

Introduction to ISTPA and the ISTPA Privacy Framework

John Sabo

Director, Security and Privacy Initiatives



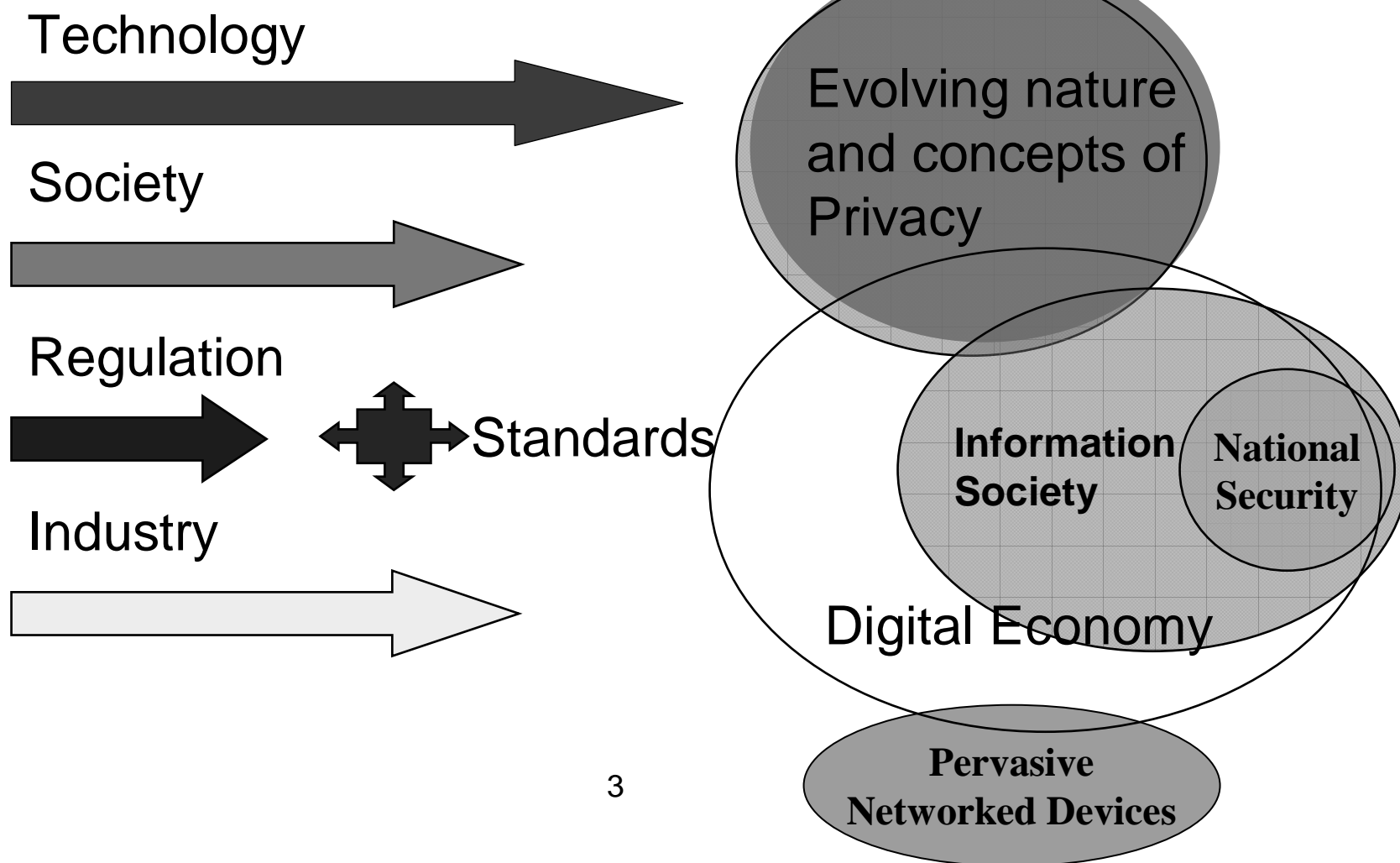
CACR 2006

Copyright © 1999-2006 International Security, Trust & Privacy Alliance
All Rights Reserved

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).

Reality Context: Complex, Changing, Challenging



ISTPA's Perspective on Achieving Resolution

- Hard Problem
- Requires Multidisciplinary, Methodology-enhanced Approach
 - ◆ Legal, Policy, Regulatory, Business, Government, Consumer, Technology
 - ◆ Use case driven, context and scenario based, modeling specific industries, legal, regulatory environments, applications: mobile commerce, healthcare, eGovernment, financial services, Homeland Security
 - ◆ CMM for Privacy Management – Unified Framework and Systems Security Engineering Capability Maturity Model

ISTPA's Perspective on Privacy

- Operational - Solution Focus
- Privacy Framework Supporting Full PI Lifecycle
- Basis for Convergence
 - Shared Privacy Vocabulary
 - Personal Information Taxonomy
 - Standardized Set of Industry Specific Use Cases
 - Platform for Multidisciplinary Collaboration
 - ◆ Policy, Law, Regulatory, Business, Consumer, Security, Technology
 - Migrate to Privacy Engineering Discipline

ISTPA Framework Submitted as ISO PAS “Fast-Track” Standard

- Submitted by ISSEA in October 2003
- Resubmitted after technical changes June 4, 2004
- Balloting was to close December 11, 2004
- Caused significant discussion, including Privacy Technology Study Group under ISO JTC-1
- Withdrawal requested by ISSEA November 22, 2004 after consultation ISSEA and a number of data protection commissioners

Wroclaw Resolution 8

8. The Conference, while acknowledging the intent and commitment of ISTPA in the area of privacy, respectfully requests the withdrawal of the ISTPA framework as a Publicly Available Specification (PAS) until the following is addressed:

- ◆ The concept of privacy on which the Draft Privacy Framework Standard is based and that the framework needs to recognize the limits of collection. The Draft defines “privacy” as “the proper handling and use of personal information throughout its life cycle, consistent with data protection principles and the preferences of the subject” The authors of the Draft understand that the collection and processing of personal information are essential to the proper functioning of modern society and commerce. processing of personal information is essential in this sense This statement rests on the assumption that there are no limits to the collection of personal data. There may be situations where the collection and. But this should not be assumed to be the rule.

Response and New Work

- Compendium of privacy laws and principles matrix (in context of Framework)
- “Services to Functions” study
- Toolset project
- Explicit inclusion of security as a Framework component
- Revision of Framework
- Use of Framework
- Possible ISO Submission

- Web Site – www.istpa.org

John Sabo

CA, Inc.

ISTPA President

John.t.sabo@ca.com

Participation Welcome

- ISTPA welcomes additional members to bring a focus on Framework applied to RFID, wireless, healthcare, financial services, government
- Privacy Passion Mandatory Requirement