that is referenced in all studied instruments
- Non-repudiation of the fact of consent should be considered: this requires an underlying security functionality
- Types of identity (e.g., anonymous, pseudonymous): supporting gradations of non-identifiable, identifiable or identified sensitive data collection and processing needs to be supported by consent

Composite Operational Definition:

Consent: The capability, including support for Sensitive Information, Informed Consent, Change of Use Consent, and Consequences of Consent Denial, provided to data subjects to allow the collection and/or specific uses of some or all of their personal data either through an affirmative process (opt-in) or implied (not choosing to opt-out when this option is provided).

6.4. Collection Limitation

Privacy Instruments examined for relationship to Collection Limitation:

- **APEC Privacy Framework** under "Collection Limitation" (Section III)
- **OECD Privacy Guidelines** under "Collection Limitation" (Paragraph 7)
- **EU Data Protection Directive** under "Principles Relating to Data Quality" (Section I)
- **UN Guidelines Concerning Computerized Personal Data Files** under "lawfulness and fairness" (Paragraph 1)
- **Japan Personal Information Protection Act** under "Restriction by the Purpose of Use" and "Proper Acquisition" (Sections 16-17)
- **Australian National Privacy Principles** under "Collection" (Sub clause 1.0-1.5)
- **The Privacy Act of 1974 (US)** under "Agency Requirements" (Subsection e)
- **CSA Model Code** under "Limiting Collection" (Clause 4.4-4.4.3)

Collection Limitation Source References:

1. **Limitation of Collection**
   Only personal information relevant to the identified purpose may be collected.

APEC	"The collection of personal information should be limited to information that is relevant to the purposes of collection and any such information should be obtained by lawful and fair means, and where appropriate, with notice to, or consent of, the individual concerned." (Paragraph 18)
OECD	"There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject." (Paragraph 7)
EU	"Member States shall provide that personal data must be: (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;" (Article 6)
UN	"Information about persons should not be collected or processed in unfair or unlawful ways, nor should it be used for ends contrary to the purposes and principles of the Charter of the United Nations." (Paragraph 1)
JPIPA	"An entity handling personal information must not handle personal information about a person, without obtaining the prior consent of the person, beyond the scope necessary for the achievement of the Purpose of Use specified under the preceding article." (Article 16, Paragraph 1)
ANPP	"An organization must not collect personal information unless the information is necessary for one or more of its functions or activities." (Sub clause 1.1)
US	"Each agency that maintains a system of records shall-- (1) maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by Executive order of the President;" [Subsection (e)(1)]
CSA	"Organizations shall not collect personal information indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfill the purposes identified." (Clause

	4.4.1)

2. <u>Fair and Lawful Means</u>
Information must be collected by fair and lawful means.

APEC	"The collection of personal information should be limited to information that is relevant to the purposes of collection and any such information should be obtained by lawful and fair means, and where appropriate, with notice to, or consent of, the individual concerned." (Paragraph 18)
OECD	"There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject." (Paragraph 7)
EU	"Member States shall provide that personal data must be: (a) processed fairly and lawfully;" (Article 6)
UN	"Information about persons should not be collected or processed in unfair or unlawful ways…" (Paragraph 1)
JPIPA	"An entity handling personal information must not acquire personal information by a fraudulent or other dishonest means." (Article 17)
ANPP	"An organization must collect personal information only by lawful and fair means and not in an unreasonably intrusive way." (Sub clause 1.2)
CSA	"Information shall be collected by fair and lawful means." (Clause 4.4)

General Study Observations:

- Stated purpose of collection should be linked to the data source identification; means of "fair and lawful" collection should be associated with the source
- Legal or business adherence to collection limitation needs to be auditable
- Collection limitation might have a time expiration associated with it
- Levels or types of identity such as gradations of non-identifiable, identifiable or identified data collection and processing need to be supported
- Collection limitation and what may be lawful or fair may be directly dependent upon levels or types of data subject identity
- "Collection relevant to purpose" is not precisely defined

Composite Operational Definition:

Collection Limitation: Constraints exercised by the data collector and user to limit the information collected to the minimum necessary to achieve a stated purpose and when required demonstrably collected by fair and lawful means.

6.5. Use Limitation

Privacy Instruments examined for relationship to Use Limitation:

- **APEC Privacy Framework** under "Uses of Personal Information" (Section IV)
- **OECD Privacy Guidelines** under "Use Limitation" (Paragraph 10)
- **EU Data Protection Directive** under "Principles Relating to Data Quality" (Section I)
- **Safe Harbor Principles** under "Data Integrity"
- **Health Insurance Portability and Accountability Act (HIPAA)** under "Uses and Disclosures of Protected Health Information: General Rules" (§ 164.502)
- **UN Guidelines Concerning Computerized Personal Data Files** under "Purpose-Specification" (Paragraph 3)
- **Japan Personal Information Protection Act** under "Restriction by the Purpose of Use" (Article 16)
- **Australian National Privacy Principles** under "Use and Disclosure" (Sub clause 2.1-2.6)
- **The Privacy Act of 1974 (US)** under "Agency Requirements" [Subsection e(11)]
- **CSA Model Code** under "Limiting Use, Disclosure and Retention" (Clause 4.5-4.5.4)

Use Limitation Source References:

1. **Acceptable Uses**
   Personal Data may only be used for the purposes stated at the time of collection.

APEC	"Personal information collected should be used only to fulfill the purposes of collection and other compatible or related purposes" (Paragraph 19)
OECD	"Personal data should not be disclosed, made available or otherwise used for purposes other than those specified" (Paragraph 10)
EU	"Member States shall provide that personal data must be: (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes." (Article 6)
SH	"Consistent with the Principles, personal information must be relevant for the purposes for which it is to be used. An organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual."
HIPAA	"When using or disclosing protected health information or when requesting protected health information from another covered entity, a covered entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request." [§ 164.502(b)(1)]
UN	"The purpose which a file is to serve and its utilization in terms of that purpose should be specified, legitimate and, when it is established, receive a certain amount of publicity or be brought to the attention of the person concerned, in order to make it possible subsequently to ensure that: • None of the said personal data is used or disclosed, except with the consent of the person concerned, for purposes

	incompatible with those specified;" (Paragraph 3)
JPIPA	"An entity handling personal information must not handle personal information about a person, without obtaining the prior consent of the person, beyond the scope necessary for the achievement of the Purpose of Use specified under the preceding article." (Article 16, Paragraph 1)
ANPP	"An organization must not use or disclose personal information about an individual for a purpose (the ***secondary purpose***) other than the primary purpose of collection unless: (a) both of the following apply: (i) the secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection; (ii) the individual would reasonably expect the organization to use or disclose the information for the secondary purpose;" (Sub clause 2.1)
US	"Each agency that maintains a system of records shall at least 30 days prior to publication of information under paragraph (4)(D) of this subsection, publish in the Federal Register notice of any new use or intended use of the information in the system," [Subsection e (11)]
CSA	"Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law." (Clause 4.5)

2. <u>Data Retention</u>
Personal Data is retained no longer than necessary to complete the stated purpose.

EU	"Member States shall provide that personal data must be: (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed." (Article 6)
UN	"The purpose which a file is to serve and its utilization in terms of that purpose should be specified, legitimate and, when it is established, receive a certain amount of publicity or be brought to the attention of the person concerned, in order to make it possible subsequently to ensure that: • The period for which the personal data are kept does not exceed that which would enable the achievement of the purpose so specified." (Paragraph 3)
FTC*	"To assure data integrity, collectors must take reasonable steps, such as using only reputable sources of data and cross-referencing data against multiple sources, providing consumer access to data, and destroying untimely data or converting it to anonymous form." (Section 4)
ANPP*	"An organization must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed under National Privacy Principle 2." (Sub clause 4.2)

CSA	"Personal information that is no longer required to fulfill the identified purposes should be destroyed, erased, or made anonymous. Organizations should develop guidelines and implement procedures to govern the destruction of personal information." (Clause 4.5.3)

*While the **Australian National Privacy Principles** and **US FTC Fair Information Practices** do not refer to Data Retention under Use, they both mention the destruction or de-identification of data after it has fulfilled its stated purpose in their Security sections.

General Study Observations:

- Stated purpose of use should be linked to the data source identification
- Means of "fair and lawful" use should be documented with the source
- Use limitation is a requirement that is dictated by nearly all legislative instruments
- In some instances, implementing regulations address data retention
- Legal or business adherence to use limitation may need to be auditable
- Use limitation might have a time expiration connected to it
- Future use should be tied to the original collection purpose
- Selected "secondary" use is allowed under law: this needs clear definition
- Retention limits and resulting destruction need to be audited

Composite Operational Definition:

Use Limitation: Controls exercised by the data collector or data user to ensure that personal information will not be used for purposes other than those specified and accepted by the data subject or provided by law, and not maintained longer than necessary for the stated purposes**.**

6.6. Disclosure

Privacy Instruments examined for relationship to Disclosure:

- **APEC Privacy Framework** under "Accountability" (Section IX)
- **Safe Harbor Principles** under "Onward Transfer"
- **Health Insurance Portability and Accountability Act (HIPAA)** under "Notice of privacy practices for protected health information" (§ 164.520)
- **Japan Personal Information Protection Act** under "Restriction of Provision to Third Parties" (Article 23)
- **Australian National Privacy Principles** under "Use and Disclosure" (Sub clause 2.1-2.6)
- **The Privacy Act of 1974 (US)** under "Agency Requirements" (Subsection b)
- **CSA Model Code** under "Limiting Use, Disclosure and Retention" (Clause 4.5)

Disclosure Source References:

1. **Third-Party Disclosure**
   Notice and Consent of the Data Subject is required to disclose information to third parties.

APEC	"When personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles." (Paragraph 26)
SH	"To disclose information to a third party, organizations must apply the Notice and Choice Principles."
HIPAA	"A covered entity may use or disclose protected health information without the written consent or authorization of the individual… provided that the individual is informed in advance of the use or disclosure and has the opportunity to agree to or prohibit or restrict the disclosure in accordance with the applicable requirements of this section. The covered entity may orally inform the individual of and obtain the individual's oral agreement or objection to a use or disclosure permitted by this section. "
JPIPA	"An entity handling personal information must not, except in the following cases, provide personal data to a third party without obtaining the prior consent of the person:" (Article 23, Paragraph 1)
ANPP	"An organization must not use or disclose personal information about an individual for a purpose (the ***secondary purpose***) other than the primary purpose of collection unless: (b) the individual has consented to the use or disclosure;" (Sub clause 2.1)
US	"No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains," (Subsection b)
CSA	"Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of

	the individual or as required by law." (Clause 4.5)

2. Third-Party Policy Requirements
Organizations must ensure that any third parties are informed of their privacy policies and will follow them or possess equivalent policies.

APEC	"When personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles." (Paragraph 26)
SH	"Where an organization wishes to transfer information to a third party that is acting as an agent it may do so if it first either ascertains that the third party subscribes to the Principles or is subject to the Directive or another adequacy finding or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant Principles."

3. Disclosure for Legal or Health Reasons
Information may be disclosed if required by law or is required in issues of health and safety.

JPIPA	"An entity handling personal information must not, except in the following cases, provide personal data to a third party without obtaining the prior consent of the person: (1) Cases in which the provision of personal data is based on laws (2) Cases in which the provision of personal data is necessary for the protection of the life, body, or property of an individual and in which it is difficult to obtain the consent of the person (3) Cases in which the provision of personal data is specially necessary for improving public hygiene or promoting the sound growth of children and in which it is difficult to obtain the consent of the person (4) Cases in which the provision of personal data is necessary for cooperating with a state institution, a local public body, or an individual or entity entrusted by one in executing the operations prescribed by laws and in which obtaining the consent of the person might impede the execution of the operations concerned" (Article 23, Paragraph 1)
ANPP	"An organization must not use or disclose personal information about an individual for a purpose (the secondary purpose) other than the primary purpose of collection unless: (e) the organization reasonably believes that the use or disclosure is necessary to lessen or prevent: (i) a serious and imminent threat to an individual's life, health or safety; or (ii) a serious threat to public health or public safety; or

	(g) the use or disclosure is required or authorized by or under law;"(Sub clause 2.1)
CSA	"Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law." (Clause 4.5)

General Study Observations:

- Disclosure is regulated but not the method of disclosure
- Disclosures, occurring as a result of security breaches, are not addressed; a security breach use case should be defined
- There is a need to address improper disclosures
- Data transfer during disclosure needs security
- Validation of third-party recipients of Personal Information is needed
- Disclosure without subject consent has varied legal reasons

Composite Operational Definition:

Disclosure: The release, transfer, provision of access to, use for new purposes, or divulging in any other manner, of information by the entity holding the information only with notice and consent of the data subject; the data collectors policies must be made known to and observed by third parties receiving the information; and sensitive health information disclosures must be managed.

6.7. Access and Correction

Privacy Instruments examined for relationship to Access and Correction:

- **APEC Privacy Framework** under "Access and Correction " (Section VIII)
- **OECD Privacy Guidelines** under "Individual Participation" (Paragraph 13)
- **EU Data Protection Directive** under "The Data Subject's Right of Access to Data" (Section V)
- **Safe Harbor Principles** under "Access"
- **Health Insurance Portability and Accountability Act (HIPAA)** under "Access of Individuals to Protected Health Information" (§ 164.524) and "Amendment of Protected Health Information" (§ 164.526)
- **UN Guidelines Concerning Computerized Personal Data Files** under "Interested-Person Access" (Paragraph 4)
- **US FTC Fair Information Practices** under "Access/Participation" (Section 3)
- **Japan Personal Information Protection Act** under "Disclosure" (Article 25) and "Correction" (Article 26)
- **Australian National Privacy Principles** under "Access and Correction" (Subcl 6.1-6.7)
- **The Privacy Act of 1974 (US)** under "Access to Records" (Subsection d)
- **CSA Model Code** under "Individual Access" (Clause 4.9-4.9.6)

Access and Correction Source References:

1. **Access to Information**
   Data Subjects are able to determine if an organization maintains data on them and should be able to request access to said information.

APEC	"Individuals should be able to: a) obtain from the personal information controller confirmation of whether or not the personal information controller holds personal information about them;" (Paragraph 23)
OECD	"An individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;" (Paragraph 13)
EU	"Member States shall guarantee every data right to obtain from the controller: (a) without constraint at reasonable intervals and without excessive delay or expense: • confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed, • communication to him in an intelligible form of the data undergoing processing and of any available information as to their source," (Article 12)

SH	"Individuals must have access to personal information about them that an organization holds…"
HIPAA	"…an individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set," [§ 164.524(a)(1)]
UN	"Everyone who offers proof of identity has the right to know whether information concerning him is being processed and to obtain it in an intelligible form, without undue delay or expense, and to have appropriate rectifications or erasures made in the case of unlawful, unnecessary or inaccurate entries and, when it is being communicated, addressees." (Paragraph 4)
FTC	"Access is the third core principle. It refers to an individual's ability both to access data about him or herself -- *i.e.*, to view the data in an entity's files -- and to contest that data's accuracy and completeness." (Section 3)
JPIPA	"When an entity handling personal information is requested by a person to disclose such retained personal data as may lead to the identification of the person concerned (such disclosure includes notifying the person that the entity has no such retained personal data as may lead to the identification of the person concerned. This applies hereinafter.), the entity must disclose the retained personal data concerned without delay by a method prescribed by a Cabinet order. However, in any of the following cases, the entity may keep all or part of the retained personal data undisclosed: (1) Cases in which disclosure might harm the life, body, property, or other rights or interests of the person or a third party (2) Cases in which disclosure might seriously impede the proper execution of the business of the entity concerned handling personal information (3) Cases in which disclosure violates other laws" (Article 25, Paragraph 1)
ANPP	"If an organization holds personal information about an individual, it must provide the individual with access to the information on request by the individual…" (Sub clause 6.1)
US	"Each agency that maintains a system of records shall-- (1) upon request by any individual to gain access to his record or to any information pertaining to him which is contained in the system, permit him and upon his request, a person of his own choosing to accompany him, to review the record and have a copy made of all or any portion thereof in a form comprehensible to him, except that the agency may require the individual to furnish a written statement authorizing discussion of that individual's record in the accompanying person's presence;" [Subsection (d)(1)]
CSA	"Upon request, an organization shall inform an individual whether or not the organization holds personal information about the individual. Organizations are encouraged to indicate the source of this information. The organization shall allow the individual access to this information. However, the organization may choose to make sensitive medical information available through a medical practitioner. In addition, the organization should provide an account

	of the use that has been made or is being made of this information and an account of the third parties to which it has been disclosed." (Clause 4.9.1)

2. Proof of Identity
Data Subjects requesting information must supply sufficient proof of identity.

APEC	"Individuals should be able to: b) have communicated to them, after having provided sufficient proof of their identity, personal information about them;" (Paragraph 23)
UN	"Everyone who offers proof of identity has the right to know whether information concerning him is being processed and to obtain it in an intelligible form, without undue delay or expense, and to have appropriate rectifications or erasures made in the case of unlawful, unnecessary or inaccurate entries and, when it is being communicated, addressees." (Paragraph 4)
CSA	"An individual may be required to provide sufficient information to permit an organization to provide an account of the existence, use, and disclosure of personal information. The information provided shall only be used for this purpose." (Clause 4.9.2)

3. Provision of Data
Requested information is provided clearly, at reasonable cost and within a reasonable timeframe.

APEC	"Individuals should be able to: b) have communicated to them, after having provided sufficient proof of their identity, personal information about them; i. within a reasonable time; ii. at a charge, if any, that is not excessive; iii. in a reasonable manner; iv. in a form that is generally understandable;" (Paragraph 23)
OECD	"An individual should have the right: b) to have communicated to him, data relating to him • within a reasonable time; • at a charge, if any, that is not excessive; • in a reasonable manner; and • in a form that is readily intelligible to him;" (Paragraph 13)
EU	"Member States shall guarantee every data right to obtain from the controller: (a) without constraint at reasonable intervals and without excessive delay or expense: • confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,

	• communication to him in an intelligible form of the data undergoing processing and of any available information as to their source," (Article 12)
HIPAA	"The covered entity must provide the access as requested by the individual in a timely manner… including arranging with the individual for a convenient time and place to inspect or obtain a copy of the protected health information, or mailing the copy of the protected health information at the individual's request. The covered entity may discuss the scope, format, and other aspects of the request for access with the individual as necessary to facilitate the timely provision of access." [§ 164.524(c)(3)]
UN	"Everyone who offers proof of identity has the right to know whether information concerning him is being processed and to obtain it in an intelligible form, without undue delay or expense, and to have appropriate rectifications or erasures made in the case of unlawful, unnecessary or inaccurate entries and, when it is being communicated, addressees." (Paragraph 4)
FTC	"To be meaningful, access must encompass timely and inexpensive access to data…" (Section 3)
ANPP	"If an organization charges for providing access to personal information, those charges: (a) must not be excessive; and (b) must not apply to lodging a request for access" (Sub clause 6.4)
CSA	"An organization shall respond to an individual's request within a reasonable time and at minimal or no cost to the individual. The requested information shall be provided or made available in a form that is generally understandable. For example, if the organization uses abbreviations or codes to record information, an explanation shall be provided." (Clause 4.9.4)

4. <u>Denial of Access</u>
In the event Data Subjects are denied access, they are informed of the reason for their denial of access and options for challenging said denial.

APEC	"If a request under (a) or (b) or a challenge under (c) is denied, the individual should be provided with reasons why and be able to challenge such denial." (Paragraph 23)
OECD	"An individual should have the right: c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial;" (Paragraph 13)
HIPAA	"The covered entity must provide a timely, written denial to the individual… The denial must be in plain language and contain: (i) The basis for the denial; (ii) If applicable, a statement of the individual's review rights under paragraph (a)(4) of this section, including a description of how the individual may exercise such review rights; and

	(iii) A description of how the individual may complain to the covered entity… or to the Secretary… The description must include the name, or title, and telephone number of the contact person or office designated" [§ 164.524(d)(2)]
JPIPA	"When an entity handling personal information has decided not to disclose all or part of such retained personal data as is requested under the preceding paragraph, the entity must notify the person of that effect without delay." (Article 25, Paragraph 2)
ANPP	"An organization must provide reasons for denial of access or a refusal to correct personal information." (Sub clause 6.7)
US	"Each agency that maintains a system of records shall-- (3) permit the individual who disagrees with the refusal of the agency to amend his record to request a review of such refusal, and not later than 30 days (excluding Saturdays, Sundays, and legal public holidays) from the date on which the individual requests such review, complete such review and make a final determination unless, for good cause shown, the head of the agency extends such 30-day period; and if, after his review, the reviewing official also refuses to amend the record in accordance with the request, permit the individual to file with the agency a concise statement setting forth the reasons for his disagreement with the refusal of the agency, and notify the individual of the provisions for judicial review of the reviewing official's determination under subsection (g)(1)(A) of this section;" [Subsection (d)(3)]

5. Correcting Information
Data Subjects are able to update or correct personal information held by the organization.

APEC	"Individuals should be able to: c) challenge the accuracy of information relating to them and, if possible and as appropriate, have the information rectified, completed, amended or deleted." (Paragraph 23)
OECD	"An individual should have the right: d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended." (Paragraph 13)
EU	"Member States shall guarantee every data right to obtain from the controller: (b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;" (Article 12)
SH	"Individuals must have access to personal information about them that an organization holds and be able to correct, amend**,** or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated."
HIPAA	"An individual has the right to have a covered entity amend protected health information or a record about the individual in a designated record set for as long as the protected health information is

	maintained in the designated record set." [§ 164.526(a)(1)]
UN	"Everyone who offers proof of identity has the right to know whether information concerning him is being processed and to obtain it in an intelligible form, without undue delay or expense, and to have appropriate rectifications or erasures made in the case of unlawful, unnecessary or inaccurate entries and, when it is being communicated, addressees." (Paragraph 4)
FTC	"To be meaningful, access must encompass… a simple means for contesting inaccurate or incomplete data, a mechanism by which the data collector can verify the information, and the means by which corrections and/or consumer objections can be added to the data file and sent to all data recipients." (Section 3)
JPIPA	"When an entity handling personal information is requested by a person to correct, add, or delete such retained personal data as may lead to the identification of the person concerned on the ground that the retained personal data is contrary to the fact, the entity must, except in cases in which special procedures are prescribed by any other laws for such correction, addition, or deletion, make a necessary investigation without delay within the scope necessary for the achievement of the Purpose of Use and, on the basis of the results, correct, add, or delete the retained personal data concerned." (Article 26, Paragraph 1)
ANPP	"If an organization holds personal information about an individual and the individual is able to establish that the information is not accurate, complete and up-to-date, the organization must take reasonable steps to correct the information so that it is accurate, complete and up-to-date." (Sub clause 6.5)
US	"Each agency that maintains a system of records shall-- (2) permit the individual to request amendment of a record pertaining to him and-- (B) promptly, either-- (i) make any correction of any portion thereof which the individual believes is not accurate, relevant, timely, or complete; or (ii) inform the individual of its refusal to amend the record in accordance with his request, the reason for the refusal, the procedures established by the agency for the individual to request a review of that refusal by the head of the agency or an officer designated by the head of the agency, and the name and business address of that official;" [Subsection (d)(2)(B)]
CSA	"An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate." (Clause 4.9)

General Study Observations:

- There are wide variations in ability to deny access and to deny requestor recourse
- "Cost and timeframe" of access and correction are important but not specified,(only described as "reasonable")
- The PI subject needs to know who has PI about them; tracking is needed

- Proper identity credentials of the PI subject are needed
- Denial of access has varied legal bases and specifics

Composite Operational Definition:

Access and Correction: Capability allowing individuals having adequate proof of identity to find out from an entity, or find out and/or to correct, their personal information, at reasonable cost, within reasonable time constraints, and with notice of denial of access and options for challenging denial.

6.8. Security/Safeguards

Privacy Instruments examined for relationship to Security/Safeguards:

- **APEC Privacy Framework** under "Security Safeguards" (Section VII)
- **OECD Privacy Guidelines** under "Security Safeguards" (Paragraph 11)
- **EU Data Protection Directive** under "Confidentiality and Security of Processing" (Section VIII)
- **Safe Harbor Principles** under "Security"
- **Health Insurance Portability and Accountability Act (HIPAA)** under "Administrative Requirements" (§ 164.530)
- **UN Guidelines Concerning Computerized Personal Data Files** under "Security" (Paragraph 7)
- **US FTC Fair Information Practices** under "Integrity/Security" (Section 4)
- **Japan Personal Information Protection Act** under "Security Control Measures" (Article 20)
- **Australian National Privacy Principles** under "Data Security" (Sub clause 4.1-4.2)
- **The Privacy Act of 1974 (US)** under "Agency Requirements" (Subsection e)
- **CSA Model Code** under "Safeguards" (Clause 4.7-4.7.5)

Security/Safeguards Source References:

1. **<u>Safeguards</u>**
   Organizations must be sure to include safeguards to prevent loss, misuse, unauthorized access, disclosure, alteration and destruction of data.

APEC	"Personal information controllers should protect personal information that they hold with appropriate safeguards against risks, such as loss or unauthorized access to personal information, or unauthorized destruction, use, modification or disclosure of information or other misuses." (Paragraph 22)
OECD	"Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data." (Paragraph 11)
EU	"Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing." (Article 17, Paragraph 1)
SH	"Organizations creating, maintaining, using or disseminating personal information must take reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction."
HIPAA	"A covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart." [§ 164.530 (c)(2)]
UN	"Appropriate measures should be taken to protect the files against both natural dangers, such as accidental loss or destruction and

	human dangers, such as unauthorized access, fraudulent misuse of data or contamination by computer viruses." (Paragraph 7)
FTC	"Security involves both managerial and technical measures to protect against loss and the unauthorized access, destruction, use, or disclosure of the data. Managerial measures include internal organizational measures that limit access to data and ensure that those individuals with access do not utilize the data for unauthorized purposes. Technical security measures to prevent unauthorized access include encryption in the transmission and storage of data; limits on access through use of passwords; and the storage of data on secure servers or computers that are inaccessible by modem." (Section 4)
JPIPA	"An entity handling personal information must take necessary and proper measures for the prevention of leakage, loss, or damage, and for other control of security of the personal data." (Article 20)
ANPP	"An organization must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorized access, modification or disclosure." (Sub clause 4.1)
US	"Each agency that maintains a system of records shall— (11) establish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained;" {Subsection (e)(11)]
CSA	"The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held." (Clause 4.7.1)

2. <u>Destruction of Data</u>
Organizations must take steps to destroy or permanently de-identify discarded data.

FTC	"To assure data integrity, collectors must take reasonable steps, such as using only reputable sources of data and cross-referencing data against multiple sources, providing consumer access to data, and destroying untimely data or converting it to anonymous form." (Section 4)
ANPP	"An organization must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed under National Privacy Principle 2."(Sub clause 4.2)
CSA	"Care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information." (Clause 4.7.5)

General Study Observations:

- No real definition of reasonable or proper safeguards is provided
- Means of destruction of outdated PI is also not defined
- Privacy management capability maturity should be formalized and include security considerations

- There is a growing expectation of notice to data subjects when an event such as a security data breach has been experienced. However, actions associated with data breach, such as required in California SB 1386, fall into categories other than security.

  Reference: Setting of identity theft "red flags" by U.S. financial institutions – http://www.federalreserve.gov/BOARDDOCS/PRESS/bcreg/2006/20060718/default.htm

- "Hooks" in privacy management for safeguards need to be pervasive; i.e., provide a means to detect suspicious activity, actual breaches and security failures while providing data subjects secure, reliable and accurate notifications

  Composite Operational Definition:

  Security/Safeguards: Policies, practices and controls that ensure the confidentiality, availability and integrity of personal information collected, used, maintained, and destroyed; and ensure that personal information will be destroyed or de-identified as required.

6.9. Data Quality

Privacy Instruments examined for relationship to Data Quality:

- **APEC Privacy Framework** under "Integrity of Personal Information" (Section VI)
- **OECD Privacy Guidelines** under "Data Quality" (Paragraph 8)
- **EU Data Protection Directive** under "Principles Relating to Data Quality" (Section I)
- **Safe Harbor Principles** under "Data Integrity"
- **UN Guidelines Concerning Computerized Personal Data Files** under "Accuracy" (Paragraph 2)
- **US FTC Fair Information Practices** under "Integrity/Security" (Section 4)
- **Japan Personal Information Protection Act** under "Maintenance of the Accuracy of Data" (Article 19)
- **Australian National Privacy Principles** under "Data Quality" (Sub clause 3)
- **The Privacy Act of 1974 (US)** under "Agency Requirements" (Subsection e)
- **CSA Model Code** under "Accuracy" (Clause 4.6-4.6.3)

Data Quality Source References:

1. **Data Accuracy**
   Organizations will ensure that all personal information is accurate, complete and kept up-to-date.

APEC	"Personal information should be accurate, complete and kept up-to-date to the extent necessary for the purposes of use." (Paragraph 21)
OECD	"Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date." (Paragraph 8)
EU	"Member States shall provide that personal data must be: (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;" (Article 6)
SH	"To the extent necessary for those purposes, an organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current."
UN	"Persons responsible for the compilation of files or those responsible for keeping them have an obligation to conduct regular checks on the accuracy and relevance of the data recorded and to ensure that they are kept as complete as possible in order to avoid errors of omission and that they are kept up to date regularly or when the information contained in a file is used, as long as they are being processed." (Paragraph 2)
FTC	"The fourth widely accepted principle is that data be accurate and secure. To assure data integrity, collectors must take reasonable steps, such as using only reputable sources of data and cross-referencing data against multiple sources, providing consumer access to data, and destroying untimely data or converting it to anonymous form." (Section 4)
JPIPA	"An entity handling personal information must endeavor to maintain personal data accurate and up to date within the scope necessary for

	the achievement of the Purpose of Use." (Article 19)
ANPP	"An organization must take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up-to-date." (Sub clause 3)
US	"Each agency that maintains a system of records shall— (5) maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination;" [Subsection (e)(5)]
CSA	"Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used." (Clause 4.6)

General Study Observations:

- There are no best practices in these instruments; just "reasonable steps"
- What is "relevant" or "necessary" is not well-defined
- "Update" mechanisms need to be defined
- Privacy taxonomy is needed to define PI types and purposes unambiguously
- Data "quality" depends on the proper validation of Personally Identifiable data
- There is no definition of data "accuracy"

Composite Operational Definition:

Data Quality: Ensures that information collected and used is adequate for purpose, relevant for purpose, not excessive in relation to the purposes for which it is collected and/or further processed, accurate at time of use, and, where necessary, kept up to date, rectified or destroyed.

6.10. Enforcement

Privacy Instruments examined for relationship to Enforcement:

- **APEC Privacy Framework** under "Preventing Harm" (Section I)
- **EU Data Protection Directive** under "Supervisory Authority" (Chapter VI)
- **Safe Harbor Principles** under "Enforcement"
- **Health Insurance Portability and Accountability Act (HIPAA)** under "Responsibilities of Covered Entities" (§ 160.310) and "Complaints to the Secretary" (§ 160.306)
- **UN Guidelines Concerning Computerized Personal Data Files** under "Supervision and Sanctions" (Paragraph 8)
- **US FTC Fair Information Practices** under "Enforcement/Redress" (Section 5)
- **Japan Personal Information Protection Act** under "Handling of Complaints by Entities Handling Personal Information" (Article 31) and "Measures to Ensure Proper Handling of Personal Information" (Article 10)
- **CSA Model Code** under "Challenging Compliance" (Clause 4.10-4.10.4)
- **California SB 1386** Section 3

Enforcement Source References:

1. **Ensuring Compliance**
   There must be a process in place to ensure an organization adheres to its set of privacy policies.

APEC	"…remedies for privacy infringements should be designed to prevent harms resulting from the wrongful collection or misuse of personal information, and should be proportionate to the likelihood and severity of any harm threatened by the collection or use of personal information." (Paragraph 1)
EU	"Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive." (Article 28, Paragraph 1)
SH	"Effective privacy protection must include mechanisms for assuring compliance with the Principles, recourse for individuals to whom the data relate affected by non-compliance with the Principles, and consequences for the organization when the Principles are not followed."
HIPAA	"A covered entity must keep such records and submit such compliance reports, in such time and manner and containing such information, as the Secretary may determine to be necessary to enable the Secretary to ascertain whether the covered entity has complied or is complying with the applicable requirements…" [§ 160.310 (a)]
UN	"The law of every country shall designate the authority which, in accordance with its domestic legal system, is to be responsible for supervising observance of the principles set forth above. This authority shall offer guarantees of impartiality, independence persons or agencies responsible for processing and establishing data, and technical competence. In the event of violation of the provisions of the national law implementing the aforementioned principles, criminal or other penalties should be envisaged together with the appropriate individual remedies." (Paragraph 8)

FTC	"To be effective, self-regulatory regimes should include both mechanisms to ensure compliance (enforcement) and appropriate means of recourse by injured parties (redress). Mechanisms to ensure compliance include making acceptance of and compliance with a code of fair information practices a condition of membership in an industry association; external audits to verify compliance; and certification of entities that have adopted and comply with the code at issue." (Section 5a)
JPIPA	"Through the appropriate division of roles between the State and local public bodies, the State shall take necessary measures to ensure the proper handling of personal information by entities handling personal information defined in the next chapter." (Article 10)
CAL	" Section 3. 1798.84. (a) Any customer injured by a violation of this title may institute a civil action to recover damages. (b) Any business that violates, proposes to violate, or has violated this title may be enjoined. (c) The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under law."

2. <u>Handling Complaints</u>
There must be a process in place for data subjects to file complaints and have said complaints reviewed.

EU	"Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim." (Article 28, Paragraph 4)
SH	"At a minimum, such mechanisms must include (a) readily available and affordable independent recourse mechanisms by which each individual's complaints and disputes are investigated and resolved by reference to the Principles and damages awarded where the applicable law or private sector initiatives so provide; (b) follow up procedures for verifying that the attestations and assertions businesses make about their privacy practices are true and that privacy practices have been implemented as presented; and (c) obligations to remedy problems arising out of failure to comply with the Principles by organizations announcing their adherence to them and consequences for such organizations."
HIPAA	"A person who believes a covered entity is not complying with the applicable requirements of this part 160 or the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter may file a complaint with the Secretary." [§ 160.306 (a)]
FTC	"Appropriate means of individual redress include, at a minimum, institutional mechanisms to ensure that consumers have a simple and effective way to have their concerns addressed. Thus, a self-regulatory system should provide a means to investigate complaints from individual consumers and ensure that consumers are aware of how to access such a system." (Section 5a)
JPIPA	"1. An entity handling personal information must endeavor to

	appropriately and promptly handle complaints about the handling of personal information. 2. An entity handling personal information must endeavor to establish a system necessary for achieving the objective mentioned in the preceding paragraph." (Article 31)
CSA	"Organizations shall put procedures in place to receive and respond to complaints or inquiries about their policies and practices relating to the handling of personal information. The complaint process should be easily accessible and simple to use." (Clause 4.10.2)

General Study Observations:

- There are implicit and explicit suggestions of an enforcement "authority"
- Enforcement includes recourse actions and "right of action"
- "Complaint" mechanisms are needed for enforcement
- Need a workflow capability to track complaints and monitor enforcement status
- Regulatory agencies should be able to inspect complaints and monitor or interact with complaint workflow
- Capturing a data subject complaint is often a key requirement
- Enforcement should be tied into audit
- Enforcement is tied to Privacy policy, but no uniform policies are described

Composite Operational Definition:

Enforcement: Mechanisms to ensure compliance with privacy policies, agreements and legal requirements and to give data subjects a means of filing complaints of compliance violations and having them addressed, including recourse for violations of law, agreements and policies.

6.11. Openness

Privacy Instruments examined for relationship to Openness:

- **APEC Privacy Framework** under "Educating and publicizing domestic privacy protections" (Part IV, Section III)
- **OECD Privacy Guidelines** under "Openness" (Paragraph 12)
- **EU Data Protection Directive** under "Notification" (Section IX)
- **Japan Personal Information Protection Act** under "Public Announcement of Matters Concerning Retained Personal Data" (Article 24)
- **Australian National Privacy Principles** under "Openness" (Sub clause 5.1-5.2)
- **The Privacy Act of 1974 (US)** under "Agency Rules" (Subsection f)
- **CSA Model Code** under "Openness" (Clause 4.8-4.8.3)

Openness Source References:

1. **Public Policies**
   An Organization must ensure that its privacy policies are clearly published and publicly available.

APEC	"For the Framework to be of practical effect, it must be known and accessible. Accordingly, Member Economies should: a) publicize the privacy protections it provides to individuals;" (Paragraph 36)
OECD	"There should be a general policy of openness about developments, practices and policies with respect to personal data." (Paragraph 12)
EU	"Member States shall take measures to ensure that processing operations are publicized." (Article 21, Paragraph 1)
JPIPA	"With respect to the retained personal data, an entity handling personal information must put the matters enumerated in the following items in an accessible condition for the person (such condition includes cases in which a reply is made without delay at the request of the person): (1) The name of the entity concerned handling personal information (2) The Purpose of Use of all retained personal data" (Article 24, Paragraph 1)
ANPP	"An organization must set out in a document clearly expressed policies on its management of personal information. The organization must make the document available to anyone who asks for it." (Sub clause 5.1)
CSA	"Organizations shall be open about their policies and practices with respect to the management of personal information. Individuals should be able to acquire information about an organization's policies and practices without unreasonable effort. This information shall be made available in a form that is generally understandable." (Clause 4.8.1)

2. Establishing Existence of Personal Data

Means should be available for establishing the existence, nature and purpose of use of personal data.

OECD	"Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller." (Paragraph 12)
EU	"Member States shall provide, in relation to processing operations not subject to notification, that controllers or another body appointed by the Member States make available at least the information referred to in Article 19 (1) (a) to (e) in an appropriate form to any person on request." (Article 21, Paragraph 3)
JPIPA	"When an entity handling personal information is requested by a person to notify him or her of the Purpose of Use of such retained personal data as may lead to the identification of the person concerned, the entity must meet the request without delay." (Article 24, Paragraph 2)
ANPP	"On request by a person, an organization must take reasonable steps to let the person know, generally, what sort of personal information it holds, for what purposes, and how it collects, holds, uses and discloses that information." (Sub clause 5.2)
US	"In order to carry out the provisions of this section, each agency that maintains a system of records shall promulgate rules, in accordance with the requirements… which shall-- (1) establish procedures whereby an individual can be notified in response to his request if any system of records named by the individual contains a record pertaining to him;" [Subsection (f)(1)]

General Study Observations:

- There is wide variation in the definition of availability of policies/practices –this necessitates a Privacy Rights Expression Language and taxonomy
- Transparent, unambiguous, granular rules that govern well defined Personal Information and varied operations on Personal Information should be supported
- Data subjects should be able to see exactly what rules govern what data and why
- Openness is tied to the Privacy policy, but no uniform policies are described

Composite Operational Definition:

Openness: Availability to individuals of the data collector's or data user's policies and practices relating to their management of personal information; and for establishing the existence of, nature and purpose of use of personal information held about them.

6.12. Three Additional Privacy Requirements

The **Anonymity** requirement is present in many privacy instruments. However, only the Australian National Privacy Principles consider it to be its own principle. Everywhere else the concept of anonymity is covered under "Security" and/or "Collection". There are also varying "degrees" of anonymity expressed in the instruments.

The Australian National Privacy Principles state "Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organization." (Sub clause 8.0). This ensures that, where practical, data subjects always have the option of remaining anonymous. This is perhaps the most effective means of ensuring privacy as, since information cannot be traced back to the data subject, the data is no longer "personal".

When anonymity is referred to under "Security", it is used as a means of securing data by rendering it "anonymous" after it's primary purpose has been fulfilled. While anonymity is not explicitly referred to under "Collection," all instruments restrict collection of data to information necessary to the purpose of collection. This implies that if identifying information is not required for the stated purpose, then data must be collected in anonymous state.

> **Anonymity: A state in which information or data are rendered anonymous so that the data subject is no longer identifiable (Reference Source Used: EU Data Protection Directive).**

The Transborder **Data Flow** requirement is inferred in all instruments. It is covered explicitly, under its own heading, or implicitly under the principle of "Disclosure" (e.g., third-party disclosure). In the event that it is covered under its own section, it usually has the same conditions for normal third-party disclosure.

The first condition of Transborder/Disclosure is to ensure that the third party possesses a privacy policy (or third country possesses a privacy act) that is equivalent to the one possessed by the Data Collector. The second common condition of the Transborder/Disclosure principle is that data not be disclosed unless required to do so in order to complete the stated purpose or without the consent of the Data Subject.

> **Data Flow: The communication of personal data across geo-political or policy jurisdictions by private or public entities involved in governmental, economic or social activities.**

For the **Sensitivity** requirement, while there is general agreement on the principle, there are potentially major differences. For example, the EU limits the collection and use of sensitive information by force of law, while others use more ambiguous language.

Generally, Data Subjects must be informed of, and explicitly consent to, the collection, use and disclosure of sensitive information (i.e. medical or health conditions, racial or ethnic origins, political views, religious or philosophical beliefs, trade union membership or information regarding sex life) unless a law or regulation specifically requires otherwise.

> **Sensitivity: Specified data or information, as defined by law, regulation or policy, which requires specific security controls or special processing.**

7. GENERAL FINDINGS AND CONCLUSIONS

7.1. Common Terminology in Privacy Requirements

Based on our review of the instruments detailed in Chapter 6, we considered approaches to developing "harmonized" terminology that would capture the core meaning and intent of each privacy principle or requirements. As a result of our analysis, and taking a practical approach to huge variations in language and the differing placement of many principles/practices in each instrument, we derived the following operationally-focused working definitions.

These terms, or their functional equivalents, appear with regularity in information privacy instruments. The definitions are operational and strive for objectivity. They attempt to provide as neutral a basis as possible for defining key terms critical to the ISTPA Privacy Framework services. We recognize that several of these definitions are cumbersome. However, the nature of this study calls for the most objective definitions possible. Following are the "Composite Operational Definitions" from Chapter 6:

Accountability: Reporting made by the business process and technical systems which implement privacy policies to the individual or entity accountable for ensuring compliance with those policies, with optional linkages to sanctions.

Notice: Information regarding an entity's privacy policies and practices including: definition of the personal information collected; its use (purpose specification); its disclosure to parties within or external to the entity; practices associated with the maintenance and protection of the information; options available to the data subject regarding the collector's privacy practices; changes made to policies or practices; and information provided to data subject at designated times and under designated circumstances.

Consent: The capability, including support for Sensitive Information, Informed Consent, Change of Use Consent, and Consequences of Consent Denial, provided to data subjects to allow the collection and/or specific uses of some or all of their personal data either through an affirmative process (opt-in) or implied (not choosing to opt-out when this option is provided).

Collection Limitation: Constraints exercised by the data collector and user to limit the information collected to the minimum necessary to achieve a stated purpose and when required demonstrably collected by fair and lawful means.

Use Limitation: Controls exercised by the data collector or data user to ensure that personal information will not be used for purposes other than those specified and accepted by the data subject or provided by law, and not maintained longer than necessary for the stated purposes**.**

Disclosure: The release, transfer, provision of access to, use for new purposes, or divulging in any other manner, of information by the entity holding the information only with notice and consent of the data subject; the data collectors policies must be made

known to and observed by third parties receiving the information, and sensitive health information disclosures must be managed.

Access and Correction: Capability allowing individuals having adequate proof of identity to find out from an entity, or find out and/or to correct, their personal information, at reasonable cost, within reasonable time constraints, and with notice of denial of access and options for challenging denial.

Security/Safeguards: Policies, practices and controls that ensure the confidentiality, availability and integrity of personal information collected, used, maintained, and destroyed; and ensure that personal information will be destroyed or de-identified as required.

Data Quality: Ensures that information collected and used is adequate for purpose, relevant for purpose, not excessive in relation to the purposes for which it is collected and/or further processed, accurate at time of use, and, where necessary, kept up to date, rectified or destroyed.

Enforcement: Mechanisms to ensure compliance with privacy policies, agreements and legal requirements and to give data subjects a means of filing complaints of compliance violations and having them addressed, including recourse for violations of law, agreements and policies.

Openness: Availability to individuals of the data collector's or data user's policies and practices relating to their management of personal information and for establishing the existence of, nature and purpose of use of personal information held about them..

Anonymity: A state in which information or data are rendered anonymous so that the data subject is no longer identifiable.

Data Flow: The communication of personal data across geo-political jurisdictions by private or public entities involved in governmental, economic or social activities.

Sensitivity: Specified data or information, as defined by law, regulation or policy, which requires specific security controls or special processing.

7.2. Correlation of Regulations and Requirements

The following table illustrates increasing comprehensiveness of privacy instruments, as they progress from the U.S. Privacy Act of 1974 through the APEC Privacy Framework of December, 2005.

When reading the table below, note that Instruments are ordered left-to-right from oldest to most recent year of publication. There are **SIX** requirements (rows, shaded grey and red text) that have a foundation in all or nearly all Instruments. We further observe that **FOUR** Instruments (columns, red text) have all or nearly all requirements. Our research is based on, but not restricted to, these named twelve privacy Instruments, and the matrix below illustrates our findings; the more complete Matrix is shown section 7.3.

	THE PRIVACY ACT OF 1974 (US)	OECD PRIVACY GUIDELINES	UN GUIDELINES CONCERNING COMPUTERIZED PERSONAL DATA	EU DATA PROTECTION DIRECTIVE	HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996	CANADIAN STANDARDS ASSOCIATION PRIVACY CODE	US FTC FAIR INFORMATION PRACTICES	SAFE HARBOR PRIVACY PRINCIPLES	AUSTRALIAN NATIONAL PRIVACY PRINCIPLES	JAPAN PERSONAL INFORMATION PROTECTION ACT	CALIFORNIA SB 1386, "SECURITY BREACH NOTIFICATION"	APEC PRIVACY FRAMEWORK
Accountability		X		X		X					X	X
Notice	X	X	X	X	X	X	X	X	X	X	X	X
Consent	X	X	X	X	X	X	X	X	X	X		X
Collection Limitation	X	X	X	X		X			X	X		X
Use Limitation	X	X	X	X	X	X		X	X	X		X
Disclosure	X				X	X		X	X	X		X
Access and Correction	X	X	X	X	X	X	X	X	X	X		X
Security/ Safeguards	X	X	X	X	X	X	X	X	X	X		X
Data Quality	X	X	X	X		X	X	X	X	X		X
Enforcement			X	X	X	X	X	X		X	X	X
Openness	X	X		X		X			X	X		X

7.3. Requirements Mapped to Framework Services

The Compendium Matrix in this paper builds up to an analysis from privacy instruments into privacy requirements. We carried the results of this study forward as an exercise of the Tool Set Process. The ISTPA Master Toolset for Privacy, a separate ISTPA project, maps Privacy **Requirements** to Framework **SERVICES**. In reading the table, please note the following observations.'

There are ten Services (columns), matching the ISTPA Privacy Framework, and fourteen Privacy Requirements (rows, bold blue text) based on this Analysis in previous chapters. We will further analyze the correlation between Privacy Requirements and the ISTPA Framework Services. For this analysis, concepts of Principle and Practice are used interchangeably. The requirement for "Purpose Specification" is expressed in Notice and "Individual Participation" falls within Consent, Disclosure, and Access & Correction. We also found that Choice is addressed under Consent, as it is expressed in HIPAA, FTC, and APEC and a point could be made to say that Sensitive Information is covered in Consent. We do note that the Validation Service stands out for a seemingly low correlation, while Interaction, Negotiation, and Agent Service have a seemingly high correlation."

	AUDIT (LOG) SERVICE	CERTIFICATION SERVICE	CONTROL SERVICE	ENFORCEMENT SERVICE	INTERACTION SERVICE	NEGOTIATION SERVICE	VALIDATION SERVICE	ACCESS SERVICE	AGENT SERVICE	USAGE SERVICE
Accountability	X	X	X	X					X	
Notice					X				X	
Consent		X			X	X		X	X	
Collection Limitation	X				X	X			X	
Use Limitation	X		X		X	X			X	X
Disclosure		X			X	X		X	X	
Access & Correction		X			X	X		X	X	
Security Safeguards	X	X	X					X	X	
Data Quality		X	X				X			
Enforcement	X			X						
Openness					X	X			X	X
Anonymity		X		X		X			X	X
Data Flow					X	X		X	X	X
Sensitivity	X				X	X			X	X

7.4. The Full Legislation-to-Requirements Matrix

The following matrix illustrates a more complete mapping of ten basic Privacy Instruments (rows) we have identified in our narrow scope of Analysis, and the ten Privacy Requirements (columns) derived from our evaluation. In the intersect we show the key element(s) of text that has guided our interpretations of language. No observations are made in addition to the two previous sections, other than to point out that the selection of text is only one observation, not a legal argument for or against our choice.

Operational Privacy Principles/ Practices Mapped to Eleven Privacy Instruments

	Accountability	Notice	Consent	Collection Limitation	Use Limitation	Disclosure	Access & Correction	Security/ Safeguards	Data Quality	Enforcement
US Privacy Act of 1974		Agency Requirements Subsection 3-4, 11	Prior Consent	Agency Requirements Subsection 1	Agency Requirements Subsection 11	Conditions of Disclosure	Access to Records	Agency Requirements Subsection 11	Agency Requirements Subsection 5	
O.E.C.D.'s Privacy Guidelines	Accountability	Purpose Specification	Individual Participation Collection Limitation	Collection Limitation	Use limitation		Individual Participation	Security Safeguards	Data Quality	
UN Guidelines 1990		Purpose-Specification		Lawfulness and Fairness	Purpose Specification		Interested-Person Access	Security	Accuracy	Supervision and Sanctions
EU Data Protection Directive	Judicial Remedies, Liabilities and Sanctions	Information Given to the Data Subject	Criteria For Making Data Processing Legitimate	Principles Relating to Data Quality	Principles Relating to Data Quality		The Data Subject's Right of Access to Data	Confidentiality and Security of Processing	Principles Relating to Data Quality	Supervisory Authority
Health Insurance Portability and Accountability Act of 1996		Notice of Privacy Practices for PHI	Uses and Disclosures Requiring an Opportunity for the Individual to Object		Uses and Disclosures of PHI: General Rules	Notice of Privacy Practices for PHI	Access of Patients to PHI Amendment of PHI	Administrative Requirements		Responsibilities of Covered Entities Complaints to the Secretary
Canadian Standards Association Privacy Code	Accountability	Identifying Purposes	Consent	Limiting Collection	Limiting Use, Disclosure and Retention	Limiting Use, Disclosure and Retention	Individual Access	Safeguards	Accuracy	Challenging Compliance
US FTC Fair Information Practices		Notice/Awareness	Choice/Consent				Access/Participation	Integrity/Security	Integrity/Security	Enforcement/Redress
Safe Harbor Privacy Principles		Notice	Choice		Data Integrity	Onward Transfer	Access	Security	Data Integrity	Enforcement
Australian National Privacy Principles		Collection	Collection	Collection	Use and Disclosure	Use and Disclosure	Access and Correction	Data Security	Data Quality	
Japan Personal Information Protection Act		Notice of Purpose of Use at the Time of Acquisition	Consent	Proper Acquisition	Restriction by the Purpose of Use	Restriction of Provision to Third Parties	Disclosure Correction	Security Control Measures	Maintenance of the Accuracy of Data	Handling of Complaints by Entities Handling PHI Measures to Ensure Proper Handling of PHI
APEC Privacy Framework	Accountability	Notice	Choice	Collection Limitation	Uses of Personal Information	Accountability	Access and Correction	Security Safeguards	Integrity of Personal Information	Preventing Harm

Close Full Screen

Note: California SB 1386 not included in this chart because of its limited and focused scope.

7.5. Conclusions

Each of the legislative instruments, analyzed above against Privacy Requirements, is concluded with a set of Observations, which are both objective and subjective insights that the analysts gained through detailed reading and study of the instruments. These Observations will aid in the revision of the ISTPA Privacy Framework and Toolset development, and in its implementation, as well as in the analysis of other legislative instruments.

By examining the multiple sets of Observations and the process used to perform the analysis, an overall set of Conclusions was drawn. These Conclusions are divided into two parts: conclusions resulting from the analysis process itself and overarching conclusions based on the analyzed instruments.

The overall objective of this Analysis was to gain insight from the breadth of legislative instruments for the purpose of improving the ISTPA Privacy Framework and for developing a “system design” approach to its implementation. For that reason, all Observations and Conclusions should be viewed as providing some insight into building privacy management systems.

Conclusions: Analysis Process

This Analysis will support the ISTPA Privacy Framework revision and the development of an operational Toolset for implementing the Framework. However, more Analysis will need to follow when these findings are applied to the Framework. Certainly, this is not the last word in analyzing worldwide legal expressions of privacy principles nor was this particular analysis necessarily exhaustive or complete. The goal of this study was achieved, though the scope of the analysis was shaped as the study progressed. All possible discussions and subtleties in the intent of instruments were impossible to include in this analysis. Instead, practical recommendations and applicable observations were found, and these will be useful in the subsequent process of Framework revision.

Conclusions: Analyzed Instruments

Although fair information practice principles (FIP) are often viewed as simple concepts (e.g., provide Notice to data subject before data is collected), in fact the FIPs are not simple at all and have huge variation within and across instruments. Consequently, in order to enable more systematic automation of privacy policies, at a minimum the major components of each FIP should be abstracted for use in examining policies and implementing practices. This issue becomes increasingly important when organizations must observe the dictates of more than one instrument.

There is value in developing what we call "composite operational definitions" for FIP - the composites incorporate primary operational characteristics of each FIP and can be useful in a number of ways. First, they can provide a basis for mapping privacy requirements by establishing categories of requirements for business processes and systems into which more granular (and therefore more automatable and auditable) requirements can be placed. Such composites can also be used to more clearly link requirements that may fall into more than one category (for example, data quality includes data destruction, which also implicates security/safeguards).

The Analysis illustrates very forcefully the importance of developing standard definitions and a taxonomy for privacy requirements in order to facilitate absolute clarity in the meaning of a requirement and where the requirement fits in the lifecycle of Personal Information (PI) and with respect to other requirements. Even if standard "working" definitions can only be achieved for fundamental privacy building blocks (perhaps the specific parts of the composite definitions), this will facilitate our internal evaluation of the ISTPA Privacy Framework functionality, as well as assisting in understanding the operational implications of privacy requirements, use of appropriate controls, development of tools, and such.

This Analysis shows that not only is the interpretation of the privacy instruments confusing, it is increasingly complex and diffuse. Privacy appears in pieces of legislation not intent or focused on privacy and is included to address a specific concern. For example, Enhanced 911 services legislation (E-911) includes an obligation by carriers to protect the privacy of geo-location information. The result is a number of overlapping and intertwined laws that are difficult to track and address, and obviously have been excluded from this Analysis.

Part of the motivation for this Analysis was as a consequence of the submission of the ISTPA Privacy Framework in 2003 by the International System Security Engineering Association (ISSEA) as a candidate ISO Publicly Available Specification (PAS) (ISO/IEC (PAS) DIS 20886), and the response to this submission by the 26th International Conference of Data Protection and Privacy Commissioners in Wroclaw, Poland. The Wroclaw Commission in 2004 formally requested that the ISTPA/ISSEA withdraw the Framework from the ISO balloting process and recommended that the Framework receive further analysis, practical implementation and subsequent revision. This Analysis is part of a best effort to respond to the challenge of the Wroclaw Commission. ISTPA expects that this analysis and the revisions to the ISTPA Privacy Framework that will result will address the concerns raised by the Wroclaw Commission. Other related work being undertaken by ISTPA and ISSEA will further support and strengthen the Framework.

Other interesting conclusions can be drawn from this study:

- Legislation and the language of instruments start to look more alike in progression over time; more recent legislation (excluding focused legislation such as California SB 1386) reflects expanded privacy expectations and tends to incorporate more requirements seen in prior legislation. More specialized requirements (such as identity anonymity) tend to appear in more recent legislation.

- Legislation tends to be expressed as disconnected requirements (e.g., practices), with no cohesive or overall “system design” focused on the life cycle of personal information. In fact, PI life cycle issues from creation, sharing, distribution, and ultimate destruction, are not uniformly treated.

- Comparison of the many imprecise concepts contained in privacy practices/principles depends on language interpretation. However, if the legislative instruments are ‘abstracted’ to a high level (within the restricted scope of this Analysis) clear commonality in requirements emerges.

A number of other specific Conclusions can be drawn. For example, the “consequences” (e.g., sanctions) of not following a particular privacy mandate are not always explicit or uniform, but are left to the judgment and enforcement of a privacy ‘authority’. Additionally, exceptions (e.g., to Disclosure, to Access) are also vaguely treated. In part, a root cause

of the wide variation in interpreting privacy legislation is that there are no uniform and precise definitions of PI/PII or even of the concept of Identity itself. For this reason, a privacy taxonomy and a “sensitivity metric” on PI are needed. As noted, life cycle issues for PI are not uniformly treated, There tends to be more focus on “up front” issues (e.g., Notice/Consent) and less focus on the back end of PI lifecycle (e.g., subsequent use, data retention). Throughout, Privacy Policy is both pervasive and implicit.

The bottom line is that this Analysis shows that an operational Privacy Management framework is badly needed, with a supporting tool set methodology for practical conversion of privacy requirements into operational privacy services. Such a framework standard and tool set would facilitate capturing and translating diffuse legal requirements so they are more readily understood, responsibly managed, and efficiently and effectively engineered into operational infrastructure.

8. APPENDICES

8.1. Appendix A: Data versus Information

Enterprises must have an ongoing process to translate "unstructured data" into truly useful "information". Data represent raw facts; Information is data made meaningful (relevant, reliable, timely, accurate, and complete). Data are unedited stimuli (business transactions, sales, payments, etc); Information is processed data (customer balance, sales trends), used to make decisions.

Data are a collection of observations, which may or may not be true. Thus data may not be factually accurate. Information is data after they are processed:

- Cleaned from errors and reduce sources of unreliability
- Analyzed to make it relevant to decision at hand
- Organized in ways that help understanding

Within businesses and government, much activity surrounds data collection; yet, most of it does not necessarily yield information. A business or government collects data every day and sometimes hourly. Information, however, provides answers to questions that guide decision-making. This distinction is important given the privacy requirements impacting information and data collection and use.

8.2. Appendix B: Source List

- **International Security Trust and Privacy Alliance – Framework Version 1.1**
  http://www.istpa.org/pdfs/ISTPAPrivacyFrameworkV1.1.pdf
- **SC 27 New Work Item Proposal on A Privacy Framework**
  http://isotc.iso.org/livelink/livelink/fetch/2000/2122/327993/755080/105
- **Electronic Privacy Information Center**
  http://epic.org/
- **The Privacy Act of 1974 (US)**
  http://www.usdoj.gov/foia/privstat.htm
- **Council of Europe Convention of 1981**
  http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm
- **OECD Guidelines on the Protection of Privacy**
  http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_119820_1_1_1,00.htm
- **United Nations guidelines concerning Computerized personal data files**
  http://ec.europa.eu/justice_home/fsj/privacy/instruments/un_en.htm
- **Hong Kong Personal Data (Privacy) Ordinance**
  http://www.privacy.com.hk/privkita.html
- **Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995**
  http://europa.eu/scadplus/leg/en/lvb/l14012.htm
- **Canadian Standards Association - Privacy Code**
  http://www.csa.ca/standards/privacy/code/Default.asp?language=english
- **Health Insurance Portability and Accountability Act (HIPAA) - Part 160 and Part 164**
  http://www.hhs.gov/ocr/combinedregtext.pdf
- **Personal Information Protection and Electronic Documents Act – Bill C-6**
  http://www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/C-6/C-6_4/90052bE.html#8
- **ILO code of practice on the Protection of workers' personal data**
  http://www.ilo.org/public/english/protection/condtrav/pdf/wc-code-97.pdf
- **US Federal Trade Commission - Fair Information Practice Principles**
  http://www.ftc.gov/reports/privacy3/fairinfo.htm
- **US-EU Safe Harbor Privacy Principles**
  http://www.export.gov/safeharbor/SHPRINCIPLESFINAL.htm
- **ITAC Ontario Privacy Diagnostic Tool (PDT) Workbook**
  http://www.itacontario.com/policy/privacy.htm
- **Australian National Privacy Principles**
  http://www.privacy.gov.au/publications/npps01.html

- **California SB 1386, Security Breach Notification**
  http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html

- **AIPCA/CICA Generally Accepted Privacy Principles**
  http://infotech.aicpa.org/Resources/Privacy/Generally+Accepted+Privacy+Principles/Generally+Accepted+Privacy+Principles/

- **Japan Personal Information Protection Act**
  http://www.privacyexchange.org/japan/JPIPA-offtrans.pdf

- **APEC Privacy Framework**
  http://www.ecom.jp/ecom_e/home/research_file/20011119recenttrend.pdf#search=%22Japan%20Personal%20Information%20%20Principles%22

- **Independent Bankers Association of America - Privacy Principles**
  http://www.ftc.gov/reports/privacy3/comments/012b.htm

- **Australian Privacy Act 1988**
  http://scaletext.law.gov.au/html/pasteact/0/157/top.htm

- **New Zealand Privacy Act 1993**
  http://rangi.knowledge-basket.co.nz/gpacts/public/text/1993/an/028.html

- **United Kingdom Data Protection Act 1998 – Chapter 29**
  http://www.opsi.gov.uk/acts/acts1998/19980029.htm

- **United Kingdom Information Commissioners Office**
  http://www.ico.gov.uk/

- **Office of the Privacy Commissioner of Canada**
  http://www.privcom.gc.ca/index_e.asp

- **Information and Privacy Commissioner of Ontario**
  http://www.ipc.on.ca/

- **Privacy Commissioner for Personal Data, Hong Kong**
  http://www.pcpd.org.hk/engindex.html

- **Privacy In the Russian Internet**
  http://www.hro.org/docs/reps/privacy/2002/eng/index.htm

- **Privacy International**
  http://www.privacyinternational.org/

- **International Privacy Resources**
  http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-82636&als[theme]=Privacy%20and%20Human%20Rights%202004

8.3. Appendix C: Other Instruments

These following laws, regulations, and guidance documents were examined, but not used in the Chapter 6 detailed analysis. We include them within an appendix given their references to practices and principles and as examples of instruments that might be considered for further research and analysis.

Ontario Privacy Diagnostic Tool

The Ontario Privacy Diagnostic Tool (PDT) is an instrument that uses a series of questions to give businesses a 'read' on how well they manage their customers' personal information. The PDT uses internationally recognized fair information practices as the basis for determining privacy readiness. The PDT is a valuable privacy assessment tool for all businesses whose success depends on the ongoing trust of their customers. Companies that use personal information as an integral part of their business (in marketing, sales, or customer relationship management, for example) and those that may be vulnerable to security breaches will find the PDT particularly valuable. The Ontario Privacy Diagnostic Tool follows the same Privacy Principles as outlined in the Canadian Standards Association Privacy Code.

http://www.ipc.on.ca/scripts/index_.asp?action=31&P_ID=12081&N_ID=1&PT_ID=15&U_ID=0

1. Identifying Purposes
2. Consent
3. Limiting Collection
4. Limiting Use, Disclosure and Retention
5. Individual Access
6. Safeguards
7. Accuracy
8. Challenging Compliance
9. Accountability
10. Openness

ILO Code of Practice on the Protection of Workers' Personal Data

The International Labour Office - Code of Practice on the Protection of Workers' Personal Data is focused entirely on workers rights and ensuring that employers do not overstep their bounds. It possesses many common traits to other policies. It acknowledges the employers need to collect data and therefore focus mainly on limiting collection, appropriate use and security. Indeed, it tends to go to extremes in defining limits on collection. Going so far as to explicitly state that polygraphs, personality tests, genetic screening and drug testing should not be used (ref. principles 6.10-6.13).

http://www.ilo.org/public/english/protection/condtrav/pdf/wc-code-97.pdf

1. Collection of Personal Data
2. Storage of Personal Data
3. Use of Personal Data
4. Communication of Personal Data
5. Individual Rights
6. Collective rights
7. Employment Agencies

Hong Kong Personal Data Ordinance

The Hong Kong Personal Data Ordinance is to protect the privacy interests of living individuals in relation to personal data. It also contributes to Hong Kong's continued economic well being by safeguarding the free flow of personal data to Hong Kong from restrictions by countries that already have data protection laws. The Ordinance covers any data relating directly or indirectly to a data subject. It applies to any data user that controls the collection, holding, processing or use of personal data.

http://www.pcpd.org.hk/english/ordinance/ordglance.html

1. Purpose and Manner of Collection
2. Accuracy and Duration of Retention
3. Use of Personal Data
4. Security of Personal Data
5. Information to be Generally Available
6. Access to Personal Data

Council of Europe Convention 108

The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data is based in particular on respect for the rule of law, as well as human rights and fundamental freedoms. It considers that it is desirable to extend the safeguards for everyone's rights and fundamental freedoms, and in particular the right to the respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing. It recognizes that it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples.

http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm
The Council of Europe Convention is very brief, containing only “the essentials”. It is notably lacking in terms of notice, consent, access, enforcement, accountability and openness.

1. Quality of Data
    a. Obtained and processed fairly and lawfully
    b. Stored for specified and legitimate purposes and not used in a way incompatible with those purposes
    c. Adequate, relevant and not excessive in relation to the purposes for which they are stored
    d. Accurate and, where necessary, kept up to date
    e. Preserved in a form that permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.
2. Special Categories of Data
3. Data Security
4. Additional Safeguards
5. Transborder Data Flow

The AICPA/CICA Privacy Framework

The American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants (AICPA/CICA) have formed the Privacy Task Force which developed the AICPA/CICA Privacy Framework that includes the AICPA/CICA Trust Services Privacy Principles and Criteria. It is not a typical source of fair information practices; some companies are using it as a checklist for identifying potential privacy issues in their operations. Using this Framework, CPAs can help organizations design

and implement sound privacy practices and policies. Businesses that implement privacy policies in accordance with this Framework will likely meet, if not exceed, most applicable privacy laws and regulations while reducing privacy-related risks.

http://infotech.aicpa.org/Resources/Privacy/

1. Management
2. Notice
3. Choice and Consent
4. Collection
5. Use and Retention
6. Disclosure to Third Parties
7. Access
8. Security
9. Quality
10. Monitoring and Enforcement

8.4. Appendix D: Glossary

Access and Correction

Capability allowing individuals having adequate proof of identity to find out from an entity, or find out and/or to correct, their personal information, at reasonable cost, within reasonable time constraints, and with notice of denial of access and options for challenging denial.

Access Control

Restricts data or service access to a particular entity or group of entities.

Access control can be either discretionary or mandatory. Access control lists (ACL's) are typically used for discretionary controls. Labels, which indicate the subject's clearance, are used for mandatory controls.

Accountability

Reporting made by the business process and technical systems which implement privacy policies to the individual or entity accountable for ensuring compliance with those policies, with optional linkages to sanctions.

Actor

Any entity that sends or requests information to or from a service; individuals and entities that interact with and invoke Framework services and capabilities. An actor may be an individual or machine, or a corporate or government entity.

Administrator

An entity that can set or override the access rights for a system. It can change settings and grant others all or a subset of access rights to the system. An administrator, however, is not the same as an auditor.

Anonymity:

A state in which information or data are rendered anonymous so that the data subject is no longer identifiable.

Aggregation (Depersonalization)

All personally identifiable information is deleted from the data, allowing the data to be analyzed in the aggregate through a data mining processes.

Agreement Object

A collection of PI combined with set of agreements that can either restrict or allow usage of the PI.

Anonymization (De-identification)

The process of replacing Personal information with a non-identifiable linkage record in order to prevent the using entity from being able to identify the individual.

A trusted third party maintains the information needed to connect the linkage record back to the individual under the controls of the existing user agreements, laws, and policies applicable to that person's information.

Anonymous

The dissociation of PI and PII across a sufficiently large population such that no PI can be associated with a particular data subject.

Audit

A chronological record of events. Audits are typically used to provide accountability.

Auditor

The entity that sets audit controls (i.e., what is being audited) and has access to the audit records or logs. The auditor is not the administrator; the administrator is often the subject of the audit.

Authentication

The process of verifying the evidence or proof of a claimed identity.

Authorization

The mechanism used to grant access to data or services subject to access controls..

Certificate

A sequence of data providing identity or attributes for an entity. It is usually signed by a trusted entity. An example is an x.509 certificate.

Collection Limitation

Constraints exercised by the data collector and user to limit the information collected to the minimum necessary to achieve a stated purpose and when required demonstrably collected by fair and lawful means.

Consent

The capability, including support for Sensitive Information, Informed Consent, Change of Use Consent, and Consequences of Consent Denial, provided to data subjects to allow the collection and/or specific uses of some or all of their personal data either through an affirmative process (opt-in) or implied (not choosing to opt-out when this option is provided).

Credential

The representation of an identity.

Data Collection Entity

An entity that either requests PI directly from the data subject or collects agreement objects from other data collection entities.

Data Flow

The communication of personal data across geo-political jurisdictions by private or public entities involved in governmental, economic or social activities.

Data Quality

Ensures that information collected and used is adequate for purpose, relevant for purpose, not excessive in relation to the purposes for which it is collected and/or further processed, accurate at time of use, and, where necessary, kept up to date, rectified or destroyed.

Data Object

The actual data, whether PI or other, which is passed into or out of a service.

Data Subject

The individual from whom information is gathered or to whom information is directly associated. This is also the “PI owner.”

De-identification (Anonymization)

The process of replacing Personal information with a non-identifiable linkage record in order to prevent the using entity from being able to identify the individual.

A trusted third party maintains the information needed to connect the linkage record back to the individual under the controls of the existing user agreements, laws, and policies applicable to that person’s information.

Depersonalization (Aggregation)

All personal information is deleted from the data, allowing the data to be analyzed in the aggregate through a data mining processes.

Disclosure

The release, transfer, provision of access to, use for new purposes, or divulging in any other manner, of information by the entity holding the information only with notice and consent of the data subject; the data collectors policies must be made known to and observed by third parties receiving the information, and sensitive health information disclosures must be managed.

Enforcement

Mechanisms to ensure compliance with privacy policies, agreements and legal requirements and to give data subjects a means of filing complaints of compliance violations and having them addressed, including recourse for violations of law, agreements and policies.

Identification

A process by which an entity claims an identity. This usually involves associating a unique label to an entity or set of entities such as a person, machine, process, or application.

There does not need to be a direct association between the entity and the unique label and these may be aliased.

Judicial Authority

A set of rules established by a governmental body that has jurisdiction over the subject and/or data collector or user.

Notice

Information regarding an entity's privacy policies and practices including: definition of the personal information collected; its use (purpose specification); its disclosure to parties within or external to the entity; practices associated with the maintenance and protection of the information; options available to the data subject regarding the collector's privacy practices; changes made to policies or practices; and information provided to data subject at designated times and under designated circumstances.

Openness

Availability to individuals of the data collector's or data user's policies and practices relating to their management of personal information and for establishing the existence of, nature and purpose of use of personal information held about them.

Personal Information (PI)

Any data directly related to an individual or entity (such as name, e-mail address, physical addresses, government identification numbers, health information, etc.), regardless of whether the subject of that data is identified.

PI controller

Any entity that holds or controls PI.

Personally Identifiable Information (PII)

Information that associates a particular PI or set of PI to a data subject.

Permissions

Any activities relating to the handling of PI that are consistent with the data subject's preferences and that may have been negotiated with a data requestor.

Preference Object

An object that represents the data subject's privacy preferences governing use of the PI.

Privacy

The right of an individual to control his or her PI and PII. See section on "Privacy Principles" in the Introduction for more information and background.

Pseudonymous

An identity that is an alias of a data subject.

Regulatory Authority

A government or non-government entity establishing rules establishing practices and controls related to management of PI.

Security/Safeguards

Policies, practices and controls that ensure the confidentiality, availability and integrity of personal information collected, used, maintained, and destroyed; and ensure that personal information will be destroyed or de-identified as required.

Sensitivity

Specified data or information, as defined by law, regulation or policy, which requires specific security controls or special processing.

Service

A functional unit defined by the ISTPA Privacy Framework that performs actions on data objects (e.g., PI, agreement objects) either by the direct request of an actor, or by a process.

Use Limitation

Controls exercised by the data collector or data user to ensure that personal information will not be used for purposes other than those specified and accepted by the data subject or provided by law, and not maintained longer than necessary for the stated purposes**.**