Privacy Management: A Positive Perspective on Privacy Standardization

2012 NSTIC/IDtrust Workshop

Gaithersburg, March 13-14, 2012

John Sabo, Director Global Government Relations, CA Technologies

Chair, OASIS IDtrust Member Section Steering Committee

NSTIC and Privacy

- The Strategy's vision is:
  - Individuals and organizations utilize secure, efficient, easy-to-use, and interoperable identity solutions to access online services **in a manner that promotes confidence, privacy, choice, and innovation**
  - The Identity Ecosystem…will increase … **Privacy protections for individuals, who will be able trust that their personal data is handled fairly and transparently**
  - The Identity Ecosystem will **use privacy-enhancing technology and policies** to inhibit the ability of service providers to link an individual's transactions, thus ensuring that no one service provider can gain a complete picture of an individual's life in cyberspace By default, only the minimum necessary information will be shared in a transaction

Fair Information Practices/Principles

- Accountability
- Notice
- Consent
- Collection Limitation
- Use Limitation
- Disclosure Constraints
- Access and Correction
- Security/Safeguards
- Data Quality
- Enforcement
- Openness
- Anonymity
- Sensitivity

Privacy and Standardization

- No common definition of privacy internationally, and many varied perspectives of what constitutes privacy and personal information
  - User interests
  - Context
  - Effective notice
  - Jurisdiction and location
  - Harmonization of privacy regulations across jurisdictions
  - Law enforcement and national security access
  - Availability
  - “Right to be Forgotten”

Innovative Technologies, New Business Models, Risk Issues and Governmental Policies are Drivers for Standardization in Privacy Management

- Networked and Cloud-based
  - government services
  - smart grid systems
  - electronic health systems
  - social networks, online business services….
- Cybersecurity risk management
- Data protection, privacy and data retention – increasingly policy-dependent
- Standards necessary to ensure policy manageability, trust and compliance
- NSTIC

OASIS Privacy Standardization Face to Face Meeting London, October 2011

- Gershon Janssen, Peter Brown, Jamie Clark, John Sabo - OASIS
- Alissa Cooper, CDT and IETF
- Martin Euchner, ITU-T, Standardization Secretariat, Advisor to SG-17
- Charles Brookson, ETSI, Chair Operations Control Group
- Steve Johnston, Canada, ISO/IEC JTC1, SG27, WG5
- Christine Runnegar, ISOC
- Rigo Wenning, W3C

SDOs Addressing Privacy

- IETF
  - Building security into RFCs - RFC 3552 guidance for incorporating security into the standardization process - would like to do that more formally with privacy
  - In progress (RFC 3323 , 3325) – privacy services to not leak information to third parties and Privacy Extensions for IPv6 – (RFC 3041, 4941) – non-persistent identifiers
- W3C
  - Range of privacy related initiatives – extending from P3P to Prime to PrimeLife projects, language for Privacy Policy Negotiation and Semantics-Driven Enforcement – Do Not Track –tracking protection working group

SDOs Addressing Privacy

- ITU-T
  - SG-17 has produced 17 recommendations addressing “privacy aspects” and currently progressing 12 drafts
  - Technical measure of PII protection of current interest to SG-17 – new work item on information management
- ETSI
  - Primarily focused on wireless security particularly GSM
  - Coordination with GSMA’s Mobile Privacy Initiative - set of universal Mobile Privacy Principles that describe the way in which mobile consumers' privacy is respected and protected when consumers use mobile applications and services
  - Mobile Privacy Design Guidelines - outlining a set of Privacy Design Guidelines for Mobile Application Development (and an annex of illustrative examples)

SDOs Addressing Privacy

❑ISO

- ISO 29100 – Privacy Framework
  - defining privacy safeguarding requirements as they relate to personally identifiable information (PII) processed by any information and communication system in any jurisdiction
- ISO 29101 – Privacy Reference Architecture
  - best practices for a consistent, technical implementation of privacy requirements as they relate to the processing of personally identifiable information (PII) in information and communication systems
- ISO 29190 – Privacy Capability Assessment Model
  - provides guidance to organizations for assessing how mature they are with respect to their processes for collecting, using, disclosing, retaining and disposing of personal information

OASIS Privacy Management Reference Model and Methodology (PMRM)

- An analytic tool and methodology developed to:
  - improve the ability to analyze use cases in which personal information is used, communicated, processed and stored
  - understand and implement appropriate operational privacy management functionality and supporting mechanisms
  - Manage privacy rules and achieve compliance across policy and system boundaries
  - support the stakeholders having an interest in the use case service or application

What Makes PMRM Unique?

- Support for networked, interoperable services, applications and devices - managing personal information **across legal, regulatory and policy environments in interconnected domains**

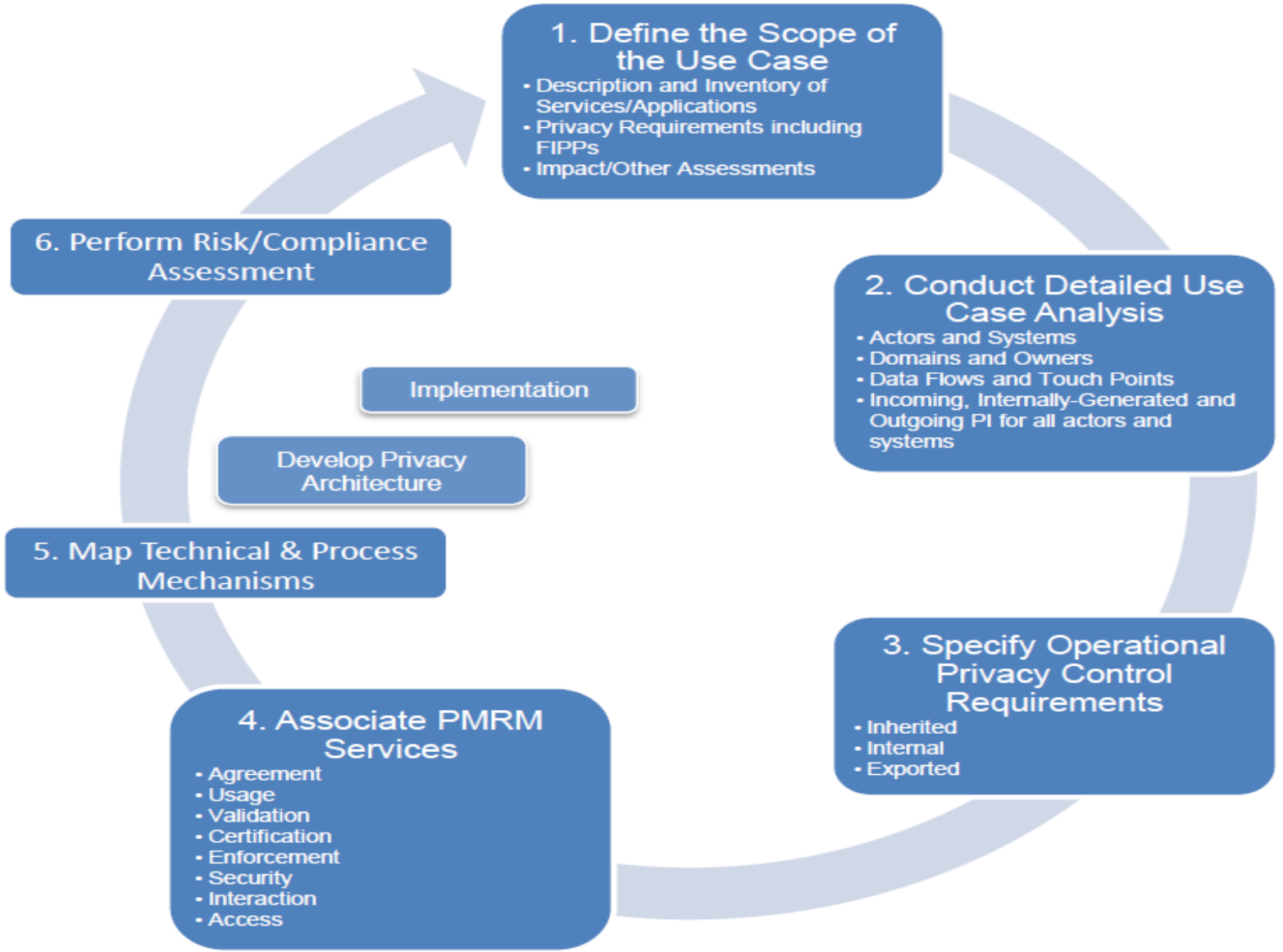
- Applicability to privacy management and compliance in cloud computing, health IT, smart grid, social networking, federated identity and similarly **complex environments**

- An **organizing structure** for exposing privacy requirements for specific business systems, organizing privacy management mechanisms, and improving systemic privacy management risk assessment

- **Support for "privacy by design"** concepts

  - ***PMRM is Not*** a static or a prescriptive model - implementers have flexibility in determining the level and granularity of analysis necessary for a particular use case

PMRM Methodology



Questions ?

john.t.sabo@ca.com
www.ca.com

www.ca.com

www.oasis-open.org

ca technologies