Privacy Management Reference Model and Methodology (PMRM) Version 1.0

Working Draft 05 – Edits to CSPRD01 of 12 April 2012

31 October 2012

Technical Committee:

OASIS Privacy Management Reference Model (PMRM) TC

Chairs:

John Sabo (john.annapolis@verizon.net), Individual
Michael Willett (mwillett@nc.rr.com), Individual

Editors:

John Sabo (john.annapolis@verizon.net), Individual
Michael Willett (mwillett@nc.rr.com), Individual
Peter F Brown (peter@peterfbrown.com), Individual
Dawn N Jutla (dawn.jutla@smu.ca), Saint Mary's University

Abstract:

The Privacy Management Reference Model and Methodology (PMRM, pronounced "pim-rim") provides a model and a methodology for:

- understanding and analyzing privacy policies and their privacy management requirements in defined use cases; and
- selecting the technical services which must be implemented to support privacy controls.

It is particularly relevant for use cases in which personal information (PI) flows across regulatory, policy, jurisdictional, and system boundaries.

Status:

This Working Draft (WD) has been produced by one or more TC Members; it has not yet been voted on by the TC or approved as a Committee Draft (Committee Specification Draft or a Committee Note Draft). The OASIS document Approval Process begins officially with a TC vote to approve a WD as a Committee Draft. A TC may approve a Working Draft, revise it, and re-approve it any number of times as a Committee Draft.

Table of Contents

1 Introduction

The Privacy Management Reference Model and Methodology (PMRM) addresses the reality of today's networked, interoperable capabilities, applications and devices and the complexity of managing personal information (PI)[1] across legal, regulatory and policy environments in interconnected domains. It is a valuable tool that helps improve privacy management and compliance in cloud computing, health IT, smart grid, social networking, federated identity and similarly complex environments where the use of personal information is governed by laws, regulations, business contracts and operational policies, but where traditional enterprise-focused models are inadequate. It can be of value to business and program managers who need to understand the implications of privacy policies for specific business systems and to help assess privacy management risks.

The PMRM is neither a static model nor a purely prescriptive set of rules (although it includes characteristics of both), and implementers have flexibility in determining the level and granularity of analysis required by a particular use case. The PMRM can be used by systems architects to inform the development of a privacy management architecture. The PMRM may also be useful in fostering interoperable policies and policy management standards and solutions. In many ways, the PMRM enables "privacy by design" because of its analytic structure and primarily operational focus.

1.1 Context

Predictable and trusted privacy management must function within a complex, inter-connected set of networks, systems, applications, devices, data, and associated governing policies. Such a privacy management capability is needed both in traditional computing and in cloud computing capability delivery environments. A useful privacy management capability must be able to establish the relationship between personal information ("PI") and associated privacy policies in sufficient granularity to enable the assignment of privacy management functionality and compliance controls throughout the lifecycle of the PI. It must also accommodate a changing mix of PI and policies, whether inherited or communicated to and from external domains or imposed internally. It must also include a methodology to carry out a detailed, structured analysis of the application environment and create a custom privacy management analysis (PMA) for the particular use case.

1.2 Objectives

The PMRM is used to analyze complex use cases, to understand and implement appropriate operational privacy management functionality and supporting mechanisms, and to achieve compliance across policy, system, and ownership boundaries. It may also be useful as a tool to inform policy development.

Unless otherwise indicated specifically or by context, the use of the term 'policy' or 'policies' in this document may be understood as referencing laws, regulations, contractual terms and conditions, or operational policies associated with the collection, use, transmission, storage or destruction of personal information or personally identifiable information.

While serving as an analytic tool, the PMRM can also aid the design of a privacy management architecture in response to use cases and as appropriate for a particular operational environment. It can also be used to help in the selection of integrated mechanisms capable of executing privacy controls in line with privacy policies, with predictability and assurance. Such an architectural view is important, because business and policy drivers are now both more global and more complex and must thus interact with many loosely-coupled systems.

[1] There is a distinction between 'personal information' (PI) and 'personally identifiable information' (PII) – see Glossary. However, for clarity, the term 'PI' is generally used in this document and is assumed to cover both. Specific contexts do, however, require that the distinction be made explicit.

In addition, multiple jurisdictions, inconsistent and often-conflicting laws, regulations, business practices, and consumer preferences, together create huge barriers to online privacy management and compliance. It is unlikely that these barriers will diminish in any significant way, especially in the face of rapid technological change and innovation and differing social and national values, norms and policy interests.

It is important to note that agreements may not be enforceable in certain jurisdictions. And a dispute over jurisdiction may have significant bearing over what rights and duties the Participants have regarding use and protection of PI. Even the definition of PI will vary. The PMRM attempts to address these issues. Because data can so easily migrate across jurisdictional boundaries, rights cannot be protected without explicit specification of what boundaries apply.

The Privacy Management Reference Model and Methodology therefore provides policymakers, program and business managers, system architects and developers with a tool to improve privacy management and compliance in multiple jurisdictional contexts while also supporting capability delivery and business objectives. In this Model, the controls associated with privacy (including security) will be flexible, configurable and scalable and make use of technical mechanisms, business process and policy components. These characteristics require a specification that is policy-configurable, since there is no uniform, internationally-adopted privacy terminology and taxonomy.

Analysis and documentation produced using the PMRM will result in a Privacy Management Analysis (PMA) that serves multiple Stakeholders, including privacy officers and managers, general compliance managers, and system developers. While other privacy instruments, such as privacy impact assessments (“PIAs”), also serve multiple Stakeholders, the PMRM does so in a way that is somewhat different from these others. Such instruments, while nominally of interest to multiple Stakeholders, tend to serve particular groups. For example, PIAs are often of most direct concern to privacy officers and managers, even though developers are often tasked with contributing to them. Such privacy instruments also tend to change hands on a regular basis. As an example, a PIA may start out in the hands of the development or project team, move to the privacy or general compliance function for review and comment, go back to the project for revision, move back to the privacy function for review, and so on. This iterative process of successive handoffs is valuable, but can easily devolve into a challenge and response dynamic that can itself lead to miscommunication and misunderstandings.

The output from using the PMRM, in contrast, should have direct and ongoing relevance for all Stakeholders and is less likely to suffer the above dynamic. This is because it should be considered as a “boundary object,” a construct that supports productive interaction and collaboration among multiple communities. Although a boundary object is fully and continuously a part of each relevant community, each community draws from it meanings that are grounded in the group’s own needs and perspectives. As long as these meanings are not inconsistent across communities, a boundary object acts as a shared yet heterogeneous understanding. The PMRM process output, if properly generated, constitutes just such a boundary object. It is accessible and relevant to all Stakeholders, but each group takes from it and attributes to it what they specifically need. As such, the PMRM can facilitate collaboration across relevant communities in a way that other privacy instruments often cannot.

1.3 Target Audiences

The intended audiences of this document and expected benefits to be realized include:

- **Privacy and Risk Officers** will gain a better understanding of the specific privacy management environment for which they have compliance responsibilities as well as detailed policy and operational processes and technical systems that are needed to achieve their organization’s privacy compliance;
- **Systems/Business Architects** will have a series of templates for the rapid development of core systems functionality, developed using the PMRM as a tool.
- **Software and Service Developers** will be able to identify what processes and methods are required to ensure that personal data is created and managed in accordance with requisite privacy provisions.
- **Public policy makers and business owners** will be able to identify any weaknesses or shortcomings of current policies and use the PMRM to establish best practice guidelines where needed.

1.4 Specification Summary

The PMRM consists of:

- A conceptual model of privacy management, including definitions of terms;
- A methodology; and
- A set of operational services,

together with the inter-relationships among these three elements.

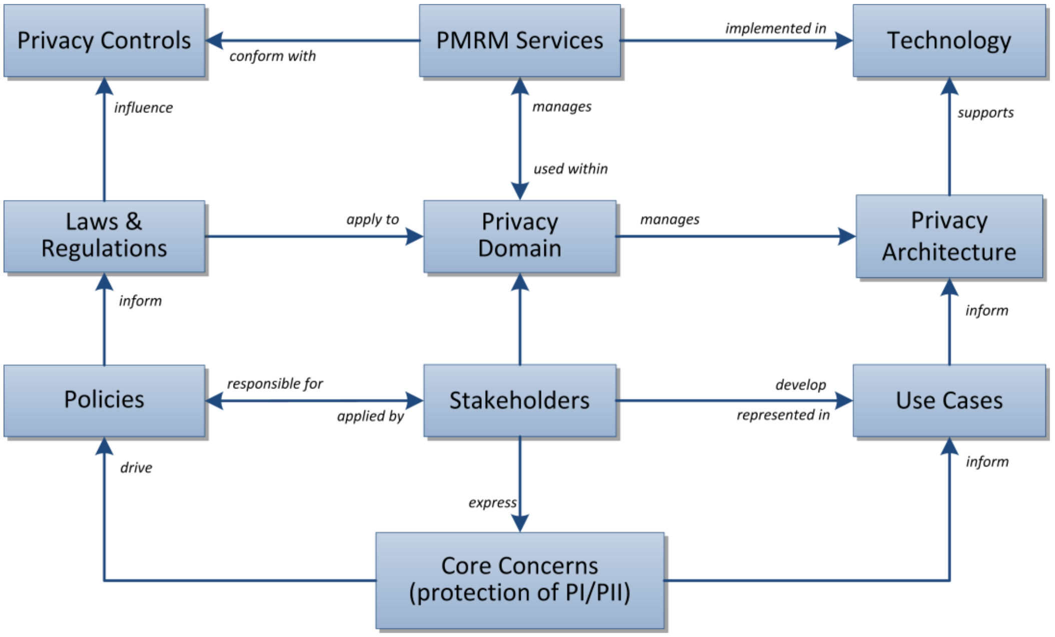

Figure 1 – The PMRM Conceptual Model

In Figure 1, we see that the core concern of privacy protection, is expressed by Stakeholders (including data subjects, policy makers, solution providers, etc.) who help, on the one hand, drive policies (which both reflect and influence actual regulation and lawmaking); and on the other hand, inform the use cases that are developed to address the specific architecture and solutions required by the Stakeholders in a particular domain.

Legislation in its turn is a major influence on privacy controls – indeed, privacy controls are often expressed as policy objectives rather than as specific technology solutions – and these form the basis of the PMRM Services that are created to conform to those controls when implemented.

The PMRM conceptual model is anchored in the principles of Service-Oriented Architecture (and particularly the principle of services operating across ownership boundaries). Given the general reliance by the privacy policy community on non-uniform definitions of so-called “Fair Information Practices/Principles” (FIP/Ps), a non-normative, working set of *operational* privacy definitions (see section 8.1) is used to provide a foundation for the Model. With their operational focus, these working definitions are not intended to supplant or to in any way suggest a bias for or against any specific policy or policy set. However, they may prove valuable as a tool to help deal with the inherent biases built into current terminology associated with privacy and to abstract their operational features.

The PMRM methodology covers a series of tasks, outlined in the following sections of the document, concerned with:

- defining and describing use-cases;
- identifying particular business domains and understanding the roles played by all Participants and systems within that domain in relation to privacy issues;
- identifying the data flows and touch-points for all personal information within a privacy domain;
- specifying various privacy controls;
- mapping technical and process mechanisms to operational services;

- performing risk and compliance assessments.

The specification also defines a set of Services deemed necessary to implement the management and compliance of detailed privacy requirements within a particular use case. The Services are sets of functions which form an organizing foundation to facilitate the application of the model and to support the identification of the specific mechanisms which will be incorporated in the privacy management architecture appropriate for that use case. The set of operational services (Agreement, Usage, Validation Certification, Enforcement, Security, Interaction, and Access) is described in Section 4 below.

The core of the specification is expressed in two normative sections: the High Level Privacy Analysis and the Detailed Privacy Management Reference Model Description. The Detailed PMRM Description section is informed by the general findings associated with the High Level Analysis. However, it is much more detail-focused and requires development of a use case which clearly expresses the complete application and/or business environment within which personal information is collected, communicated, processed, stored, and disposed.

It is also important to point out that the model is not generally prescriptive and that users of the PMRM may choose to adopt some parts of the model and not others. However, a complete use of the model will contribute to a more comprehensive privacy management architecture for a given capability or application. As such, the PMRM may serve as the basis for the development of privacy-focused capability maturity models and improved compliance frameworks. The PMRM provides a model foundation on which to build privacy architectures.

Use of the PMRM by and within a particular business domain and context (with a suitable Use Case), will lead to the production of a Privacy Management Analysis (PMA). An organization may have one or more PMAs, particularly across different business units, or it may have a unified PMA. Theoretically, a PMA may apply across organizations, states, and even countries or other geo-political regions.

Figure 2 below shows the high-level view of the PMRM methodology that is used to create a PMA. Although the stages are numbered for clarity, no step is an absolute pre-requisite for starting work on another step and the overall process will usually be iterative. Equally, the process of establishing an appropriate privacy architecture, and determining when and how technology implementation will be carried out, can both be started at any stage during the overall process.

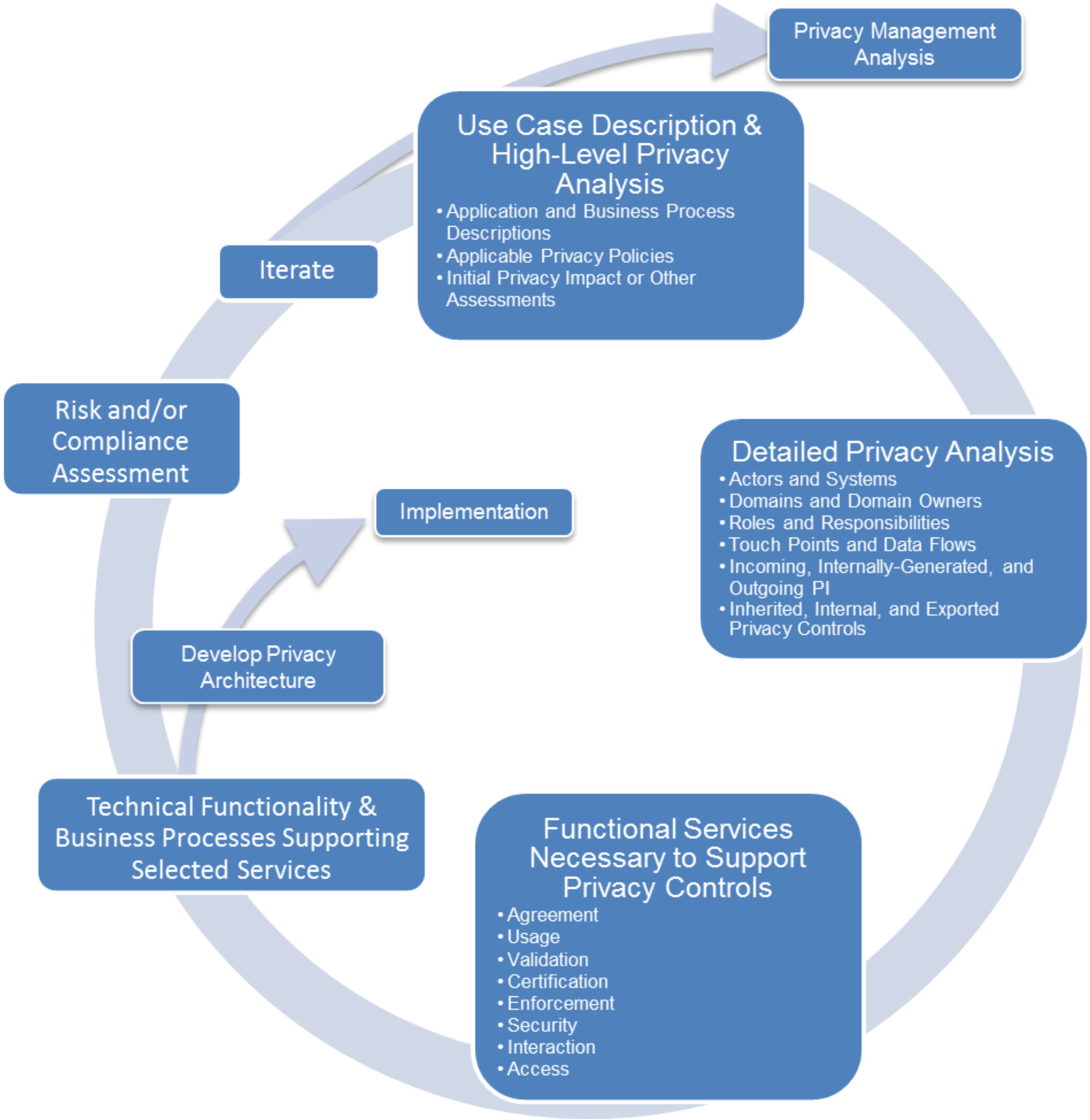
Privacy Management Analysis
Use Case Description & High-Level Privacy Analysis
•Application and Business Process Descriptions
•Applicable Privacy Policies
•Initial Privacy Impact or Other Assessments
Iterate
Risk and/or Compliance Assessment
Implementation
Detailed Privacy Analysis
•Actors and Systems
•Domains and Domain Owners
•Roles and Responsibilities
•Touch Points and Data Flows
•Incoming, Internally-Generated, and Outgoing PI
•Inherited, Internal, and Exported Privacy Controls
Develop Privacy Architecture
Technical Functionality & Business Processes Supporting Selected Services
Functional Services Necessary to Support Privacy Controls
•Agreement
•Usage
•Validation
•Certification
•Enforcement
•Security
•Interaction
•Access

Figure 2 - The PMRM Methodology

1.5 Terminology

References are surrounded with [square brackets] and are in **bold** text.

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in **[RFC2119]**.

A glossary of key terms used in this specification as well as operational definitions for sample Fair Information Practices/Principles (“FIP/Ps”) are included in Section 8 of the document. We note that words and terms used in the discipline of data privacy in many cases have meanings and inferences associated with specific laws, regulatory language, and common usage within privacy communities. The use of such well-established terms in this specification is unavoidable. However we urge readers to consult the definitions in the glossary and clarifications in the text to reduce confusion about the use of such terms within this specification.

1.6 Normative References

[RFC2119] S. Bradner, *Key words for use in RFCs to Indicate Requirement Levels*, http://www.ietf.org/rfc/rfc2119.txt, IETF RFC 2119, March 1997.

1.7 Non-Normative References

[SOA-RM] OASIS Standard, "Reference Model for Service Oriented Architecture 1.0", 12 October 2006. http://docs.oasis-open.org/soa-rm/v1.0/soa-rm.pdf

[SOA-RAF] OASIS Specification, "SOA Reference Architecture Foundation 1.0" {Pending Designated Cross-Reference}

[NIST 800-53] "Security and Privacy Controls for Federal Information Systems and Organizations – Appendix J: Privacy Controls Catalog", NIST Special Publication 800-53 Draft Appendix J, July 2011.

2 Develop Use Case Description and High-Level Privacy Analysis

The first phase in applying the PMRM methodology requires the scoping of the application or business service in which personal information (PI) is associated - in effect, identifying the complete environment in which the application or capabilities where privacy and data protection requirements are applicable. The extent of the scoping analysis and the definitions of “application” or “business capability” are set by the Stakeholders using the PMRM within a particular domain. These may be defined broadly or narrowly, and may include lifecycle (time) elements.

The high level analysis may also make use of privacy impact assessments, previous risk assessments, privacy maturity assessments, compliance reviews, and accountability model assessments as determined by domain Stakeholders. However, the scope of the high level privacy analysis (including all aspects of the capability or application under review and all relevant privacy policies) must correspond with the scope of the second phase, covered in Section 3, “Detailed Privacy Use Case Analysis”, below.

2.1 Application and Business Process Descriptions

Task #1: Use Case Description

Objective Provide a general description of the Use Case.

Example

A California utility, with a residential customer base with smart meters installed, wants to promote the increased use of electric vehicles in its service area by offering significantly reduced electricity rates for nighttime recharging of vehicle battery. The system also permits the customer to use the charging station at another customer’s site [such as at a friend’s house] and have the system bill the vehicle owner instead of the customer whose charging station is used.

This Use Case involves utility customers who have registered with the utility to enable EV charging (EV customer). An EV customer plugs in the car at her residence and requests “charge at cheapest rates”. The utility is notified of the car’s presence, its ID number and the approximate charge required (provided by the car’s on board computer). The utility schedules the recharge to take place during the evening hours and at times determined by the utility (thus putting diversity into the load).

The billing department calculates the amount of money to charge the EV customer based on EV rates and for the measured time period.

The same EV customer drives to a friend’s home (also a registered EV customer) and requests a quick charge to make sure that she can get back home. When she plugs her EV into her friend’s EV charger, the utility identifies the fact that the EV is linked to a different customer account than that of the site resident, and places the charging bill on the correct customer’s invoice.

The billing department now calculates the amount of money to invoice the customer who owns the EV, based on EV rates and for the measured time period.

The utility has a privacy policy that incudes selectable options for customers relating to the use of PI and PII associated with location and billing information, and has implemented systems to enforce those policies.

Task #2: Use Case Inventory

Objective Provide an inventory of the capabilities, applications and policy environment under review at the level of granularity appropriate for the analysis covered by the PMRM and define a High Level Use Case which will guide subsequent analysis. In order to facilitate the analysis described in the Detailed Privacy Use Case Analysis in Section 4, the components of the Use Case Inventory should align as closely as possible with the components that will be analyzed in the corresponding detailed use case analysis.

Context The inventory can include applications and business processes; products; policy environment; legal and regulatory jurisdictions; systems supporting the capabilities and applications; data; time; and other factors Impacting the collection, communication, processing, storage and disposition of PI. The inventory should also include the types of data subjects covered by the use case together with specific privacy options (such as policy preferences, privacy settings, etc. if these are formally expressed) for each type of data subject.

Example

Systems: Utility Communications Network, Customer Billing System, EV On Board System…

Legal and Regulatory Jurisdictions:

California Constitution, Article 1, section 1 gives each citizen an "inalienable right" to pursue and obtain "privacy."

Office of Privacy Protection - California Government Code section 11549.5.

Automobile "Black Boxes" - Vehicle Code section 9951.

…

Personal Information Collected on Internet:

Government Code section 11015.5. This law applies to state government agencies…

The California Public Utilities Commission, which “serves the public interest by protecting consumers and ensuring the provision of safe, reliable utility service and infrastructure at reasonable rates, with a commitment to environmental enhancement and a healthy California economy”…

Policy: The Utility has a published Privacy Policy covering the EV recharging/billing application

Customer: The Customer’s selected settings for policy options presented via customer-facing interfaces.

2.2 Applicable Privacy Policies

Task #3: Privacy Policy Conformance Criteria

Objective Define and describe the criteria for conformance of a system or business process (identified in the use case and inventory) with an applicable privacy policy. As with the Use Case Inventory described in Task #2 above, the conformance criteria should align with the equivalent elements in the Detailed Privacy Use Case Analysis described in Section 3. Wherever possible, they should be grouped by the relevant FIP/Ps and expressed as privacy constraints.

Note that whereas Task #2 itemizes the environmental elements relevant to the Use Case, Task #3 focuses on the privacy requirements specifically.

Example

Privacy Policy Conformance Criteria:

(1) Ensure that the utility does not share data with third parties without the consumer's consent…etc.

(2) Ensure that the utility supports strong levels of:

(a) Identity authentication

(b) Security of transmission between the charging stations and the utility information systems…etc.

(3) Ensure that personal data is deleted on expiration of retention periods…

…

2.3 Initial Privacy Impact (or other) Assessment(s) [optional]

Task #4: Assessment Preparation

Objective Prepare an initial privacy impact assessment, or as appropriate, a risk assessment, privacy maturity assessment, compliance review, or accountability model assessment applicable within the scope of analysis carried out in sections 2.1 and 2.2 above. Such an assessment can be deferred until a later iteration step (see Section 4.3) or inherited from a previous exercise.

Example

Since the Electric Vehicle (EV) has a unique ID, it can be linked to a specific customer. As such, customer's whereabouts may be tracked through utility transaction visibility…

The EV charging and vehicle management system may retain data, which can be used to identify patterns of charging and location information that can constitute PI.

Unless safeguards are in place and (where appropriate) under the customer control, there is a danger that intentionally anonymized PI nonetheless become PII…

The utility wishes to capture behavioral and movement patterns and sell this information to potential advertisers or other information brokers to generate additional revenue. This information constitutes PII. The collection and use of this information should only be done with the explicit, informed consent of the customer.

3 Develop Detailed Privacy Analysis

Goal Prepare and document a detailed Privacy Management Analysis of the Use Case which corresponds with the High Level Privacy Analysis and the High Level Use Case Description.

Constraint The Detailed Use Case must be clearly bounded and must include the following components.

3.1 Identify Participants and Systems, Domains and Domain Owners, Roles and Responsibilities, Touch Points and Data Flows

Task #5: **Identify Participants**

Objective Identify Participants having operational privacy responsibilities.

Definition A “Participant” is any Stakeholder creating, managing, interacting with, or otherwise subject to, PI managed by a System within a Privacy Domain.

Example

Participants Located at the Customer Site:

Registered Customer

Participants Located at the EV’s Location:

Registered Customer Host (Temporary host for EV charging), Registered Customer Guest

Participants Located within the Utility’s domain:

Service Provider (Utility)

Contractors and Suppliers to the Utility

Task #6: **Identify Systems**

Objective Identify the Systems where PI is collected, communicated, processed, stored or disposed within a Privacy Domain.

Definition For purposes of this specification, a System is a collection of components organized to accomplish a specific function or set of functions having a relationship to operational privacy management.

Example

System Located at the Customer Site(s):

Customer Communication Portal

EV Physical Re-Charging and Metering System

System Located in the EV(s):

EV: Device

EV On-Board System: System

System Located within the EV manufacturer's domain:

EV Charging Data Storage and Analysis System

System Located within the Utility's domain:

EV Program Information System (includes Rates, Customer Charge Orders, Customers enrolled in the program, Usage Info etc.)

EV Load Scheduler System

Utility Billing System

Remote Charge Monitoring System

Partner marketing system for transferring usage pattern and location information

Task #7: Identify Privacy Domains and Owners

Objective Identify the Privacy Domains included in the use case together with the respective Domain Owners.

Definition A "Domain" covers 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.

A "Domain Owner" is the Participant responsible for ensuring that privacy controls and PMRM services are managed in business processes and technical systems within a given Domain.

Context Privacy Domains may be under the control of data subjects or Participants with a specific responsibility within a Privacy Domain, such as data controllers; capability providers; data processors; and other distinct entities having defined operational privacy management responsibilities.

Rationale Domain Owner identification is important for purposes of establishing accountability.

Example

Utility Domain:

The physical premises located at…. which includes the Utility’s program information system, load scheduling system, billing system, and remote monitoring system

This physical location is part of a larger logical privacy domain, owned by the Utility and extends to the Customer Portal Communication system at the Customer’s site, and the EV On-Board software application System installed in the EV by the Utility, together with cloud-based services hosted by….

Customer Domain:

The physical extent of the customer’s home and adjacent land as well as the EV, wherever located, together with the logical area covered by devices under the ownership and control of the customer (such as mobile devices).

Example

The EV On-Board System belongs to the utility Privacy Domain Owner.

The EV (with its ID Number) belongs to the Customer Domain Owner and the Vehicle Manufacturer Domain Owners, but the EV ID may be accessed by the Utility.

Task #8: Identify Roles and Responsibilities within a Domain

Objective For any given use case, identify the roles and responsibilities assigned to specific Participants and Systems within a specific privacy domain

Rationale Any Participant may carry multiple roles and responsibilities and these need to be distinguishable, particularly as many functions involved in processing of PI are assigned to functional roles, with explicit authority to act, rather to specific participant.

Example

Role: EV Manufacturer Privacy Officer

Responsibilities: Ensure that all PI data flows from EV On-Board System conform with contractual obligations associated with the Utility and vehicle owner as well as the Collection Limitation and Information Minimization FIP/P. in its privacy policies.

Task #9: Identify Touch Points

Objective Identify the touch points at which the data flows intersect with Privacy Domains or Systems within Privacy Domains.

Definition Touch Points are the intersections of data flows with Privacy Domains or Systems within Privacy Domains.

Rationale The main purpose for identifying touch points in the use case is to clarify the data flows and ensure a complete picture of all Privacy Domains and Systems in which PI is used.

Example

The Customer Communication Portal provides an interface through which the Customer communicates a charge order to the Utility. This interface is a touch point.

When the customer plugs into the charging station, the EV On-Board System embeds communication functionality to send EV ID and EV Charge Requirements to the Customer Communication Portal. This functionality provides a further touch point.

Task #10: Identify Data Flows

Objective Identify the data flows carrying PI and privacy constraints among Domains in the Use Case.

Constraint Data flows may be multidirectional or unidirectional.

Example

When a charging request event occurs, the Customer Communication Portal sends Customer information, EV identification, and Customer Communication Portal location information to the EV Program Information System managed by the Utility.

This application uses metadata tags to indicate whether or not customer' identification and location data may be shared with authorized third parties, and to prohibit the sharing of data that provides customers' movement history, if derived from an aggregation of transactions.

3.2 Identify PI in Use Case Privacy Domains and Systems

Objective Specify the PI collected, created, communicated, processed or stored within Privacy Domains or Systems in three categories.

Task #11: Identify Incoming PI

Definition Incoming PI is PI flowing into a Privacy Domain, or a system within a Privacy Domain.

Constraint Incoming PI may be defined at whatever level of granularity appropriate for the scope of analysis of the Use Case and the Privacy Policies established in Section 2.

Task #12: Identify Internally Generated PI

Definition Internally Generated PI is PI created within the Privacy Domain or System itself.

Constraint Internally Generated PI may be defined at whatever level of granularity appropriate for the scope of analysis of the Use Case and the Privacy Policies established in Section 2.

Example Examples include device information, time-stamps, location information, and other system-generated data that may be linked to an identity.

Task #13: Identify Outgoing PI

Definition Outgoing PI is PI flowing out of one system to another system within a Privacy Doman or to another Privacy Domain.

Constraint Outgoing PI may be defined at whatever level of granularity appropriate for the scope of analysis of the Use Case and the Privacy Policies established in Section 2.

Example

Incoming PI:

Customer ID received by Customer Communications Portal

Internally Generated PI:

Current EV location associated with customer information, and time/location information logged by EV On-Board system

Outgoing PI:

Current EV ID and location information transmitted to Utility Load Scheduler System

3.3 Specify Required Privacy Controls Associated with PI

Goal For Incoming, Internally Generated and Outgoing PI, specify the privacy controls required to enforce the privacy policy associated with the PI. Privacy controls may be pre-defined or may be derived. In either case, privacy controls are typically associated with specific Fair Information Practices Principles (FIP/Ps) that apply to the PI.

Definition Control is a process designed to provide reasonable assurance regarding the achievement of stated objectives.

Definition Privacy Controls are administrative, technical and physical safeguards employed within an organization or Privacy Domain in order to protect PI. They are the means by which privacy policies are satisfied in an operational setting.

Task #14: Specify Inherited Privacy Controls

Objective Specify the required Privacy Controls which are inherited from Privacy Domains or Systems within Privacy Domains.

Example:

The utility inherits a Privacy Control associated with the Electric Vehicle's ID (EVID) from the vehicle manufacturer's privacy policies.

The utility inherits the consumer's Operational Privacy Control Requirements, expressed as privacy preferences, via a link with the customer communications portal when she plugs her EV into friend Rick's charging station.

The utility must apply Jane's privacy preferences to the current transaction. The Utility accesses Jane's privacy preferences and learns that Jane does not want her association with Rick exported to the Utility's third party partners. Even though Rick's privacy settings differ around his PI, Jane's non-consent to the association being transmitted out of the Utility's privacy domain is sufficient to prevent commutative association. Thus if Rick were to charge his car's batteries at Jane's, the association between them would also not be shared with third parties.

Task #15: **Specify Internal Privacy Controls**

Objective Specify the Privacy Controls which are mandated by internal Privacy Domain policies.

Example

Use Limitation Internal Privacy Controls

The Utility complies with California Code SB 1476 of 2010 (Public Utilities Code §§ 8380-8381 Use Limitation).

It implements the 2011 California Public Utility Commission (CPUC) privacy rules, recognizing the CPUC's regulatory privacy jurisdiction over it and third parties with which it shares customer data.

Further, it adopts NIST 800-53 Appendix J's "Control Family" on Use Limitation – e.g. it evaluates any proposed new instances of sharing PII with third parties to assess whether they are authorized and whether additional or new public notice is required.

Task #16: **Specify Exported Privacy Controls**

Objective Specify the Privacy Controls which must be exported to other Privacy Domains or to Systems within Privacy Domains.

Example

The Utility exports Jane's privacy preferences associated with her PI to its third party partner, whose systems are capable of understanding and enforcing these preferences. One of her privacy control requirements is to not share her EVID with marketing aggregators or advertisers.

4 Identify Functional Services Necessary to Support Privacy Controls

Privacy controls are usually stated in the form of a policy declaration or requirement and not in a way that is immediately actionable or implementable. Until now, we have been concerned with the real-world, human side of privacy but we need now to turn attention to the digital world and “system-level” concerns. “Services” provide the bridge between those requirements and a privacy management implementation by providing privacy constraints on system-level actions governing the flow of PI between touch points.

4.1 Services Needed to Implement the Controls

A set of operational Services is the organizing structure which will be used to link the required Privacy Controls specified in Section 4.3 to operational mechanisms necessary to implement those requirements.

Eight Privacy Services have been identified, based on the mandate to support an arbitrary set of privacy policies, but at a *functional level*. The eight Services can be logically grouped into three categories:

- **Core Policy**: Agreement, Usage
- **Privacy Assurance**: Security, Validation, Certification, Enforcement
- **Presentation and Lifecycle**: Interaction, Access

These groupings, illustrated below, are meant to clarify the “architectural” relationship of the Services in an operational design. However, the functions provided by all Services are available for mutual interaction without restriction.

Core Policy Services	***Privacy Assurance Services***		***Presentation & Lifecycle Services***
Agreement	Validation	Certification	Interaction
Usage	Security	Enforcement	Access

A system architect or technical manager should be able to integrate these privacy Services into a functional architecture, with specific mechanisms selected to implement these functions. In fact, a key purpose of the PMRM is to stimulate design and analysis of the specific functions - both manual and automated - that are needed to implement any set of privacy policies. In that sense, the PMRM is an analytic tool.

The PMRM identifies various system capabilities that are not typically described in privacy practices and principles. For example, a policy management (or “usage and control”) function is essential to manage the PI usage constraints established by a data subject information processor or by regulation, but such a function is not explicitly named in privacy principles/practices. Likewise, interfaces (and agents) are not explicit in the privacy principles/practices, but are necessary to represent other essential operational capabilities.

Such inferred capabilities are necessary if information systems are to be made “privacy configurable and compliant.” Without them, enforcing privacy policies in a distributed, fully automated environment will not be possible, and businesses, data subjects, and regulators will be burdened with inefficient and error-prone manual processing, inadequate privacy governance and compliance controls, and inadequate compliance reporting.

As used here,

- A “Service” is defined as a collection of related functions and mechanisms that operate for a specified purpose;
- An “Actor” is defined as a system-level, digital ‘proxy’ for either a (human) Participant or an (non-human) system-level process or other agent.

The eight privacy Services defined are **Agreement, Usage, Security, Validation, Certification, Enforcement, Interaction,** and **Access.** Specific operational behavior of these Services is governed by the privacy policy and constraints that are configured in a particular implementation and jurisdictional context. These will be identified as part of the Use Case analysis. Practice with use cases has shown that the Services listed above can, together, operationally encompass any arbitrary set of privacy requirements.

The functions of one Service may invoke another Service. In other words, functions under one Service may “call” those under another Service (for example, pass information to a new function for subsequent action). In line with principles of Service-Oriented Architecture (SOA)[2], the Services can thus interact in an arbitrary interconnected sequence to accomplish a privacy management task or set of privacy lifecycle requirements. Use cases will illustrate such interactions and their sequencing as the PMRM is used to solve a particular privacy problem. By examining and by solving multiple use cases, the PMRM can be tested for applicability and robustness.

The table below provides a description of each Service’s functionality and an informal definition of each Service:

SERVICE	FUNCTIONALITY	PURPOSE
AGREEMENT	Define and document permissions and rules for the handling of PI based on applicable policies, data subject 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	Manage and negotiate permissions and rules
USAGE	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	Control PI use
VALIDATION	Evaluate and ensure the information quality of PI in terms of Accuracy, Completeness, Relevance, Timeliness and other relevant qualitative factors	Check PI
CERTIFICATION	Ensure that the credentials of any Actor, Domain, System , or system component are compatible with their assigned roles in processing PI; and verify their compliance and trustworthiness against defined policies and assigned roles.	Check credentials
ENFORCEMENT	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)	Monitor and respond to audited exception conditions
SECURITY	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	Safeguard privacy information and operations
INTERACTION	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	Information presentation and communication
ACCESS	Enable data-subjects , 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	View and propose changes to stored PI

[2] See for example the **[SOA-RM]** and the **[SOA-RAF]**

4.2 Service Details and Function Descriptions

4.2.1 Core Policy Services

1. Agreement Service

- 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.

Example

As part of its standard customer service agreement, a bank requests selected customer PI, with associated permissions for use. Customer negotiates with the bank (whether via an electronic interface, by telephone or in person) to modify the permissions. Customer provides the PI to the bank, with the modified and agreed to permissions. This agreement is signed by both parties, stored in an appropriate representation and the customer is provided a copy.

2. Usage Service

- 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.

Example

A third party has acquired specific PI, consistent with agreed permissions for use. Before using the PI, the third party has implemented functionality ensuring that the usage of the PI is consistent with these permissions.

4.2.2 Privacy Assurance Services

3. Validation Service

- Evaluate and ensure the information quality of PI in terms of Accuracy, Completeness, Relevance, Timeliness and other relevant qualitative factors.

Example

PI is received from an authorized third party for a particular purpose. Specific characteristics of the PI, such as date the information was originally provided, are checked to ensure the PI meets specified use requirements.

4. Certification Service

- Ensure that the credentials of any Actor, Domain, System, or system component are compatible with their assigned roles in processing PI;
- Verify that an Actor, Domain, System, or system component supports defined policies and conforms with assigned roles.

Example

A patient enters an emergency room, presenting identifying credentials. Functionality has been implemented which enables hospital personnel to check those credentials against a patient database information exchange. Additionally, the certification service's authentication processes ensures that the information exchange is authorized to receive the request.

5. Enforcement Service

- Initiate response actions, policy execution, and recourse when audit controls and monitoring indicate that an Actor or System does not conform to defined laws, regulations, policies or the terms of a permission (agreement).

Example

A magazine's subscription service provider forwards customer PI to a third party not authorized to receive the information. A routine audit of the service provider's system reveals this unauthorized disclosure practice, alerting the appropriate responsible official (the organization's privacy officer), who takes appropriate action.

6. Security Service

- Make possible the trustworthy processing, communication, storage and disposition of privacy operations;
- Provide the procedural and technical mechanisms necessary to ensure the confidentiality, integrity, and availability of personal information.

Example

PI is transferred between authorized recipients, using transmission encryption, to ensure confidentiality.

Strong standards-based, identity, authentication and authorization management systems are implemented to conform to data security policies.

4.2.3 Presentation and Lifecycle Services

7. Interaction Service

- 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.

Example:

Your home banking application uses a graphical user interface (GUI) to communicate with you, including presenting any relevant privacy notices, enabling access to PI disclosures, and providing customer with options to modify privacy preferences.

The banking application utilizes email alerts to notify customers when policies have changed and uses postal mail to confirm customer-requested changes.

8. Access Service

- Enable data-subjects, as required and/or allowed by permission, policy, or regulation, to review their PI held within a Domain and propose changes and/or corrections to it.

Example:

A national credit bureau has implemented an online service enabling customers to request their credit score details and to report discrepancies in their credit histories.

4.3 Identify Services satisfying the privacy controls

The Services defined in Section 4.1 encompass detailed Functions and Mechanisms needed to transform the privacy controls of section 3.3 into an operational system design for the use case. Since the detailed use case analysis focused on the data flows – incoming, internally generated, outgoing – between Systems (and Actors), the Service selections should be on the same granular basis.

Task #17: Identify the Services necessary to support operation of identified privacy controls.

Perform this task for each data flow exchange of PI between systems.

This detailed conversion into Service operations can then be synthesized into consolidated sets of Service actions per System involved in the Use Case.

On further iteration and refinement, the engaged Services can be further delineated by the appropriate Functions and Mechanisms for the relevant privacy controls.

Examples:

Based upon

a) Internally Generated PI (Current EV location logged by EV On-Board system), and
b) Outgoing PI (Current EV location transmitted to Utility Load Scheduler System),
convert to operational Services as follows:

“Log EV location”:

Validation EV On-Board System checks that the reporting of a particular charging location has been opted-in by EV owner

Enforcement If location has not been authorized by EV Owner for reporting and the location data has been transmitted, then notify the Owner and/or the Utility

Interaction Communicate EV Location to EV On-Board System

Usage EV On-Board System records EV Location in secure storage; EV location data is linked to agreements

“Transmit EV Location to Utility Load Scheduler System (ULSS)”:

Interaction Communication established between EV Location and ULSS

Security Authenticate the ULSS site; secure the transmission

Certification ULSS checks the credentials of the EV On-Board System

Validation Validate the EV Location against accepted locations

Usage ULSS records the EV Location, together with agreements

5 Define the Technical Functionality and Business Processes Supporting the Selected Services

Each Service is composed of a set of operational Functions, reflected in defined business processes and technical solutions.

The **Functions** step is critical because it necessitates either designating the particular business process or technical mechanism being implemented to support the Services required in the use case or the absence of such a business process or technical mechanism.

5.1 Identify Functions Satisfying the Selected Services

Up to this point in the PMRM methodology, the primary focus of the use case analysis has been on the “what” - PI, policies, control requirements, the Services needed to manage privacy. Here the PMRM requires a statement of the “how” – what business processes and technical mechanisms are identified as providing expected functionality.

Task #18: **Identify the Functions that satisfy the selected Services**

Examples

“Log EV Location” (uses services **Validation**, **Enforcement**, **Interaction**, and **Usage** Services**):**

Function: Encrypt the EV Location and Agreements and store in on-board solid-state drive

“Transmit EV Location to Utility Load Scheduler System (ULSS)” (uses **Interaction**, **Security**, **Certification**, **Validation**, and **Usage** Services):

Function: Establish a TLS/SSL communication between EV Location and ULSS, which includes mechanisms for authentication of the source/destination

6 Perform Risk and/or Compliance Assessment

Task #19: Conduct Risk Assessment

Objective Once the requirements in the Use Case have been converted into operational Services, an overall risk assessment should be performed from that operational perspective

Constraint Additional controls may be necessary to mitigate risks within Services. The level of granularity is determined by the Use Case scope. Provide operational risk assessments for the selected Services within the use case.

Examples

“Log EV location”:

Validation EV On-Board System checks that location is not previously rejected by EV owner
Risk: On-board System has been corrupted

Enforcement If location is previously rejected, then notify the Owner and/or the Utility
Risk: On-board System not current

Interaction Communicate EV Location to EV On-Board System
Risk: Communication link not available

Usage EV On-Board System records EV Location in secure storage, together with agreements
Risk: Security controls for On-Board System are compromised

“Transmit EV Location to Utility Load Scheduler System (ULSS)”:

Interaction Communication established between EV Location and ULSS
Risk: Communication link down

Security Authenticate the ULSS site; secure the transmission
Risk: ULSS site credentials are not current

Certification ULSS checks the credentials of the EV On-Board System
Risk: EV On-Board System credentials do not check

Validation Validate the EV Location against accepted locations
Risk: Accepted locations are back-level

Usage ULSS records the EV Location, together with agreements
Risk: Security controls for the ULSS are compromised

7 Initiate Iterative Process

Goal A ‘first pass’ through the Tasks above can be used to identify the scope of the Use Case and the underlying privacy policies and constraints. Additional iterative passes would serve to refine the Use Case and to add detail. Later passes could serve to resolve “TBD” sections that are important, but were not previously developed.

Note that a ‘single pass’ analysis might mislead the PMRM user into thinking the Use Case was fully developed and understood. Iterative passes through the analysis will almost certainly reveal further details. Keep in mind that the ultimate objective is to develop insight into the Use Case sufficient to provide a reference model for an operational, Service-based, solution.

Task #20: Iterate the analysis and refine.

Iterate the analysis in the previous sections, seeking further refinement and detail.

8 Operational Definitions for Fair Information Practices/Principles ("FIPPs") and Glossary

As explained in the introduction, every specialized domain is likely to create and use a domain-specific vocabulary of concepts and terms that should be used and understood in the specific context of that domain. PMRM is no different and this section contains such terms.

In addition, a number of "operational definitions" are intended to be used in the PMRM to support development of the "Detailed Privacy Use Case Analysis" described in Section 4. Their use is completely optional, but may be helpful in organizing privacy policies and controls where there are inconsistencies in definitions across policy boundaries or where existing definitions do not adequately express the operational characteristics associated with Fair Information Practices/Principles.

8.1 Operational FIPPs

The following 14 Fair Information Practices/Principles are composite definitions derived from a comprehensive list of international legislative instruments. These operational FIPPs can serve as a sample set, as needed.

Accountability

Functionality enabling reporting by the business process and technical systems which implement privacy policies, to the data subject or Participant accountable for ensuring compliance with those policies, with optional linkages to redress and sanctions.

Notice

Functionality providing Information, in the context of a specified use, regarding policies and practices exercised within a Privacy Domain including: definition of the Personal Information collected; its use (purpose specification); its disclosure to parties within or external to the domain; practices associated with the maintenance and protection of the information; options available to the data subject regarding the processor's privacy practices; retention and deletion; changes made to policies or practices; and other information provided to the data subject at designated times and under designated circumstances.

Consent

Functionality, including support for Sensitive Information, Informed Consent, Change of Use Consent, and Consequences of Consent Denial, enabling data subjects to agree to the collection and/or specific uses of some or all of their Personal Information either through an affirmative process (opt-in) or implied (not choosing to opt-out when this option is provided).

Collection Limitation and Information Minimization

Functionality, exercised by the information processor, that limits the information collected, processed, communicated and stored to the minimum necessary to achieve a stated purpose and, when required, demonstrably collected by fair and lawful means.

Use Limitation

Functionality, exercised by the information processor, that ensures that Personal Information will not be used for purposes other than those specified and accepted by the data subject or provided by law, and not maintained longer than necessary for the stated purposes.

Disclosure

Functionality that enables the transfer, provision of access to, use for new purposes, or release in any manner, of Personal Information managed within a Privacy Domain in accordance with notice and consent permissions and/or applicable laws and functionality making known the information processor's policies to external parties receiving the information.

Access and Correction

Functionality that allows an adequately identified data subject to discover, correct or delete, Personal Information managed within a Privacy Domain; functionality providing notice of denial of access; and options for challenging denial when specified.

Security/Safeguards

Functionality that ensures the confidentiality, availability and integrity of Personal Information collected, used, communicated, maintained, and stored; and that ensures specified Personal Information will be de-identified and/or destroyed as required.

Information Quality

Functionality that ensures that information collected and used is adequate for purpose, relevant for purpose, accurate at time of use, and, where specified, kept up to date, corrected or destroyed.

Enforcement

Functionality that ensures compliance with privacy policies, agreements and legal requirements and to give data subjects a means of filing complaints of compliance violations and having them addressed, including recourse for violations of law, agreements and policies.

Openness

Functionality, available to data subjects, that allows access to an information processors policies and practices relating to the management of their Personal Information and that establishes the existence, nature, and purpose of use of Personal Information held about the data subject.

Anonymity

Functionality that prevents data being collected or used in a manner that can identify a specific natural person.

Information Flow

Functionality that enables the communication of personal information across geo-political jurisdictions by private or public entities involved in governmental, economic, social or other activities.

Sensitivity

Functionality that provides special handling, processing, security treatment or other treatment of specified information, as defined by law, regulation or policy.

8.2 Glossary

Actor

A system-level, digital ‘proxy’ for either a (human) Participant (or their delegate) interacting with a system or a (non-human) in-system process or other agent.

Audit Controls

Processes designed to provide reasonable assurance regarding the effectiveness and efficiency of operations and compliance with applicable policies, laws, and regulations.

Boundary Object

A sociological construct that supports productive interaction and collaboration among multiple communities.

Control

A process designed to provide reasonable assurance regarding the achievement of stated objectives.

Domain Owner

A Participant having responsibility for ensuring that privacy controls and privacy constraints are implemented and managed in business processes and technical systems in accordance with policy and requirements.

Incoming PI

PI flowing into a Privacy Domain, or a system within a Privacy Domain.

Internally Generated PI

PI created within the Privacy Domain or System itself.

Monitor

To observe the operation of processes and to indicate when exception conditions occur.

Outgoing PI

PI flowing out of one system to another system within a Privacy Doman or to another Privacy Domain.

Participant

A Stakeholder creating, managing, interacting with, or otherwise subject to, PI managed by a System within a Privacy Domain.

PI

Personal Information – any data which describes some attribute of, or that is uniquely associated with, a natural person.

PII

Personally identifiable information – any (set of) data that can be used to uniquely identify a natural person.

Policy

Laws, regulations, contractual terms and conditions, or operational rules or guidance associated with the collection, use, transmission, storage or destruction of personal information or personally identifiable information

Privacy Architecture

A collection of proposed policies and practices appropriate for a given domain resulting from use of the PMRM

Privacy Constraint

An operational mechanism that controls the extent to which PII may flow between touch points.

Privacy Control

An administrative, technical or physical safeguard employed within an organization or Privacy Domain in order to protect PII.

Privacy Domain

A physical or logical area within the use case that is subject to the control of a Domain Owner(s)

Privacy Management

The collection of policies, processes and methods used to protect and manage PI.

Privacy Management Analysis

Documentation resulting from use of the PMRM and that serves multiple Stakeholders, including privacy officers and managers, general compliance managers, and system developers

Privacy Management Reference Model and Methodology (PMRM)

A model and methodology for understanding and analyzing privacy policies and their management requirements in defined use cases; and for selecting the technical services which must be implemented to support privacy controls.

(PMRM) Service

A collection of related functions and mechanisms that operate for a specified purpose.

System

A collection of components organized to accomplish a specific function or set of functions having a relationship to operational privacy management.

Touch Point

The intersection of data flows with Privacy Domains or Systems within Privacy Domains.

Appendix A. Acknowledgments

The following individuals have participated in the creation of this specification and are gratefully acknowledged:

Participants:

Peter F Brown, Individual Member
Gershon Janssen, Individual Member
Dawn Jutla, Saint Mary's University
Gail Magnuson, Individual Member
Joanne McNabb, California Office of Privacy Protection
John Sabo, Individual Member
Stuart Shapiro, MITRE Corporation
Michael Willett, Individual Member

Appendix B. Revision History

Revision	Date	Editor	Changes Made
WD05	2012-10-17	John Sabo	Incorporate agreed dispositions to issues raised during First Public Review
WD05	2012-10-19	Peter F Brown	Minor edits, terminology alignment and clean-up of formatting
WD05	2012-10-31	Peter F Brown	This document