

# PRIVACY HORIZONS: TERRA INCOGNITA

29<sup>th</sup> International Conference of  
Data Protection and Privacy Commissioners

September 25 to 28, 2007  
Montreal, Canada



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

29<sup>e</sup> Conférence internationale des commissaires  
à la protection des données et de la vie privée

du 25 au 28 septembre 2007  
Montréal, Canada

# **Making Privacy Operational**

## **Updating the ISTPA Privacy Framework**

**John T. Sabo**

**President, International Security Trust and  
Privacy Alliance (ISTPA)**

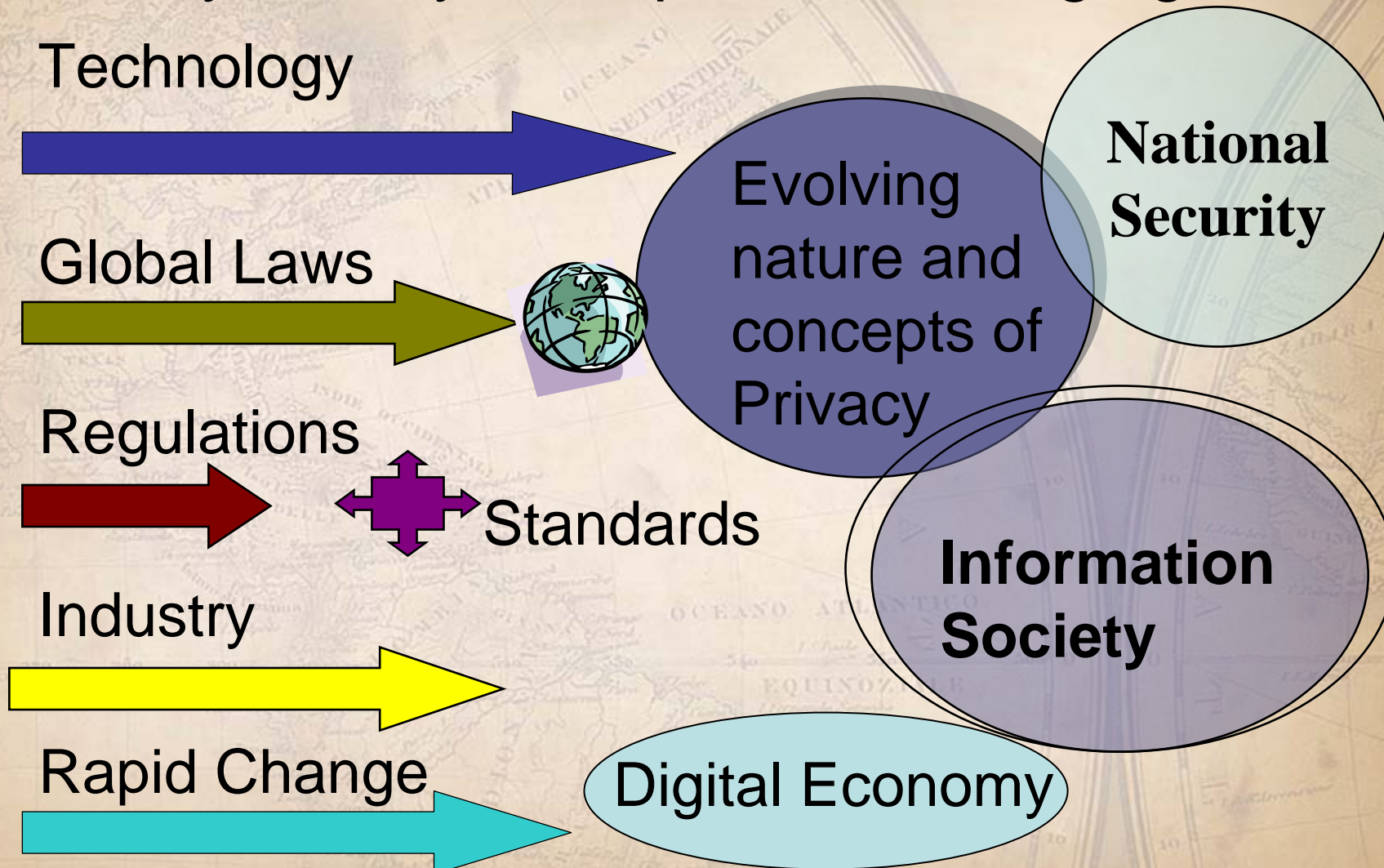
**Director Global Government Relations  
CA, Inc.**



## What is the ISTPA?

- The International Security, Trust, and Privacy Alliance (ISTPA), founded in 1999, is a global alliance of companies, institutions and technology providers working together to clarify and resolve existing and evolving issues related to security, trust, and privacy.
- ISTPA's focus is on the protection of personal information (PI)
- See [www.istpa.org](http://www.istpa.org)

# Privacy Reality: Complex, Challenging



# Global Privacy Laws and Policies – Wide Variance

OECD Privacy Principles

Fair Information Practices

HIPAA

APEC Privacy Framework

EU Data Directive

U.S. Privacy Act

CSA Model Code



# ISTPA's Perspective on Privacy

- Operational - Solution Focus
  - Migrate to privacy engineering discipline
  - Privacy framework supporting full privacy lifecycle
  - *Not a policy framework* – rather this is a technical framework for business processes and supporting IT systems
- Platform for multidisciplinary collaboration
- Must address variations in law and policies
- Industry Specific Use Cases

## ISTPA Framework v 1.1 Concepts

- An open, policy configurable set of collaborating services and capabilities used to guide the analysis, design and implementation and assessment of privacy solutions and infrastructure
- An architectural approach that provides a template usable by IT architects and program managers to develop interoperable applications

# ISTPA Privacy v 1.1 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

# ISTPA Framework Submitted as ISO Publicly Available Specification

- Submitted by ISSEA (International Systems Security Engineering Association) in October 2003 - 2004
- Balloting was to close December 11, 2004
- Caused significant discussion, including Privacy Technology Study Group under ISO JTC-1
- Withdrawal requested November 22, 2004 for additional work

## Recent Work: “Analysis of Privacy Principles: Making Privacy Operational”

- Select representative global privacy laws & directives
- Analyze disparate language, definitions and expressed requirements
- Parse expressed requirements into working set of privacy “principles”
- Cross-map and derive common and unique requirements

## 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

# Derived 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

# Next Steps: Path to ISTPA Privacy Framework v 2.0

- Use *Analysis* study to evaluate existing Framework – full document available online
- *Analysis* being used by external organizations
- Complete expansion of Framework functions, including function labeling
- Continue collaboration with ISSEA on security mapping
- Continue development of Master Toolset project to make Framework more accessible and usable
- Expected draft v 2.0: 2008

Questions?

[john.t.sabo@ca.com](mailto:john.t.sabo@ca.com)



[www.istpa.org](http://www.istpa.org)