Evolving OASIS Privacy by Design Standards

Dawn N. Jutla, PhD, Director, Board of OASIS
Professor of Computer Science and Business, Sobey School of Business, Saint Mary’s University
Convener and co-Chair/co-editor, OASIS PbD-SE TC with Commissioner Ann Cavoukian; co-editor, OASIS PMRM

PRIVACY ENGINEERING WORKSHOP
April 9-10, 2014
National Institute of Standards and Technologies, US Dept. of Commerce
EMERGING Standards to make Privacy-by-Design Instinctual on the Internet

FOR EVERY ORGANIZATION AND SOFTWARE ENGINEER – ON PURPOSE, IN A MANAGED WAY
GARTNER 2014 PREDICTS:
By 2017, 80% of consumers will **collect, track and barter** their personal data for cost savings, convenience and customization.
Why should business care ... about consumer privacy & empowerment over personal data?

- Loss of customers, customer loyalty, stock value, and brand reputation
- Increased legal costs, class action lawsuits
- Shareholder and board dissatisfaction
OASIS Privacy by Design Documentation for Software Engineers (PbD-SE) TC

Enabling privacy to be embedded into IT system design and architecture

Dawn Jutla, dawn.jutla@gmail.com, Chair
Ann Cavoukian, Commissioner.ipc@ipc.on.ca, Chair
Gershon Janssen, gershon@qroot.com, Secretary

Table of Contents

- Announcements
- Overview
- Subcommittees
- TC Liaisons
- Technical Work Produced by the Committee
- Expository Work Produced by the Committee
- External Resources
- Mailing Lists and Comments
- Press and Commentary
- Additional Information
OASIS Privacy Management Reference Model (PMRM) TC

Providing a guideline for developing operational solutions to privacy issues

Michael Willett, mwillett@nc.rr.com, Chair
John Sabo, john.annapolis@verizon.net, Chair
Gershon Janssen, gershon@qroot.com, Secretary

Table of Contents
- Announcements
- Overview
- Subcommittees
- Technical Work Produced by the Committee
- Expository Work Produced by the Committee
- External Resources
- Mailing Lists and Comments
- Additional Information

Announcements

Participation in the OASIS PMRM TC is open to all interested parties, including privacy policy makers, privacy and security consultants, auditors, IT systems architects and designers of systems that collect, process, use, share, transport, secure, or destroy Personal Information. OASIS also invites representatives of other TCs, external organizations, and standards bodies that may find the PMRM useful in developing privacy management use cases in their contexts. Contact member-services@oasis-open.org for more information on joining the TC.

Overview

The OASIS PMRM TC works to provide a standards-based framework that will help business process engineers, IT analysts, architects, and developers implement privacy and security policies in their operations. PMRM picks up where broad privacy policies

Related links
- Charter
- IPR Statement
- FAQ
- Membership
- Obligated Members
- Email Archives
- Comments Archive
- Ballots
- Documents
- Schedule
- Press

TC Sponsors
- NIST
- Primeron Technologies, Inc.
- Veterans Health Administration

Organizations listed above are OASIS Sponsor-level members who have representatives serving on this TC.
PbD principles are internationally recognized with mappings/alignment to FIPPs, GAPPs and NIST 800-53 Appendix J controls.

Help stakeholders to visualize privacy requirements and design from software conception to retirement.

A specification of a methodology, mappings, and guidance to help software engineers to:

- Model and translate Privacy by Design (PbD) principles to conformance requirements within software engineering tasks,
- Produce privacy-aware software, and document artifacts as evidence of PbD-principle compliance.
- Collaborate with management and auditors to simplify demonstration of compliance/audits.
OASIS Privacy Management Reference Model and Methodology (PMRM) Emerging Standard

TC Chair: John T. Sabo, Retired TC co-Chair: Michael Willett

PMRM provides a model and methodology for translating & mapping privacy requirements, as the basis for a PRIVACY SERVICE ARCHITECTURE: [http://j.mp/oasisPMRM](http://j.mp/oasisPMRM)

KEY STRENGTH: Gets at how personal data flow among data platforms... 360 stakeholder view of privacy requirements.

Major elements of this emerging standard’s methodology and the PbD-SE methodology unify and align with the state-of-the-art in the:

- Dennedy, Finneran, and Fox’s Privacy Engineering Manifesto book (industry-led – McAfee)
- Shostack’s Threat Modeling book (industry led - Microsoft)
- Content in the Privacy Engineering program at Carnegie Mellon and extant privacy literature (university-led)
Scope of the OASIS PbD-SE and OASIS PMRM Standard-Track Work Products

**Defining** Principles, Legal, and Policy Requirements

**Defining** detailed privacy requirements across contexts & privacy services

**Designing** Architecture for Privacy Software

**Building** Privacy-enriched Software Apps and Systems

- Privacy-by-Design Principles & FIPPs & GAPPs
- Privacy Laws and Policies
- Privacy Control Statements
- Detailed Privacy Requirements
- Multiple Points of View
- Stakeholder Connectivity and Contexts
- Privacy Components and Services
- Privacy Software Architecture
- Privacy-enriched Software Apps and Systems

OASIS PbD-SE crosses the entire 4-stage spectrum from principles to implementation.
Applicable to all organizations and individuals producing Information Technology Products and Services

Software Engineer: A person that adopts engineering approaches, such as established methodologies, processes, architectures, measurement tools, standards, organization methods, management methods, quality assurance systems and the like, in the development of large scale software, seeking to result in high productivity, low cost, controllable quality, and measurable development schedule.

Source: Adapted from Y. Wang, Senior Member of the IEEE and ACM. Theoretical Foundations of Software Engineering, Schulich School of Engineering, University of Calgary, 2011.

Large scale software extends to include apps that scale to millions of users

Organizations and individuals adopting design processes, privacy methodologies, models, and standards to obtain better user privacy going forward.
### RACI Definitions

- **R** - Who is Responsible
  - The person who is assigned to do the work

- **A** - Who is Accountable
  - The person who makes the final decision and has the ultimate ownership

- **C** - Who is Consulted
  - The person who must be consulted before a decision or action is taken

- **I** - Who is Informed
  - The person who must be informed that a decision or action has been taken

#### RACI Chart for OASIS PbD-SE Methodology (WIP)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>3.1 Assess Organizational Readiness</strong></td>
<td>Document Privacy Policy Document</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Document Privacy Roles/Training Program in Organization</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>3.2 Scope Privacy Requirements &amp; Reference Architecture</strong></td>
<td>Document Functional Privacy Requirements &amp; hooks to Reference Architecture</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>3.3 Conduct Risk Analysis on Use Cases</strong></td>
<td>Document Business Model with Personal Data Flows</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>3.4 Identify Privacy Resource Allocation</strong></td>
<td>Document privacy resource allocation to SE team</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>3.5 Create RACI for Producing Artifacts</strong></td>
<td>Document RACI assignment to artifact production</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>3.6 Customize Privacy Architecture</strong></td>
<td>Document Privacy Architecture</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>3.7 Conduct Periodic Review</strong></td>
<td>Document Review of Artifacts throughout the PDLC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>3.8 Execute Code Testing &amp; Privacy Evaluation</strong></td>
<td>Document testing and evaluation for privacy usability - <strong>metrics</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>3.9 Create Retirement Plan</strong></td>
<td>Document plan for retirement of software solution</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>3.10 Sign-off</strong></td>
<td>Document sign off with checklist</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>PbD “Sub-Principles”</strong></td>
<td><strong>Compliance Criteria</strong></td>
<td><strong>Requirement(s)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------------------</td>
<td>--------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>I. Proactive not Reactive; Preventative not Remedial</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| 1.1–Demonstrable Leadership: A clear commitment, at the highest levels, to prescribe and enforce high standards of privacy protection, generally higher than prevailing legal requirements. | • Commitment to apply OASIS Specification to software engineering project | • Documentation MUST normatively reference PdD-se specification  
• Documentation MUST reference the applicable privacy policy |
| 1.2–Defined Community of Practice: Demonstrable privacy commitment shared by organization members, user communities and stakeholders. | • Relevant stakeholders and team assembled for project | • Documentation must describe privacy champ, lead.  
• Documentation MUST describe assignment of privacy resources to software teams, and responsibilities, accountability, consultation, and information supplied to all software stakeholders |
| 1.3–Proactive and iterative: Continuous processes to identify privacy and data protection risks arising from poor designs, practices and outcomes, and to mitigate unintended or negative impacts in proactive and systematic ways. | • OASIS Specification applied throughout the software engineering life cycle.  
• Privacy metrics are defined and monitored in a system of regular reviews | • Project plan MUST include privacy section  
• Other documents SHOULD include privacy section *(might be limited to saying not applicable)*  
• Documentation MUST include privacy review reports *(either in reviewed documents or in separate report)*  
• Documentation MUST include defined privacy metrics. |
# Privacy as the Default Setting

## 2.1 Purpose Specificity

Purposes must be specific and limited, and be amenable to engineering controls.

### Compliance Criteria

- OASIS PbD-SE methodology and OASIS PMRM specifications applied
- For each functional use case/user story, document models of privacy requirements/design with the EQUIVALENT to the unified modeling language (UML) used in software engineering:
  - Use Case Template or User Story Boards
  - Use Case Diagram
  - Misuse Case Diagram
  - Class Diagram
  - Activity Diagram
  - Sequence Diagram

## 2.2 Adherence to Purposes

Methods must be in place to ensure that personal data is collected, used and disclosed:

- in conformity with specific, limited purposes;
- in agreement with data subject consent; and
- in compliance with applicable laws and regulations.

### Compliance Criteria

- The OASIS PMRM Privacy Use Case Template is RECOMMENDED for describing 360° view of stakeholder privacy requirements.
- Documentation MUST describe functional use case/user story; privacy requirements; design requirements.

## 2.3 Engineering Controls

Strict limits should be placed on each phase of data processing lifecycle represented in software, including:

- Limiting Collection;
- Collecting by Fair and Lawful Means;
- Collecting from Third Parties;
- Uses and Disclosures;
- Retention;
- Disposal, Destruction; and Redaction
- Transparency and Visibility

### Compliance Criteria

- Documentation MUST describe data and behavioural requirements for each use case/user story, and possible misuses of data.
- Documentation MUST describe selection of privacy controls/services and where they apply to functional requirements.

### Document Identification

Document identification of privacy controls and services e.g. the PMRM-type Services:

- e.g. Agreement, Validation, Usage, Interaction, Certification, Security, Enforcement, and Access
- AND other
- e.g. Minimization, De-Identification, Monitoring, Data classification services.
### 3. Privacy Embedded into Design

#### 3.1 Holistic and Integrative: Privacy commitments must be embedded in holistic and integrative ways

- Followed Privacy architectural design principles e.g. Comprehension (Visibility and Transparency), Consciousness (Awareness), Consent, Choice, Context (Locality etc.), Confinement, Consistency, Access, Security..
- Privacy Architecture easily integrated into functional architecture

- Documentation MUST include identification of privacy architectural design principles
- Documentation MUST contain a Privacy Architecture
- Documentation MUST contain description of the Business Model showing personal data flows for software services

#### 3.2 Systematic and Auditable: A systematic, principled approach should be adopted that relies upon accepted standards and process frameworks, and is amenable to external review.

- Acknowledged software engineering process/methodology adopted
- Privacy Metrics, e.g. effectiveness, monitored

- Documentation MUST identify the software engineering process/methodology used
- Documentation SHOULD contain evidence of monitoring of privacy metrics

#### 3.3 Review and Assess: Detailed privacy impact and risk assessments should be used as a basis for design decisions.

- Completed PIA and Risk Assessment
- Completed Priority Matrix of Privacy Controls/Threats from Risk Analysis

- Documentation MUST contain a PIA
- Documentation MUST contain Privacy Risk Assessment for use cases/user stories

#### 3.4 Human-Proof: The privacy risks should be demonstrably minimized and not increase through use, misconfiguration, or error.

- Appropriate privacy failsafe mechanisms adopted

- Documentation MUST contain identification and description of privacy controls.
## Privacy Architecture Design Principles: The 7 Cs

<table>
<thead>
<tr>
<th>Principle</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comprehension</td>
<td>Users should <em>understand</em> how personal identifiable information (PII) is handled, who’s collecting it and for what purpose, and who will process the PII and for what purpose across software platforms. Users are entitled to visibility to know all parties that can access their PII, how to access/correct their own data, the limits to processing transparency, why the PII data is being requested, when the data will expire (either from a collection or database), and what happens to it after that. This category also includes legal rights around PII, and the implications of a contract when one is formed.</td>
</tr>
<tr>
<td>Consciousness</td>
<td>Users should be <em>aware</em> of when data collection occurs, when a contract is being formed between a user and a data collector, when their PII is set to expire, who’s collecting the data, with whom the data will be shared, how to subsequently access the PII, and the purposes for which the data is being collected.</td>
</tr>
<tr>
<td>Choice</td>
<td>Users should have <em>choices</em> regarding data collection activities in terms of opting in or out, whether or not to provide data, and how to correct their data.</td>
</tr>
<tr>
<td>Consent</td>
<td>Users must first consent (meaning informed, explicit, unambiguous agreement) to data collection, use, and storage proposals for any PII. Privacy consent mechanisms should explicitly incorporate mechanisms of comprehension, consciousness, limitations, and choice.</td>
</tr>
<tr>
<td>Context</td>
<td>Users should/must be able to <em>change privacy preferences</em> according to context. Situational or physical context—such as crowded situations (for example, when at a service desk where several people can listen in on your exchange when you provide a phone number, or when you are in the subway with cameras and audio on wearables around you)—is different from when you perform a buy transaction with Amazon.com or provide information to an app registered with an aggregator that sells to advertisers. Data also has context (such as the sensitivity of data, for example, financial and health data) could dictate different actions on the same PII in different contexts.</td>
</tr>
<tr>
<td>Confinement</td>
<td>Users must/should be able to set/request limits on who may access their PII, for what purposes, and where and possibly when/how long it may be stored. Setting limits could provide some good opportunities for future negotiation between vendors and users.</td>
</tr>
<tr>
<td>Consistency</td>
<td>Users should <em>anticipate with reasonable certainty</em> what will occur if any action in their PII is taken. That is, certain actions should be predictable on user access of giving out of PII.</td>
</tr>
</tbody>
</table>

PRIVACY ARCHITECTURAL BLUEPRINT

- Employee
- Management
- Auditor
- Strategic Partner
- Operational Partner
- Customer

User Request → To-Access

- Policy Design → To-Implementation
- Monitor → To-Develop
- Monitor → To-Comply
- Audit → To-Assurance
- De-identify → To-Partner
- Complaint → To-Resolution

Analyze → To-Learn/Continuously Improve

Services for Integration

- Privacy Policy Mgmt
- Data Mgmt. & Analytics
- Audit
- Contract & Rule Mgmt.
- Visualization
- Compliance Mgmt.
- Monitoring
- Retention Mgmt

PMRM Services: Agreement, Usage, Validation, Security, Certification, Enforcement, Interaction, Access

Privacy Knowledge Base Mgmt
Privacy Context/User Preference Mgmt Service
De-identification Service
Redaction Service
Analytics Services
Data classification Service

FUNCTIONAL PRIVACY SERVICES

FUNCTIONAL SOFTWARE

User

©Dawn N. Jutla
The Software Engineers’ 1000 word models: Example Representations for Documentation
Spreadsheets

- **Columns**
  - Description of Personal Data/Data Cluster
  - Personal Info Category
  - PII Classification
  - Source
  - Collected by
  - Collection Method
  - Type of Format
  - Used By
  - Purpose of Collection
  - Transfer to De-Identification
  - Security Control during Data Transfer
  - Data Repository Format
  - Storage or data retention site
  - Disclosed to
  - Retention Policy
  - Deletion Policy

- **DFDs**

- **Compare design options** (identifiability, linkability, observability)
<table>
<thead>
<tr>
<th>ACTOR:</th>
<th>PI-In</th>
<th>Actor Source</th>
<th>Requirements</th>
<th>PMRM SVCs</th>
<th>[Context Narrative]</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>ECS</td>
<td>Incoming Data Flows</td>
<td>[Examples – Qualify with Context]</td>
<td>• ECS Privacy and Security Policy • jurisdictional regulations • OnStar</td>
<td>• Security • Control • Audit • Interaction • Validation • Usage</td>
<td>Incident involving Californians with all health info within the City of Sacramento</td>
<td>Data elements require further definition</td>
</tr>
<tr>
<td>Incident Report</td>
<td>External sources</td>
<td></td>
<td>• ECS Privacy and Security Policy • jurisdictional regulations • OnStar • OnStar</td>
<td>• Security • Control • Audit • Interaction • Validation • Usage</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Situational Awareness Report</td>
<td>External Sources</td>
<td></td>
<td>• ECS Privacy and Security Policy • jurisdictional regulations • OnStar • OnStar</td>
<td>• Security • Control • Audit • Interaction • Validation • Usage</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Patient EHR Information</td>
<td>Service Provider and other Healthcare systems</td>
<td></td>
<td>• HIPAA security and privacy rules • HITECH • 3rd party inherited policy agreements</td>
<td>• Security • Control • Audit • Interaction • Validation • Certification • Usage</td>
<td></td>
<td>If Individual access or enforcement are necessary to the ECS, then Access and enforcement services required</td>
</tr>
<tr>
<td>Situation Assessment</td>
<td>On-site Care/Incident Commander</td>
<td></td>
<td>• General scene information</td>
<td>• None</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
OASIS PMRM & PbD-SE Methodology Step: Describe the business processes and data flows using a data lifecycle description model and provide the level of detail needed to include all actors and touch points.
Visualizing Privacy Services in a UML Sequence Diagram
**System**

**SuperContainer**

**Security**

**SSL** – All communication over secure communication connection

**Pseudonymization**

**PII Replacement** – Replace PII with codes in program’s input data

**Notice and Agreement**

**Privacy Notice** – on storage and usage of obtained data

**Agreement** – Obtain agreement on storage and use of obtained data

**Anonymization**

**Default:** k-anonymity

**L-diversity**
User-provided personal data (each platform and merchant may get different data attributes) in a single service

User profiles sent to advertiser networks, aggregators, and to merchants

Ads, offers, deals etc.

Personal data flows between platforms.

© Dawn N. Jutla
Vision without Execution is Hallucination

Examples of such documentation exist across industries but not CONSISTENTLY

Roles of Education and Adoption

*Institutionalize* Privacy Engineering within Software Engineering in Community College and University Programs ... in Computer Science, Engineering, Business, and the Arts

Create tools to make it EASIER for software engineers to comply to OASIS Emerging Privacy Standards without losing productivity
POSSIBLE FUTURE TOOLS IN SOFTWARE ENGINEERING
EDUCATION/OASIS PbD-SE ADOPTION
STATUS CHECK ON THE PRIVACY FIELD

Status: IMMATURE
Progress: TOO SLOW
Funding: UNDERFUNDED
Priority: COMPETING INTERESTS – (all stakeholders)
Risk: CITIZENS LOSE ALL PRIVACY
Impact: IMMEASURABLE in terms of the freedoms of future generations

A lot more time-consuming work to do ...
Our changing societies with wearables, wireless, augmented reality, big data, and IoT machines communicating (M2M).