

# Making Privacy Operational

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

**Michael Willett, Seagate**



**John Sabo, CA, Inc.**



**The Privacy Symposium  
Harvard University  
20 August 2008**

## 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)

## ISTPA's Perspective on Privacy

- **Operational – Technical, Operational Focus**
  - ◆ ...“making Privacy Operational”
  - ◆ based on legal, policy and business process drivers
  - ◆ privacy management is multi-dimensional with extended lifecycle requirements
- **Privacy Framework v1.1** published in 2002
  - ◆ supports the full “Lifecycle” of Personal Information
- **“Analysis of Privacy Principles: An Operational Study”** published in 2007
- See **[www.istpa.org](http://www.istpa.org)** for downloads

# Three Dimensions of Privacy Management

- **Principles/Legislation/Policies**
  - ◆ Requirements and constraints on the collection and use of personal information by government and private sector organizations
- **Business Processes**
  - ◆ Data collection, processing and storage systems and business applications which make use of PI
- **Operational Privacy Management and Compliance**
  - ◆ Architectures and applications which incorporate standardized privacy management services and controls

## Principles/Legislation/Policies

# **“Analysis of Privacy Principles: An Operational Study”**

## Laws, Directives, Codes Analyzed

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

## Analysis Methodology

- **Select** 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

# Comparative Analysis-Sample

## ■ 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

## Derived Privacy Requirements

- **Accountability**
  - **Notice**
  - **Consent**
  - **Collection Limitation**
  - **Use Limitation**
  - **Disclosure**
  - **Access & Correction**
  - **Security/Safeguards**
  - **Data Quality**
  - **Enforcement**
  - **Openness**
- **Less common:**
  - **Anonymity**
  - **Data Flow**
  - **Sensitivity**

## What we Discovered

### Example: Notice Principle

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

# PI Lifecycle Implications of “Notice”

**Notice:** Information regarding an entity’s privacy policies and practices

information provided to data subject at designated times and under designated circumstances

definition of the personal information collected

its use (purpose specification)

its disclosure to parties within or external to the entity

**PI  
Collection**

**Use, Linkage, Re-use, Aggregation**

**Destruction?**



changes made to policies or practices

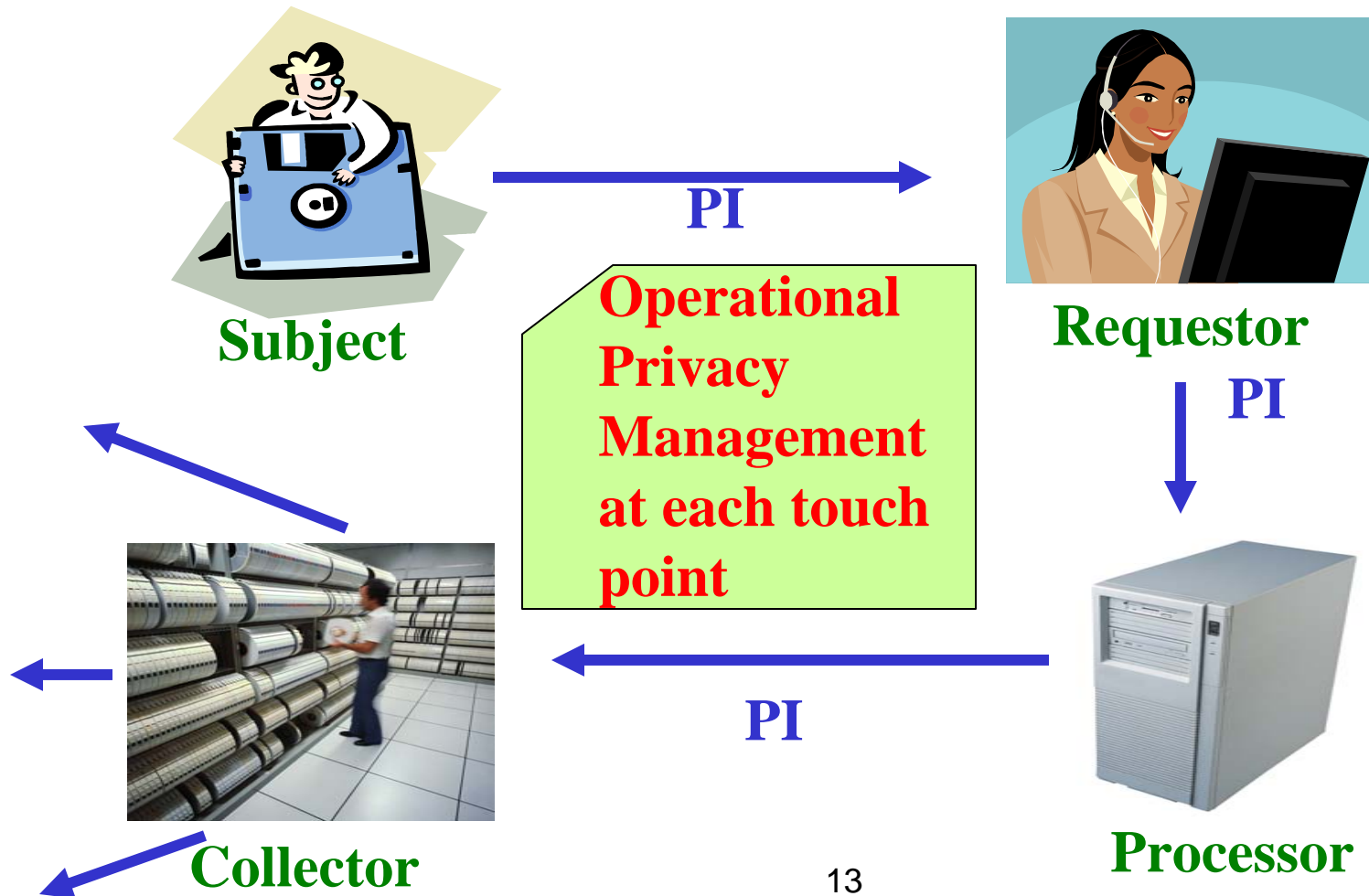
options available to the data subject regarding the collector’s privacy practices

practices associated with the maintenance and protection of the information

# Operational Privacy Management

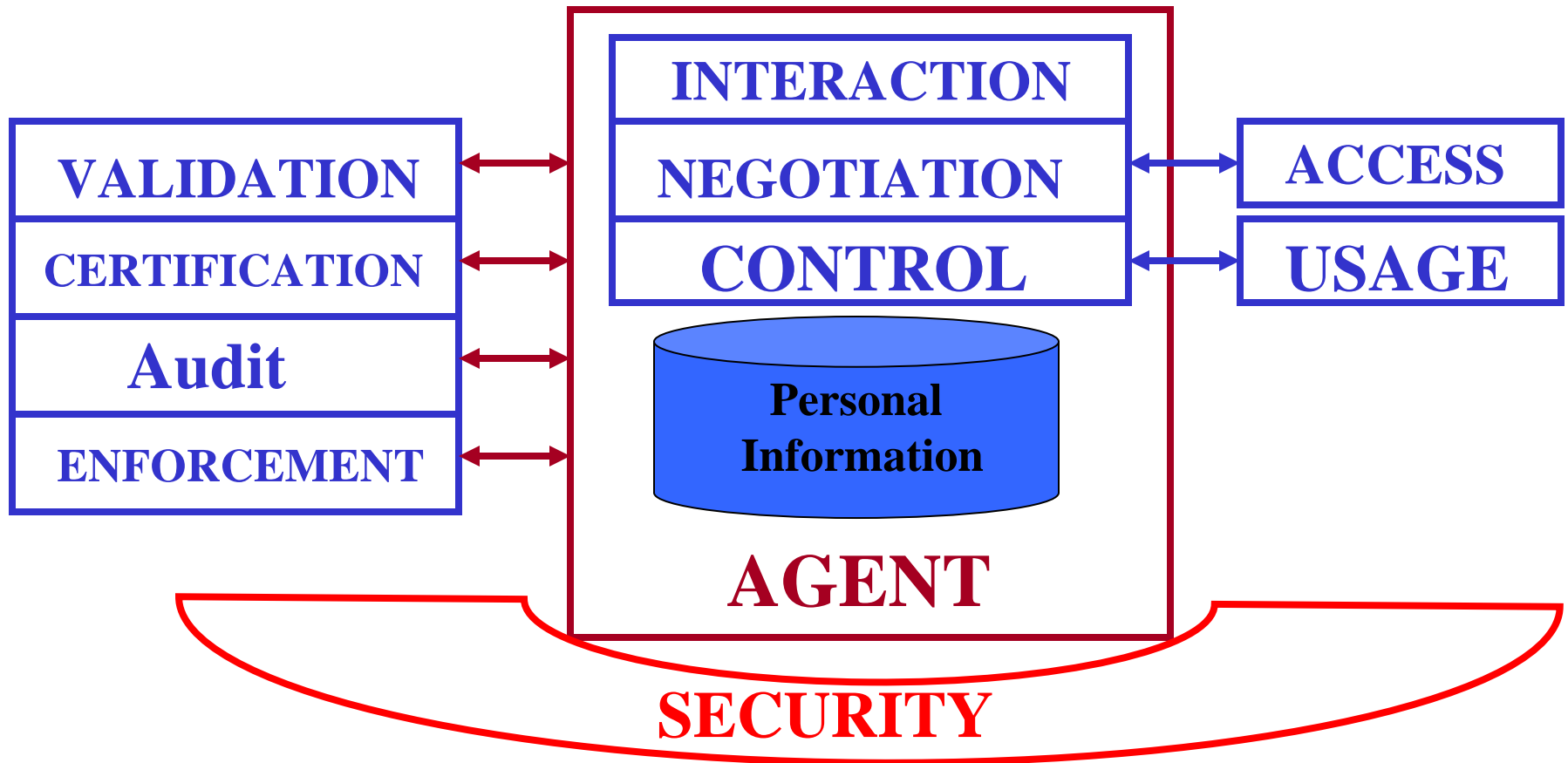
## Revising the Framework

## PI Life Cycle Perspective

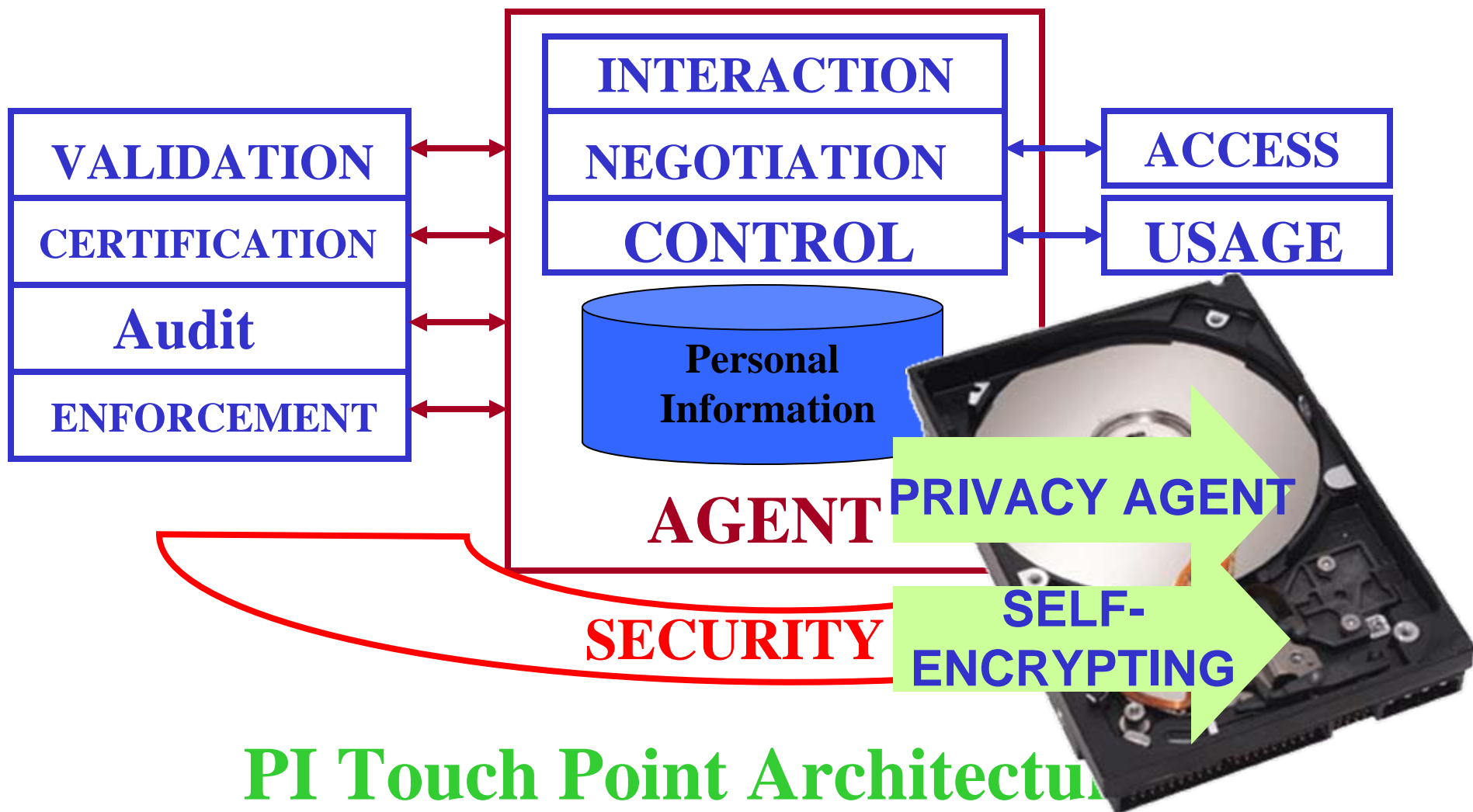


# Designing a Privacy Management System

Step by Step ....



## PI Touch Point Architecture

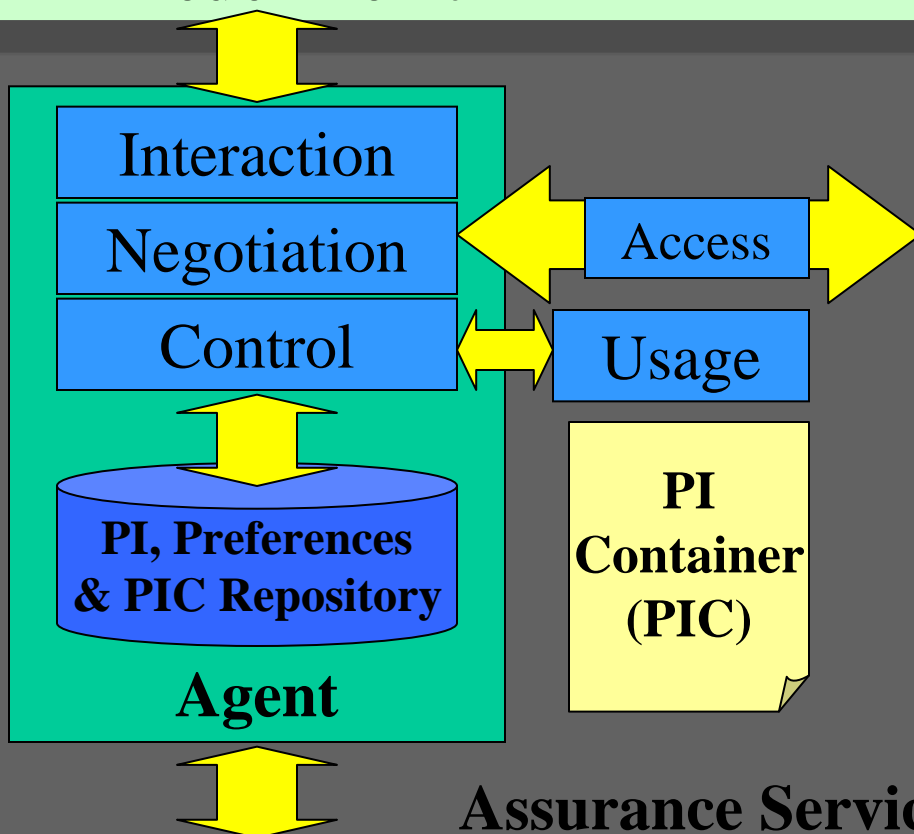


## ISTPA Privacy Framework Services

- **Control** – policy – data management
- **Certification** – credentials, trusted processes
- **Interaction** - manages data/preferences/notice
- **Negotiation** – of agreements, rules, permissions
- **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 review/suggest updates to PI

# Making Privacy Operational

## PI Touch Point



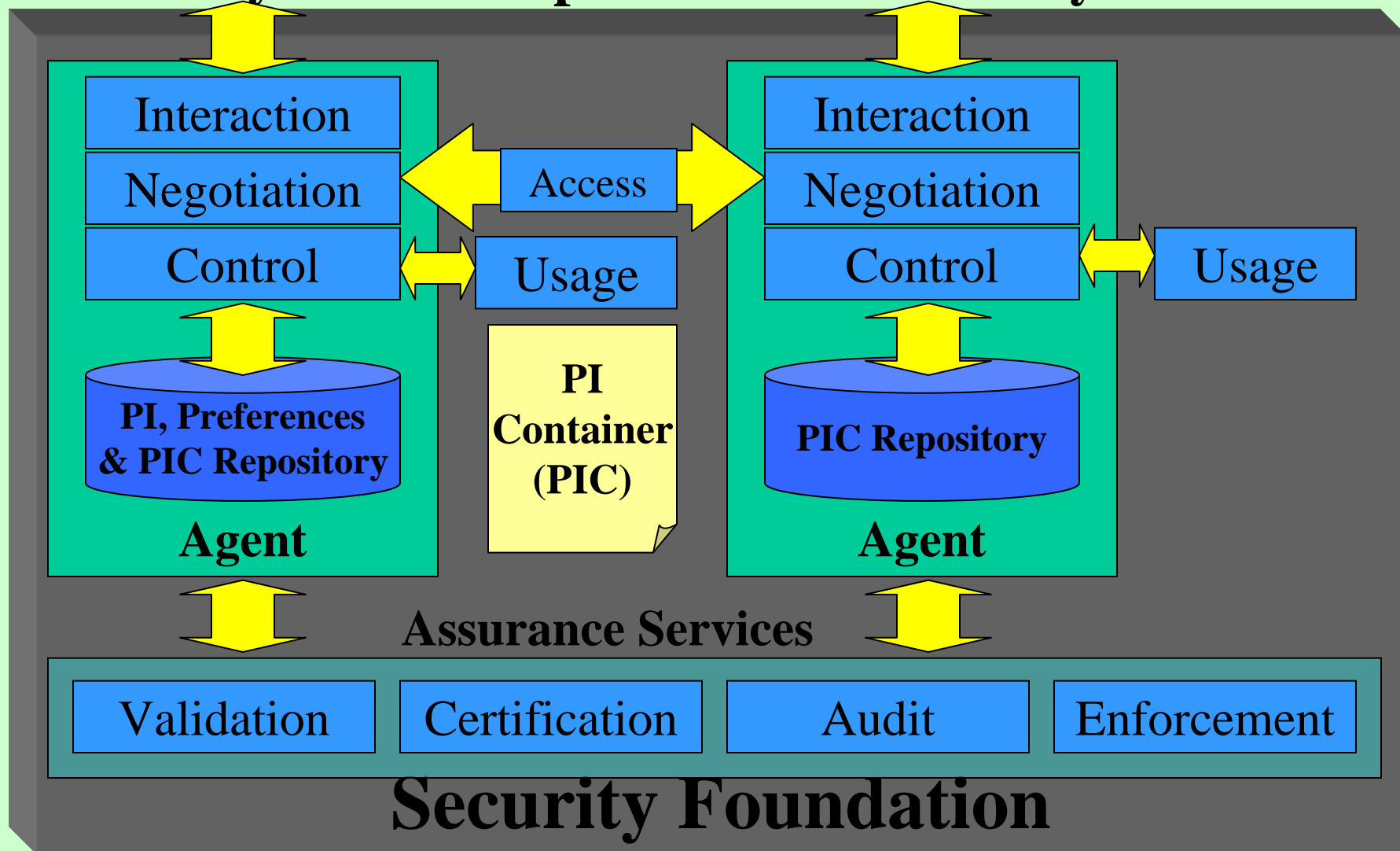
- Each Touch Point node configured with operational stack
- Privacy Policy is an input “parameter” to Control
- Agent is the Touch Point programming persona
- PIC contains PI and usage agreements

## Security Foundation

## Legal, Regulatory, and Policy Context

# Privacy SERVICES

**Any two touch points in the PI life cycle**



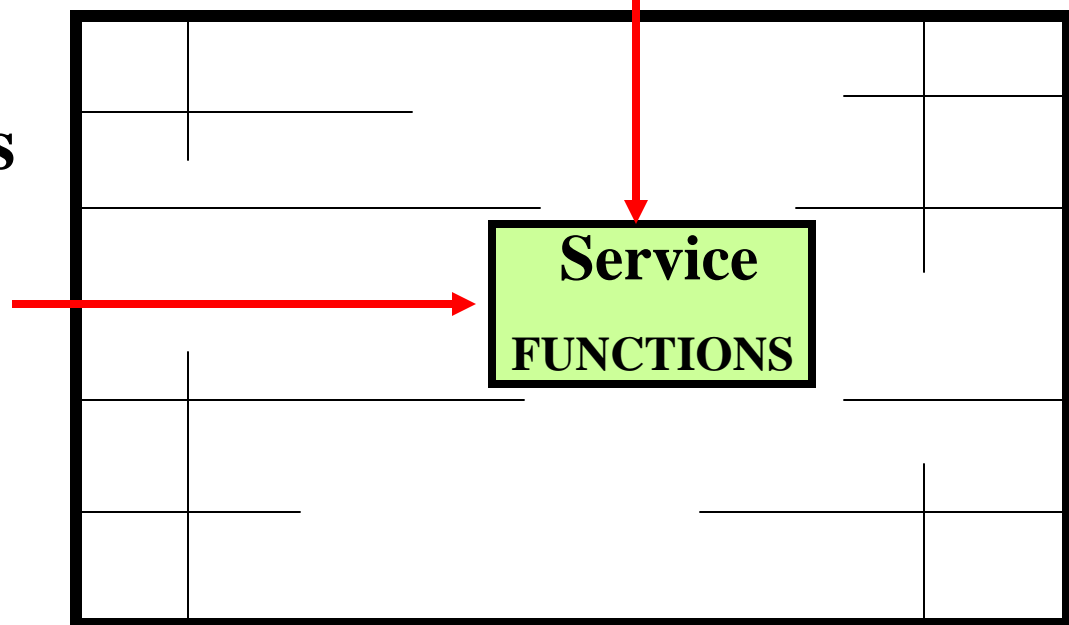
**Legal, Regulatory, and Policy Context**

# Converting Privacy Requirements to Privacy Management Operations

## ■ “Matrix” Conversion (ISTPA ToolKit Process):

**Privacy  
Requirements  
(eg,  
Principles,  
Legislation)**

### 10 Framework Services



## Next Steps for the ISTPA Privacy Framework

- Undergoing revision now
- Using the *Analysis* findings, major revisions to Service definitions and lifecycle issues for integrating services
- ISTPA has joined the OASIS standards organization as an institutional member to explore standards development
- *We welcome your input and support!*

# MAKING PRIVACY OPERATIONAL

## Questions?

**Michael Willett, Seagate**  
**michael.willett@seagate.com**



**John Sabo, CA, Inc.**  
**john.t.sabo@ca.com**

