Enterprise Privacy-Enhancing Technologies (ePETs)

Stuart Shapiro

Principal Information Privacy and Security Engineer

The MITRE Corporation

February 2, 2009

Move Toward Comprehensive Risk Management

- Breaches of personally identifiable information (PII) and breach notification requirements
  - Monetary cost
  - Public trust
  - Both private and public sector
    - OMB guidelines on incident handling, including reporting, risk-based assessment, and notification, 2006
    - OMB directive to minimize use of Social Security Numbers and PII generally, 2007

- Convergence of enterprise information risk
  - Infosec
  - Privacy
  - Intellectual property

From PETs to ePETs

- Searches for practical PETs produce tools that are overwhelmingly
  - Intended to be used by individuals, not enterprises
  - Aimed at preventing the collection of PII in the first place
- Enterprises, on the other hand, need to *manage* PII throughout the information life cycle: collection, processing, use, disclosure, retention, destruction
  - Need technologies to support PII-related business processes
- Effective support of PII-related enterprise business processes may or may not require privacy-specific technologies
  - Deployment/configuration of other technologies in ways that support privacy
  - Note sample technologies mentioned in ISE Privacy Guidelines
- ePETs are enterprise-oriented tools, including those that are not privacy-specific

PET Models and Some Arbitrary Examples

- Data subject
  - Privacy History Eraser
  - Tor
- Data steward
  - Camouflage
  - Symantec Data Loss Prevention

A Partial Commercial ePET Categorization

- Data desensitization/anonymization
  - de-identification, data masking, obfuscation
- Content identification
- Policy enforcement
  - Network monitoring
  - Endpoint event detection
  - Enterprise digital rights management (eDRM)

From Technologies to Business Processes

- ePETs by themselves don’t necessarily help if they don’t support relevant business processes
- ePET and business process categorization enable appropriate mappings
- 70/20/10 heuristic
  - 70% of PII-related enterprise business processes are common across organizations
  - 20% of PII-related enterprise business processes are specific to the *type* of organization
  - 10% of PII-related enterprise business processes are specific to the *individual* organization
  - Specialization may involve additional high-level processes and/or additional sub-processes
  - Concept is more important than the specific numbers

Constructing a Mapping

- Direct
  - ePETs to business processes
- Indirect (to business processes via some intermediary)
  - Use cases
    - Use cases can align ePETs with critical business processes
  - Fair Information Practices
    - FIPs can align ePETs with privacy compliance and risk areas
  - Privacy program components
    - Privacy stack can align ePETs with operational privacy elements
- Sanity check: Do ePETs in the same category map to the same __________?
  - *Purpose of categorization is to facilitate technology selection and deployment*

Workshop Objectives

- Explore the topic of ePETs from multiple points of view
  - Enterprises managing PII
  - Enterprise information infrastructure
  - Government regulators
  - Researchers

- Develop a common understanding and a basis for moving forward as a community of interest

Workshop Agenda

1:00 – 1:15	Introduction	Ann Cavoukian, IPC of Ontario
1:15 – 1:35	Setting the Stage	Stuart Shapiro, MITRE
1:35 – 1:55	Initial Reactions	Panelists
1:55 – 2:15	Point of View	Ken Anderson, Ontario IPC
2:15 – 2:30	Point of View	Charmaine Lowe, Office of the BC CIO
2:30 – 2:45	Point of View	Khaled El Emam, University of Ottawa
2:45 – 3:00	Point of View	Joseph Alhadeff, Oracle
3:00 – 3:20	Break	
3:20 –	Discussion	All

A Working Definition of ePETs

Enterprise privacy-enhancing technologies are data stewardship tools that help organizations appropriately (i.e., in accordance with Fair Information Practices) manage PII throughout the information life cycle.

Additional Material

U.S. Federal Government Drivers

- Privacy Act
- E-Government Act

- Office of Management and Budget (OMB) directives to federal agencies
  - Agency privacy officers (senior agency official for privacy), 2005
  - Incident handling, including reporting, risk-based assessment, and notification, 2006
  - Minimize use of Social Security Numbers and personally identifiable information (PII) generally, 2007
  - Counts and breakdowns for privacy reviews and issues, 2008

Moving Beyond Point Solutions

- Architectures serve as broad templates that carry with them certain desirable properties
  - System
  - Enterprise
- Given that privacy is a desirable property, can we identify/develop architecture(s) that by their nature support privacy?
  - Support PII-related business processes through appropriate use of ePETs
- Privacy-enhanced architecture (PEA)
  - Systematic deployment, configuration, and coordination of privacy controls so as to comprehensively address privacy risk
  - Controls should map to business processes as well as risks

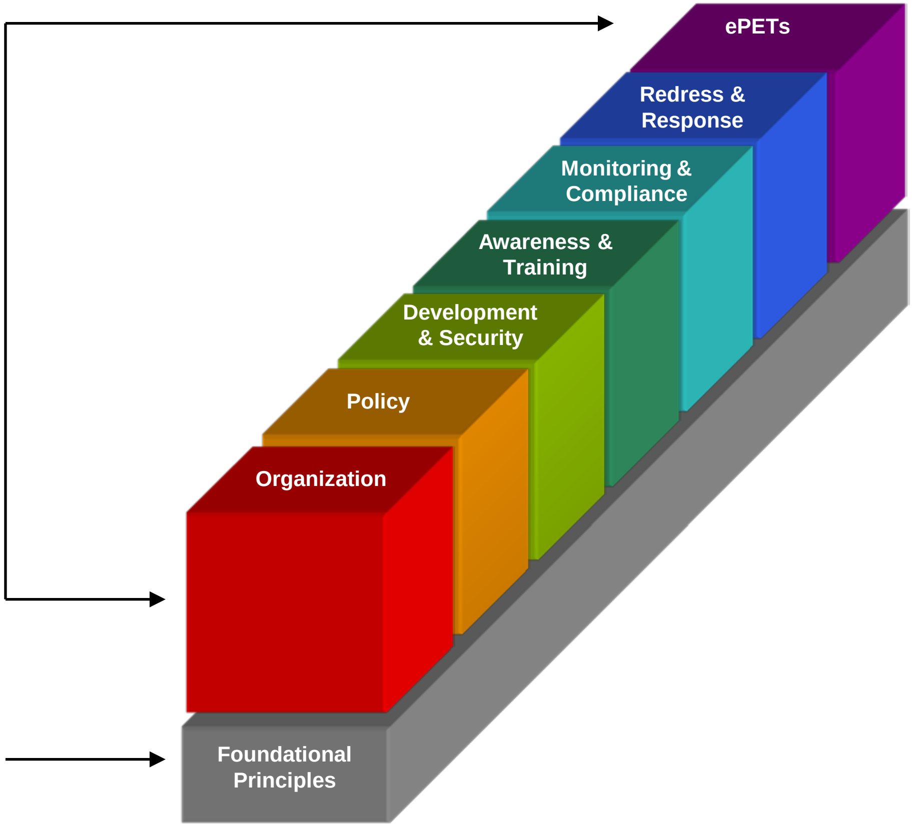
Privacy-Enhanced Architecture (PEA): Two Approaches

- Technological pointillism
  - Systematic deployment of point solutions so as to provide comprehensive privacy risk management at the system or enterprise level
  - E.g., adaptation of U.S. National Institute of Standards and Technology (NIST) computer security guidance
    - System category > confidentiality/integrity/availability impact levels > control sets
- Technological palette
  - Seamlessly embedding ePETs within system or enterprise design so as to achieve comprehensive privacy risk management
  - Analogy with service-oriented architecture (SOA)
    - Focus on business processes
    - Loose coupling of services and specific technologies
  - E.g., dynamic data desensitization, design of downstream business processes

Effective Privacy Programs

Components of a Privacy Program

Components are built on Foundational Privacy Principles



ePETs

Redress & Response

Monitoring & Compliance

Awareness & Training

Development & Security

Policy

Organization

Foundational Principles