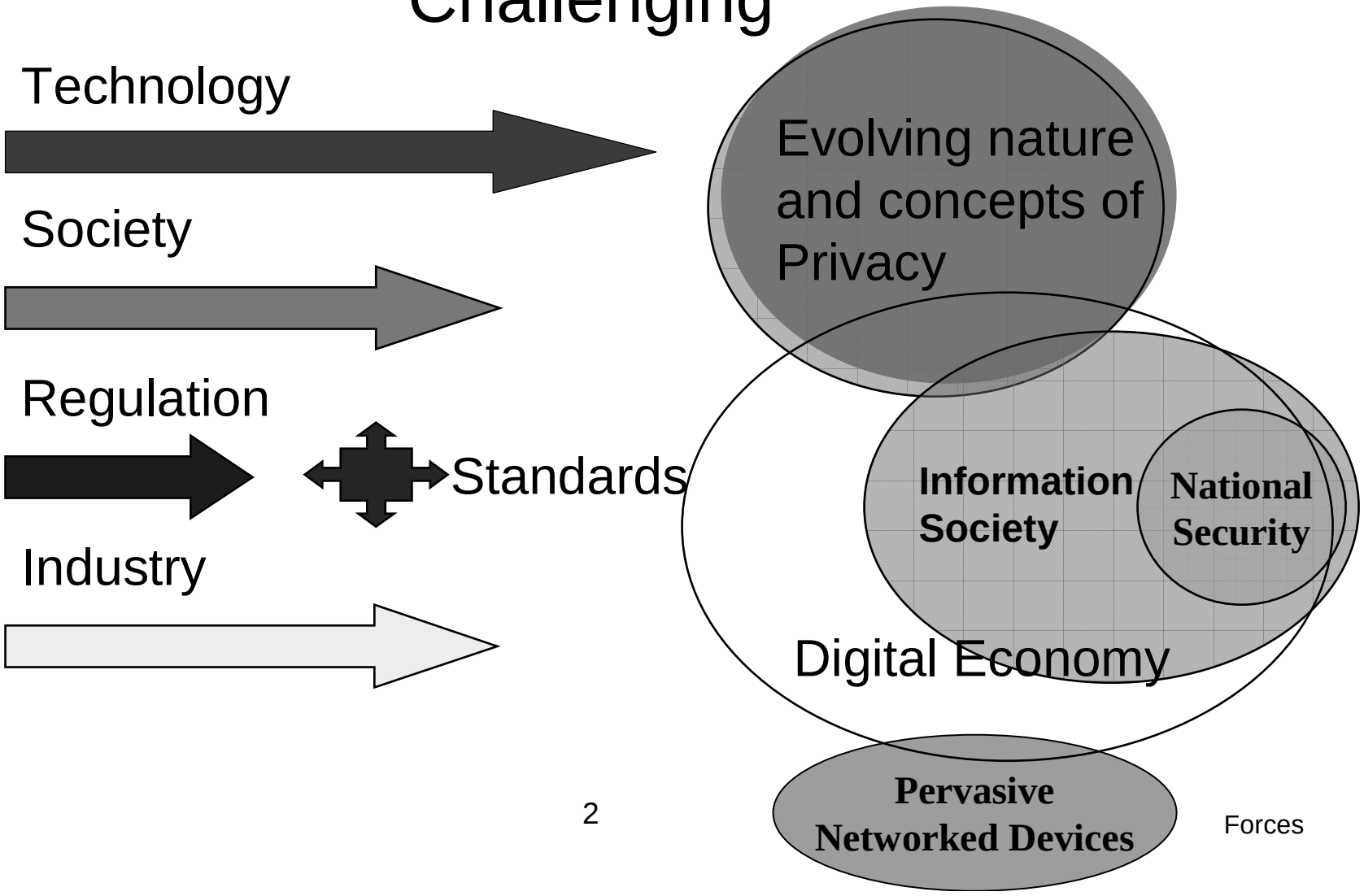
Compendium of Operational Privacy Principles

John Sabo
Director, Security and Privacy Initiatives

CACR 2006

Privacy Reality: Complex, Changing, Challenging



Forces

Fair Information Principles and Practices

The Starting Point:

- Notice and Awareness
- Choice and Consent
- Access (by the subject of the personal information)
- Information Quality and Integrity
- Update and Correction
- Enforcement and Recourse

Compendium - Operational Relationship of Privacy Principles

- Select major representative international privacy laws and directives
- Analyze disparate language, definitions and expressed requirements
- Parse expressed requirements into working set of privacy categories and terms
- Cross-map common and unique requirements
- Establish basis for a *revised* operational privacy framework to ensure ISTPA Framework Services supports full suite of requirements
  - ***Note: For purposes of this discussion, we use the term "principles" generically to describe privacy actions and more abstract principles defined in the laws and directives.***

Laws and Directives Considered

- **US Privacy Act of 1974 -** US
- Council of Europe Convention 108
- **The OECD Guidelines – Principles** - OECD
- **UN Guidelines Concerning Personalized Computer Files -** UN
- Hong Kong Personal Data (Privacy) Ordinance
- **EU Directive 95/46/EC Information Privacy Principles -** EU
- **Health Insurance Portability and Accountability Act** - HIPAA
- **Canadian Standards Association Model Code -** CSA
- International Labour Organization (ILO) Code of Practice on the Protection of Workers' Personal Data
- **US FTC statement of Fair Information Practice Principles** - FTC
- **US-EU Safe Harbor Privacy Principles** - SH
- Ontario Privacy Diagnostic Tool
- **Australian Privacy Act – National Privacy Principles** - ANPP
- The AICPA/CICA Privacy Framework
- **Japan Personal Information Protection Act** - PIPA
- **APEC Privacy Framework** - APEC
- **. . . .**

Compendium Example

APEC Privacy Framework 2005

- Preventing harm
- Integrity of Personal Information
- Notice
- Security Safeguards
- Collection Limitations
- Access and Correction
- Uses of Personal Information
- Accountability
- Choice

CSA Canadian Privacy Principles – 2001

- Accountability
- Identifying Purposes
- Consent
- Limiting Collection
- Limiting Use, Disclosure and Retention
- Accuracy
- Safeguards
- Openness
- Individual Access
- Challenging Compliance

Compendium Example-2

OECD Guidelines – 1980

- Collection Limitation
- Data Quality
- Purpose Specification
- Use Limitation
- Security Safeguards
- Openness
- Individual Participation
- Accountability

Australian Privacy Principles – 2001

- Collection
- Use and Disclosure
- Data Quality
- Data Security
- Openness
- Access and Correction
- Identifiers
- Anonymity
- Transborder Data Flows
- Sensitive Information

Common ‘Requirements’

- **Accountability**
- **Notice**
- **Consent**
- **Collection Limitation**
- **Use Limitation**
- **Disclosure**
- **Access & Correction**
- **Security/Safeguards**
- **Data Quality**
- **Enforcement**
- **Openness**

Less common:

- **Anonymity**
- **Data Flow**
- **Sensitivity**

Anonymity

- **Anonymity, defined as:** a state in which data is rendered anonymous so that the data subject is no longer identifiable (Reference Source Used: EU Data Directive)
- The **Anonymity** requirement is present in many privacy acts. 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 between the policies.
- The Australian National Privacy Principles state that “Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organization.”
- When anonymity is referred to under “Security”, it is used as a means of securing data by rendering it “anonymous” after its primary purpose has been fulfilled. While anonymity is not explicitly referred to under “Collection”, all policies 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.

Data Flow

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

- The Trans-Border **Data Flow** requirement is covered in all policies. It is covered either explicitly, under its own heading, or under the principle of “Disclosure” under third-party disclosure.

- In the event that it is covered under its own section, it usually follows the came conditions for normal third-party disclosure. The first condition of Trans-Border/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 Trans-Border/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.

Sensitivity

- **Sensitivity, defined as:** specified data or information, as defined by law, regulation or policy that requires stronger security controls or special processing

- 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 potentially 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.

Correlation

	US PRIVACY ACT OF 1974	O.E.C.D.'S GUIDELINES	UN GUIDELINES 1990	EU DATA PROTECTION	HIPAA	CANADIAN CSA	US FTC	SAFE HARBOR	AUSTRALIAN NPP	JAPAN PIPA	APEC
Accountability		X		X		X					X
Notice	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 & 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
Openness	X	X		X		X			X	X	X

	Audit	Certification	CONTROL	Enforcement	Interaction	Negotiation	Validation	Access	Agent	USAGE
Accountability	X	X	X	X					X	
Notice					X				X	
Consent		X			X	X		X	X	
Collection Limitation	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

Representative Observations

Observations on Notice

- Notice, based on ISTPA analysis, has a unique set of characteristics distinct from the content of the notification
- Notice can have various specific purposes and characteristics:
  - terms of collection and use
  - policies
  - change in privacy policies
  - timing
  - other (e.g., data breaches)
- Notice is in some instances analogous to communications - a vessel or process that can be filled with various content messages

Notice of Collection-1

Notice must be provided to Data Subject of 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 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)

Notice of Collection-2

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

- **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)
- **PIPA:** "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)

Policy Notification-1

Data Subject must be notified of 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)]b

Policy Notification-2

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

- **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)]

Changes in Policy or Data Use-1

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)]

Changes in Policy or Data Use-2

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.

- **PIPA:** "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)

Language

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)]

Timing of Notification-1

- **The EU, HIPAA and UN do not state when notification should be sent**
- **There are two dominant positions on WHEN the Data Subject should be notified.**
- **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 PIPA state that Notification must be provided *by the time of collection* and no later.**

Timing of Notification-2

- **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)

Timing of Notification-3

- **PIPA:** "…**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)

General Study Observations

- Notice is one of the Privacy Requirements dictated by all legislation both explicitly stated and implied
- 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 schema
- Notice, whether for initial collection and use or change in use, reflects the initial relationship between an organization and the individual.

Implications for the Framework

- An optional requirement for a 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 notice requirement. by the organization that has the initial relationship with the data subject
- Notice and response should "travel" with the data through the lifecycle issue of notice

- Usability (readability, navigation) of notices and unambiguous and granular traceability is needed
- Notice is an action, that is timed and has certain content pieces. This structure – including temporality - needs to be reflected in the Framework

Notice – Draft Operational Definition

Notice: statement of 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, and options available to the data subject regarding the collector's privacy practices, and characteristics associated with its language and availability.

Compendium - Analysis and Integration

- Valuable exercise – forces a rigorous analysis of privacy
- Establishing basis for ensuring Framework service functionality addresses all principles
- Next time we see privacy principles we know how to translate them into the ‘common set’ or treat them as exception requirements
- Basis for standardized operational terminology, syntax, taxonomy
- Derived generic definitions for core principles

Issues for Discussion

- Defining basic principles and addressing exception processing
- Value of operational definitions
- Granularity necessary to achieve improvements in protection of PI/PII
- Other issues….

Questions?

John Sabo

John.t.sabo@ca.com