Analysis of Privacy and Data Protection Laws and Directives Around the World

Michael Willett (Seagate)

ISTPA Board and Framework Chair

Track IIB: Global Privacy Policy

The Privacy Symposium: Boston, 23 Aug 2007
What is the ISTPA?

- The International Security, Trust, and Privacy Alliance (ISTPA) is a global alliance of companies, institutions, and technology providers working together to resolve issues related to security, trust, and privacy.
- “Making Privacy Operational”
- Published the Privacy Framework
- See www.istpa.org
ISTPA Privacy Framework Services

- Control – policy – data management
- Certification – credentials, trusted processes
- Interaction - manages data/preferences/notice
- Negotiation – of agreements, rules, privileges
- Agent – software that carries out processes
- Usage – data use, aggregation, anonymization
- Audit – independent, verifiable accountability
- Validation - checks accuracy of PI
- Enforcement – including redress for violations
- Access - subject correct/update PI
Making Privacy Operational

- Each Touch Point node configured with operational stack
- Privacy Policy is an input "parameter" to Control
- Agent is the Touch Point programming persona
-PIC contains PI and usage agreements

Legal, Regulatory, and Policy Context
Recent publication: “Analysis of Privacy Principles: Making Privacy Operational”

- Selected representative global privacy laws/directives
- Analyzed disparate language, definitions and expressed requirements
- Parsed expressed requirements into working set of composite privacy “principles”
- Cross-map and derive common/unique requirements
- Comprehensive observations and conclusions
Selected Laws, Directives, Codes

- The Privacy Act of 1974 (U.S.)
- OECD Privacy Guidelines
- UN Guidelines
- EU Data Protection Directive
- Canadian Standards Association Model Code
- Health Insurance Portability and Accountability Act (HIPAA)
- US FTC Fair Information Practice Principles
- US-EU Safe Harbor Privacy Principles
- Australian Privacy Act
- Japan Personal Information Protection Act
- APEC Privacy Framework
- California Security Breach Bill
Core Privacy Principles

- Accountability
- Notice
- Consent
- Collection Limitation
- Use Limitation
- Disclosure
- Access & Correction
- Security/Safeguards

- Data Quality
- Enforcement
- Openness

Additionally:

- Anonymity
- Data Flow
- Sensitivity
Example - “Notice Principle” includes:

- 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
- information provided to data subject at designated times and under designated circumstances
Core Principles (partial list)

**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.

**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).
Core Principles - continued

**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.

**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.
Conclusions (sampling)

- "composite operational definitions“ have unifying value
- standard definitions and a taxonomy for privacy requirements facilitate better clarity
- interpretation of privacy instruments confusing, increasingly complex and diffuse
- more recent legislation reflects expanded privacy expectations, more requirements
- legislation: disconnected requirements with no overall “system design” for PI life cycle
- comparison of imprecise concepts depends on language interpretation
- “consequences” (e.g., sanctions) are not always explicit or uniform, but left to the judgment and enforcement of a privacy ‘authority’
- exceptions (e.g., to Disclosure, to Access) are vaguely treated
- more focus on “up front” (e.g., Notice/Consent), less focus on the “back end” (e.g., subsequent use, data retention)
- Privacy Policy is both pervasive and implicit

- Net: operational Privacy Management framework is badly needed
Next Steps: Path to ISTPA Privacy Framework v 2.0

- Use *Analysis* study to evaluate existing Framework (full document available online)
- *Analysis* also being used by other organizations
- Complete expansion of Framework functions, including function labeling (modeling, automation)
- Continue collaboration with ISSEA on security mapping to the Framework
- Continue development of Master Toolset project to make Framework more accessible and usable
- Expected draft v 2.0: 2008
MAKING PRIVACY OPERATIONAL

Questions?

Michael Willett

michael.willett@seagate.com