Privacy Management Reference Model and Methodology (PMRM)

John Sabo
Co-Chair, PMRM Technical Committee
Chair, OASIS IDtrust Member Section
What is the Privacy Management Reference Model (PMRM)?

• Adopted as a formal Committee Specification July 2013
• An analytic tool and methodology developed to:
  o improve the ability to analyze use cases in which personal information is used, communicated, processed and stored
  o understand and implement appropriate operational privacy management functionality and supporting mechanisms
  o achieve compliance across policy and system boundaries
  o support the stakeholders having an interest in the use case service or application

• See www.oasis-open.org for PMRM TC information and the Committee Specification
Why is the PMRM Important?
How relevant to cloud environments?

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

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

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

- 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
Three Major Components

• A conceptual model of privacy management, including definitions of terms

• A methodology

• A set of operational services together with the inter-relationships among these three elements.
PMRM Methodology

Use Case Description & High-Level Privacy Analysis
- Application and Business Process Descriptions
- Applicable Privacy Policies
- Initial Privacy Impact or Other Assessments

Risk and/or Compliance Assessment

Iterate

Implementation

Develop Privacy Architecture

Detailed Privacy Analysis
- Actors and Systems
- Domains and Domain Owners
- Roles and Responsibilities
- Touch Points and Data Flows
- Incoming, Internally-Generated, and Outgoing PI
- Inherited, Internal, and Exported Privacy Controls

Technical Functionality & Business Processes Supporting Selected Services

Functional Services Necessary to Support Privacy Controls
- Agreement
- Usage
- Validation
- Certification
- Enforcement
- Security
- Interaction
- Access

Privacy Management Analysis
# PMRM – Methodology Flow

## High Level Privacy Use Case Analysis

<table>
<thead>
<tr>
<th>Services/Applications</th>
<th>Privacy Requirements</th>
<th>Impact/Other Assessments</th>
</tr>
</thead>
</table>

## Detailed Privacy Use Case Analysis

<table>
<thead>
<tr>
<th>Domains and Owners</th>
<th>Risks - Responsibilities</th>
<th>Data Flows and Touch Points</th>
<th>Systems [and Subsystems]</th>
<th>Actors</th>
</tr>
</thead>
</table>

## PI in Use Case Systems

- **System 1**
  - Incoming/Internally Generated/Outgoing

- **System n**
  - Incoming/Internally Generated/Outgoing
Operational Privacy Control Requirements

<table>
<thead>
<tr>
<th>Inherited</th>
<th>Internal</th>
<th>Exported</th>
</tr>
</thead>
</table>

Services Required for Operationalized Controls

<table>
<thead>
<tr>
<th>Agreement</th>
<th>Usage</th>
<th>Validation</th>
<th>Certification</th>
<th>Enforcement</th>
<th>Security</th>
<th>Interaction</th>
<th>Access</th>
</tr>
</thead>
</table>

Technical and Process Mechanisms

Risk Assessment

Iterative Process
# PMRM Services

<table>
<thead>
<tr>
<th>Core Policy Services</th>
<th>Privacy Assurance Services</th>
<th>Presentation &amp; Lifecycle Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agreement</td>
<td>Validation</td>
<td>Interaction</td>
</tr>
<tr>
<td>Usage</td>
<td>Security</td>
<td>Enforcement</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Access</td>
</tr>
<tr>
<td>SERVICE</td>
<td>FUNCTIONALITY</td>
<td>INFORMAL DEFINITION</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>AGREEMENT</td>
<td>Define and document permissions and rules for the handling of PI based on applicable policies, individual preferences, and other relevant factors; provide relevant Actors with a mechanism to negotiate or establish new permissions and rules; express the agreements for use by other Services</td>
<td>Manage and negotiate permissions and rules</td>
</tr>
<tr>
<td>USAGE</td>
<td>Ensure that the use of PI complies with the terms of any applicable permission, policy, law or regulation, including PI subjected to information minimization, linking, integration, inference, transfer, derivation, aggregation, and anonymization over the lifecycle of the use case</td>
<td>Control PI use</td>
</tr>
<tr>
<td>VALIDATION</td>
<td>Evaluate and ensure the information quality of PI in terms of Accuracy, Completeness, Relevance, Timeliness and other relevant qualitative factors</td>
<td>Check PI</td>
</tr>
<tr>
<td>CERTIFICATION</td>
<td>Validate the credentials of any Actor, Domain, System or Subsystem, or system component involved in processing PI; verify compliance and trustworthiness of that Actor, Domain, System or Subsystem, or system component against defined policies</td>
<td>Check credentials</td>
</tr>
<tr>
<td>ENFORCEMENT</td>
<td>Initiate response actions, policy execution, and recourse when audit controls and monitoring indicate that an Actor or System does not conform to defined policies or the terms of a permission (agreement)</td>
<td>Monitor and respond to audited exception conditions</td>
</tr>
<tr>
<td>SECURITY</td>
<td>Provide the procedural and technical mechanisms necessary to ensure the confidentiality, integrity, and availability of personal information; make possible the trustworthy processing, communication, storage and disposition of privacy operations</td>
<td>Safeguard privacy information and operations</td>
</tr>
<tr>
<td>INTERACTION</td>
<td>Provide generalized interfaces necessary for presentation, communication, and interaction of PI and relevant information associated with PI; encompasses functionality such as user interfaces, system-to-system information exchanges, and agents</td>
<td>Information presentation and communication</td>
</tr>
<tr>
<td>ACCESS</td>
<td>Enable data-subject Actors, as required and/or allowed by permission, policy, or regulation, to review their PI that is held within a Domain and propose changes and/or corrections to their PI</td>
<td>View and propose changes to stored PI</td>
</tr>
</tbody>
</table>
Applying the PMRM in Practice
– TC developing draft Use Case Template

- Need for a tool based on the PMRM specification to facilitate use case development and analysis

- A draft template based on PMRM was developed for the OASIS Privacy by Design workshop at the KuppingerCole European Identity Conference in Munich, May 2013

- Being refined and used to facilitate work of the OASIS Privacy by Design Documentation for Software Engineers (PbD-SE) Technical Committee

- Will help make the PMRM methodology more accessible for stakeholders, including business managers, technical teams and regulators
Use Case Template Development Overview

(Five Stages)

Regulatory and Business Policies
Privacy Controls
Functional Services

Applications
Data Subjects
Domains
Domain Owners
Roles

Data Flows
Touch Points

Use Case Title
Category
Description

Systems
Products
PI/PII
3. General description of the Use Case:

- The Acme Insurance Company in Toronto, Canada, offers customers the opportunity to enroll in a program to have specific vehicular data automatically transmitted from their vehicle to the company. With data subject consent and agreement with the privacy policies associated with this program, Acme will establish a communication link to the vehicle manufacturer, located in Bruges, and receive specific vehicle data relevant to driving behaviors, including speed, location, trip frequency and duration, miles driven, and safety function deployments such as ABS activation. These data flows are integrated with Acme’s backend systems, which include algorithms for calculating driving patterns related to driving behaviors and risk of accidents. In exchange, the Acme Insurance Company offers a program of increasing reductions in the customer’s premiums for driving patterns indicative of good driving behaviors and reduced accident risk. Local insurance agents have access to summary information related to their customer driving patterns.
Use Case Development - Stage One

[Description highlights]

• customers may enroll in a program to have specific vehicular data automatically transmitted from their vehicle to Acme to assess driving behaviors
• In return, Acme Insurance offers yearly reductions in the customer’s premiums for driving patterns indicative of good driving behaviors and reduced accident risk
• with data subject consent and agreement with privacy policies, the company opens a communication link to the vehicle manufacturer for that customer’s vehicle data
• data includes speed, location, time/date, trip frequency and duration, miles driven, safety function deployments such as ABS activation
• Insurance company backend systems use algorithms to infer driving patterns indicative of driving behaviors, accident risk
• Local insurance agents have access to summary driving information for their customers
• the insurance company and manufacturer are located in different countries and certain applications and systems are cloud-based
Use Case Development

Stage Two

4. Application(s) associated with Use Case (Relevant applications and products where personal information is communicated, created, processed, stored or deleted):

- Vehicle’s Internal Communications Application (Vehicle Data Collection and Communication to Vehicle Manufacturer)
- Vehicle Manufacturer Backend Data Collection Application
- Insurance Company’s Data Collection and Analysis Application
- Insurance Company’s Customer Facing Web Portal
- Insurance Company’s Agent Portal
Use Case Development

Stage Two

5. Data subject(s) associated with Use Case (Include any data subjects associated with any of the applications in the use case)

- The registered Insured person associated with the vehicle VIN
- Other drivers designated by the vehicle owner
6. Domain Owners, Domains and Roles associated with Use Case – Definitions:

- **Domain Owner** - the Participant responsible for ensuring that privacy controls and functional services are managed in business processes and technical systems within a given domain.

- **Domain** - both physical areas (such as a customer site or home) and logical areas (such as a wide-area network or cloud computing environment) that are subject to the control of a particular domain owner.

- **Roles** - the roles and responsibilities assigned to specific Participants and Systems within a specific privacy domain.
Use Case Development

Stage Two

6. Domain Owners, Domains and Roles associated with Use Case - continued

- **Domain 1**: Hudson Motor Company’s Vehicle Communications Data Center, Vehicle Owner’s Web Portal and Backend Data Collection Application

- **Domain 1 Owners**: VP, Vehicle Manufacturer’s Vehicle Communication and Data Division and Director, Cloud Hosting Service (CHS)

- **Roles**: Application design, development, content, testing, integration testing with external systems, and adherence to corporate security and privacy policies; management of raw datasets of vehicle information; security, availability, other SLA’s
6. Domain Owners, Domains and Roles associated with Use Case - continued

- **Domain 2:** Acme Insurance Customer Vehicle Data Communications and Processing Application
- **Domain Owner:** VP for Customer Vehicle Support Programs
- **Role:** Application concept and specifications, content, production certification, communication with external systems, and adherence to corporate security and privacy policies; management of sub-sets of vehicle information associated with operation of the vehicle, including date/time of operation, location, speed, braking data, airbag deployment....
Use Case Development
Stage Two

6. Domain Owners, Domains and Roles associated with Use Case - continued

- **Domain 3**: Acme Insurance Software Development Group

- **Domain Owner**: CTO

- **Role**: Application design, software development, testing, integration testing, production certification, communication with external systems, and adherence to corporate security and privacy policies; management of live test data associated with operation of the vehicle, including date/time of operation, location, speed, braking data, airbag deployment....
Use Case Development

Stage Two

6. Domain Owners, Domains and Roles associated with Use Case - continued

- **Domain 4:** Insurance Company Customer Portal

- **Domain 4 Owners:** VP for Customer Vehicle Support Programs and Director, Empire Cloud Systems (ECS)

- **Role:** Application concept and specifications, content, production certification, communication with external systems, and adherence to corporate security and privacy policies; management of individual customer preferences, consent information, additional vehicle operators, and driving information.
Use Case Development

Stage Two

6. Domain Owners, Domains and Roles associated with Use Case - continued

- **Domain 5**: Insurance Company Analytics Processing System for Vehicle Data

- **Domain Owner**: VP for Advanced Analytics

- **Role**: Schema and analytics design, software development and testing, data processing, data storage, data disposition, reports and files output to Customer Profile Department; management of driving evaluation assessment data derived from system-based algorithms
6. Domain Owners, Domains and Roles associated with Use Case - continued

- **Domain 6**: Customer Profile Department

- **Domain Owner**: Director, Customer Profile Department

- **Role**: Review of files and driving profiles received from Analytics, interface with insurance agents servicing customers, review of automated decision recommendations requiring further analysis' management of summary assessment information
Use Case Development
Stage Two

6. Domain Owners, Domains and Roles associated with Use Case - continued

- **Domain 7**: Local Insurance Agent

- **Domain Owner**: EVP for Regional Sales

- **Role**: Review of files and summary driving profiles received from Analytics, interface with customers, explanation of summary assessment information
7. Systems supporting the Use Case applications (System - a collection of components organized to accomplish a specific function or set of functions having a relationship to operational privacy management)

- Insurance Customer Web Portal (customer interface)
- Insurance Vehicle Data Processing System (“VDPS”)
- Vehicle Manufacturer Data Management/Communication System (“Up-Star”)
- ....
8. **PI and PII covered by the Use Case** *(The PI and PII collected, created, communicated, processed, stored or deleted within privacy domains or systems, applications or products)*

   - Registered driver name, Account Number, VIN
   - Registered driver contact information
   - Linked vehicle operational data
   - Linked vehicle time and location data
   - Linked evaluation assessment and summary information

[Note: per domain, system, application or product depending on level of use case analysis]
Use Case Development
Stage Four

9. Data Flows and Touch Points Linking Domains or Systems

- Touch points - the points of intersection of data flows with privacy domains or systems within privacy domains
- Data flows – data exchanges carrying PI and privacy policies among domains in the use case
Use Case Development
Stage Four

9. Data Flows and Touch Points Linking Domain Clusters
10. Legal, regulatory and/or business policies governing PI and PII in the Use Case (The policies and regulatory requirements governing privacy conformance within use case domains or systems and links to their sources)

- Government(s) regulations
- Vehicle Manufacturer privacy policies
- Telecom Carrier privacy policies
- Cloud Hosting policies and agreements
- Insurance Company privacy policies
- Data Subject Consent preferences
- Specific policies governing apps (e.g., “Data Communications to Manufacturer”)

- Links to policies ....
  - http://acmeinsurancegroupinc.biz/vehicle.privacy/
  - http://HudsonCarCompany.biz/privacy_vehicle/....
Use Case Development
Stage 5

11. Privacy controls required within the Use Case

• Control - a process designed to provide reasonable assurance regarding the achievement of stated objectives

[Note: to be developed against specific domain, system, or applications as required by internal governance policies and regulations]
12. Functional Services Necessary to Support Privacy Controls

- Service - a collection of related functions and mechanisms that operate for a specified purpose

<table>
<thead>
<tr>
<th>Core Policy Services</th>
<th>Privacy Assurance Services</th>
<th>Presentation &amp; Lifecycle Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agreement</td>
<td>Validation</td>
<td>Interaction</td>
</tr>
<tr>
<td>Usage</td>
<td>Security</td>
<td>Enforcement</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Access</td>
</tr>
</tbody>
</table>
PMRM and PbD

Starting Point: Use Case Development

- PMRM offers basis for development of standardized use case templates, use cases, and PbD policy and technical assessments
- High-level use case development is an important first step
- Useful for understanding lifecycle of policies, operational implementations and conformance
- Input from multiple stakeholders
- PMRM TC welcomes your participation!
Privacy by Design
The 7 Foundational Principles

Ann Cavoukian, Ph.D.
Information & Privacy Commissioner
Ontario, Canada

Privacy by Design is a concept I developed back in the 90’s, to address the ever-growing and systemic effects of Information and Communication Technologies, and of large-scale networked data systems.

Privacy by Design advances the view that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization’s default mode of operation.

Initially, deploying Privacy-Enhancing Technologies (PETs) was seen as the solution. Today, we realize that a more substantial approach is required — extending the use of PETs to PETS Plus — taking a positive-sum (full functionality) approach, not zero-sum. That’s the “Plus” in PETS Plus: positive-sum, not the either/or of zero-sum (a false dichotomy).

Privacy by Design extends to a “Trilogy” of encompassing applications: 1) IT systems; 2) accountable business practices; and 3) physical design and networked infrastructure.

Principles of Privacy by Design may be applied to all types of personal information, but should be applied with special vigour to sensitive data such as medical information and financial data. The strength of privacy measures tends to be commensurate with the sensitivity of the data.

The objectives of Privacy by Design — ensuring privacy and gaining personal control over one’s information and, for organizations, gaining a sustainable competitive advantage — may be accomplished by practicing the following 7 Foundational Principles (see over page):
Thank You

john.annapolis@verizon.net

www.oasis-open.org