



Privacy Management Reference Model and Methodology (PMRM) Version 1.0

Committee Specification Draft 02

13 December 2012

Specification URIs

This version:

<http://docs.oasis-open.org/pmr/PMRM/v1.0/csd02/PMRM-v1.0-csd02.pdf> (Authoritative)
<http://docs.oasis-open.org/pmr/PMRM/v1.0/csd02/PMRM-v1.0-csd02.html>
<http://docs.oasis-open.org/pmr/PMRM/v1.0/csd02/PMRM-v1.0-csd02.doc>

Previous version:

<http://docs.oasis-open.org/pmr/PMRM/v1.0/csprd01/PMRM-v1.0-csprd01.pdf> (Authoritative)
<http://docs.oasis-open.org/pmr/PMRM/v1.0/csprd01/PMRM-v1.0-csprd01.html>
<http://docs.oasis-open.org/pmr/PMRM/v1.0/csprd01/PMRM-v1.0-csprd01.doc>

Latest version:

<http://docs.oasis-open.org/pmr/PMRM/v1.0/PMRM-v1.0.pdf> (Authoritative)
<http://docs.oasis-open.org/pmr/PMRM/v1.0/PMRM-v1.0.html>
<http://docs.oasis-open.org/pmr/PMRM/v1.0/PMRM-v1.0.doc>

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 document was last revised or approved by the OASIS Privacy Management Reference Model (PMRM) TC on the above date. The level of approval is also listed above. Check the “Latest version” location noted above for possible later revisions of this document.

Technical Committee members should send comments on this specification to the Technical Committee’s email list. Others should send comments to the Technical Committee by using the

“Send A Comment” button on the Technical Committee’s web page at <http://www.oasis-open.org/committees/pmrm/>.

For information on whether any patents have been disclosed that may be essential to implementing this specification, and any offers of patent licensing terms, please refer to the Intellectual Property Rights section of the Technical Committee web page (<http://www.oasis-open.org/committees/pmrm/ipr.php>).

Citation format:

When referencing this specification the following citation format should be used:

[PMRM-v1.0]

Privacy Management Reference Model and Methodology (PMRM) Version 1.0. 13 December 2012. OASIS Committee Specification Draft 02. <http://docs.oasis-open.org/pmrm/PMRM/v1.0/csd02/PMRM-v1.0-csd02.html>.

Notices

Copyright © OASIS Open 2012. All Rights Reserved.

All capitalized terms in the following text have the meanings assigned to them in the OASIS Intellectual Property Rights Policy (the "OASIS IPR Policy"). The full [Policy](#) may be found at the OASIS website.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published, and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this section are included on all such copies and derivative works. However, this document itself may not be modified in any way, including by removing the copyright notice or references to OASIS, except as needed for the purpose of developing any document or deliverable produced by an OASIS Technical Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR Policy, must be followed) or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY OWNERSHIP RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

OASIS requests that any OASIS Party or any other party that believes it has patent claims that would necessarily be infringed by implementations of this OASIS Committee Specification or OASIS Standard, to notify OASIS TC Administrator and provide an indication of its willingness to grant patent licenses to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification.

OASIS invites any party to contact the OASIS TC Administrator if it is aware of a claim of ownership of any patent claims that would necessarily be infringed by implementations of this specification by a patent holder that is not willing to provide a license to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification. OASIS may include such claims on its website, but disclaims any obligation to do so.

OASIS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on OASIS' procedures with respect to rights in any document or deliverable produced by an OASIS Technical Committee can be found on the OASIS website. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this OASIS Committee Specification or OASIS Standard, can be obtained from the OASIS TC Administrator. OASIS makes no representation that any information or list of intellectual property rights will at any time be complete, or that any claims in such list are, in fact, Essential Claims.

The name "OASIS" is a trademark of [OASIS](#), the owner and developer of this specification, and should be used only to refer to the organization and its official outputs. OASIS welcomes reference to, and implementation and use of, specifications, while reserving the right to enforce its marks against misleading uses. Please see <http://www.oasis-open.org/policies-guidelines/trademark> for above guidance.

Table of Contents

1	Introduction.....	6
1.1	Context.....	6
1.2	Objectives	6
1.3	Target Audiences.....	7
1.4	Specification Summary	8
1.5	Terminology	10
1.6	Normative References	11
1.7	Non-Normative References	11
2	Develop Use Case Description and High-Level Privacy Analysis.....	12
2.1	Application and Business Process Descriptions.....	12
	Task #1: Use Case Description	12
	Task #2: Use Case Inventory.....	13
2.2	Applicable Privacy Policies	14
	Task #3: Privacy Policy Conformance Criteria.....	14
2.3	Initial Privacy Impact (or other) Assessment(s) [optional]	14
	Task #4: Assessment Preparation	14
3	Develop Detailed Privacy Analysis.....	16
3.1	Identify Participants and Systems, Domains and Domain Owners, Roles and Responsibilities, Touch Points and Data Flows.....	16
	Task #5: Identify Participants	16
	Task #6: Identify Systems	16
	Task #7: Identify Privacy Domains and Owners	17
	Task #8: Identify Roles and Responsibilities within a Domain.....	18
	Task #9: Identify Touch Points.....	18
	Task #10: Identify Data Flows.....	18
3.2	Identify PI in Use Case Privacy Domains and Systems	19
	Task #11: Identify Incoming PI.....	19
	Task #12: Identify Internally Generated PI.....	19
	Task #13: Identify Outgoing PI.....	19
3.3	Specify Required Privacy Controls Associated with PI	19
	Task #14: Specify Inherited Privacy Controls	20
	Task #15: Specify Internal Privacy Controls	20
	Task #16: Specify Exported Privacy Controls.....	20
4	Identify Functional Services Necessary to Support Privacy Controls	21
4.1	Services Needed to Implement the Controls	21
4.2	Service Details and Function Descriptions	23
	4.2.1 Core Policy Services	23
	1. Agreement Service	23
	2. Usage Service	23
	4.2.2 Privacy Assurance Services.....	23
	3. Validation Service	23
	4. Certification Service.....	23
	5. Enforcement Service	24

6.	Security Service	24
4.2.3	Presentation and Lifecycle Services	24
7.	Interaction Service	24
8.	Access Service	24
4.3	Identify Services satisfying the privacy controls	25
	Task #17: Identify the Services necessary to support operation of identified privacy controls. ...	25
5	Define the Technical Functionality and Business Processes Supporting the Selected Services	26
5.1	Identify Functions Satisfying the Selected Services	26
	Task #18: Identify the Functions that satisfy the selected Services	26
6	Perform Risk and/or Compliance Assessment.....	27
	Task #19: Conduct Risk Assessment	27
7	Initiate Iterative Process	28
	Task #20: Iterate the analysis and refine.	28
8	Operational Definitions for Fair Information Practices/Principles (“FIPPs”) and Glossary.....	29
8.1	Operational FIPPs	29
8.2	Glossary.....	30
Appendix A.	Acknowledgments	32
Appendix B.	Revision History	33

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.

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

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

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

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

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

80 1.3 Target Audiences

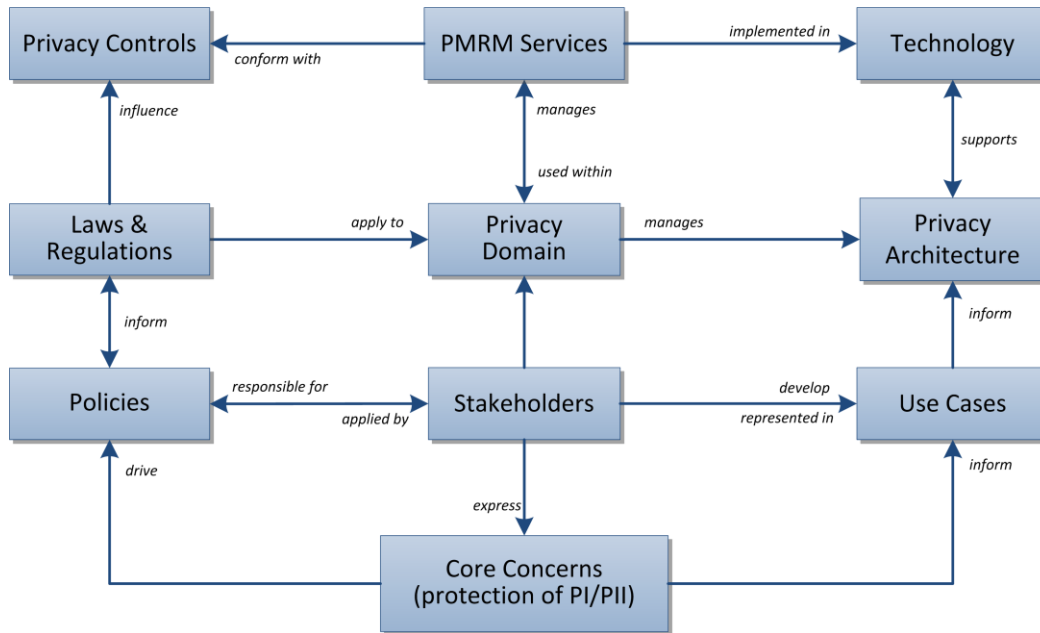
81 The intended audiences of this document and expected benefits to be realized include:

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

93 **1.4 Specification Summary**

94 The PMRM consists of:

- 95 • A conceptual model of privacy management, including definitions of terms;
 - 96 • A methodology; and
 - 97 • A set of operational services,
- 98 together with the inter-relationships among these three elements.



99
100 *Figure 1 – The PMRM Conceptual Model*

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

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

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

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

- 119 • defining and describing use-cases;
- 120 • identifying particular business domains and understanding the roles played by all Participants and
121 systems within that domain in relation to privacy issues;
- 122 • identifying the data flows and touch-points for all personal information within a privacy domain;
- 123 • specifying various privacy controls;
- 124 • mapping technical and process mechanisms to operational services;
- 125 • performing risk and compliance assessments.

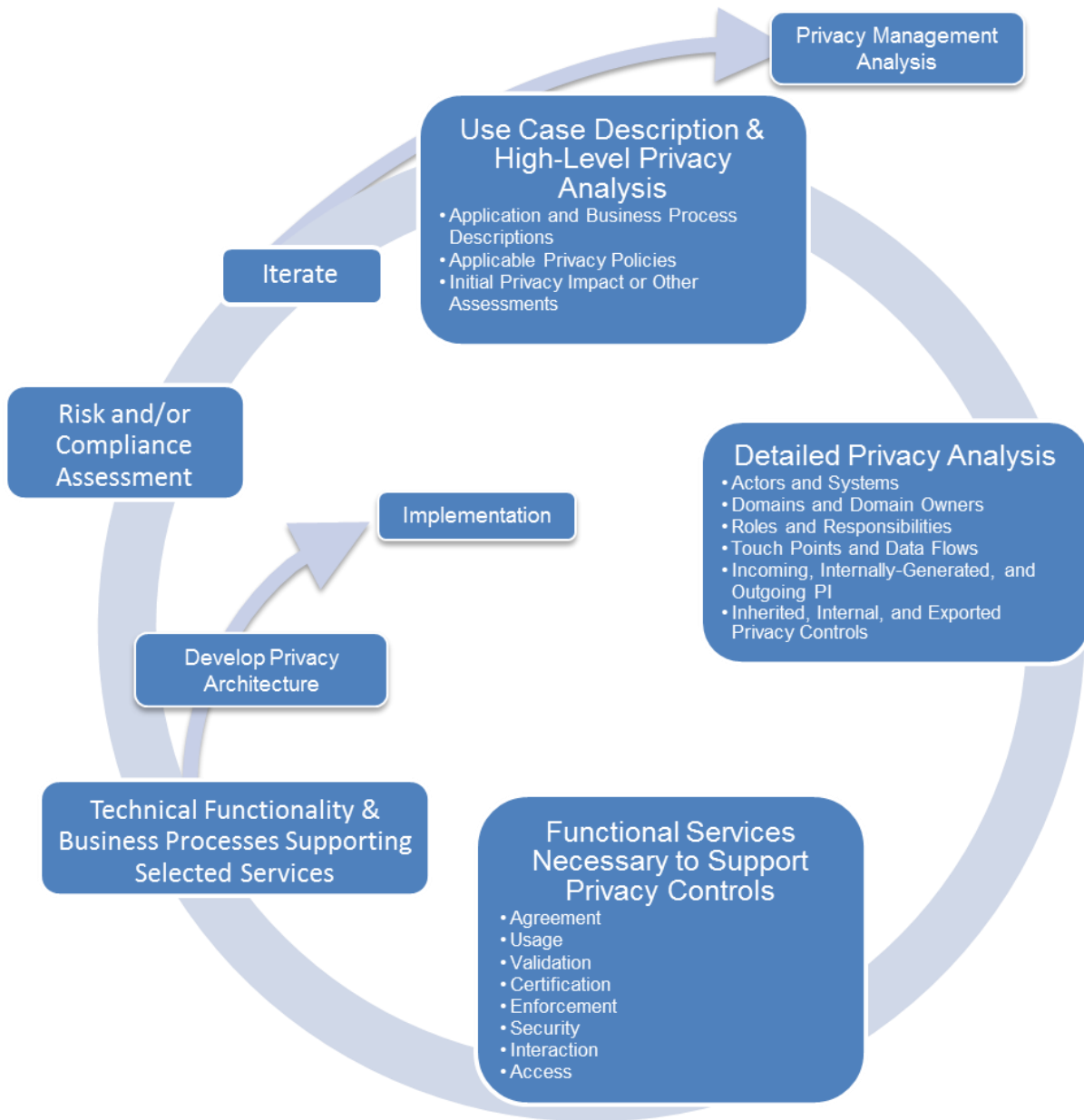
126 The specification also defines a set of Services deemed necessary to implement the management and
127 compliance of detailed privacy requirements within a particular use case. The Services are sets of
128 functions which form an organizing foundation to facilitate the application of the model and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

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

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

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

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



153
154 *Figure 2 - The PMRM Methodology*

155 **1.5 Terminology**

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

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

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

166 within this specification. Readers should also be aware that terms used in the different examples are
167 sometimes more “conversational” than in the formal, normative sections of the text and may not
168 necessarily be defined in the glossary of terms.

169 **1.6 Normative References**

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

172 **1.7 Non-Normative References**

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

175 **[SOA-RAF]** OASIS Specification, "Reference Architecture Foundation for SOA v1.0",
176 November 2012. [http://docs.oasis-open.org/soa-rm/soa-ra/v1.0/cs01/soa-ra-v1.0-](http://docs.oasis-open.org/soa-rm/soa-ra/v1.0/cs01/soa-ra-v1.0-cs01.pdf)
177 [cs01.pdf](http://docs.oasis-open.org/soa-rm/soa-ra/v1.0/cs01/soa-ra-v1.0-cs01.pdf)

178 **[NIST 800-53]** "Security and Privacy Controls for Federal Information Systems and
179 Organizations – Appendix J: Privacy Controls Catalog", NIST Special Publication
180 800-53 Draft Appendix J, July 2011.

181 **2 Develop Use Case Description and High-Level**
182 **Privacy Analysis**

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

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

194 **2.1 Application and Business Process Descriptions**

195 **Task #1: Use Case Description**

196 **Objective** Provide a general description of the Use Case.

197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218

Example²

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 includes 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.

219 **Task #2: Use Case Inventory**

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

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

² **Note:** The boxed examples are not to be considered as part of the normative text of this document.

233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250

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.

251

2.2 Applicable Privacy Policies

252

Task #3: Privacy Policy Conformance Criteria

253
254
255
256
257
258

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.

259
260

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

261
262
263
264
265
266
267
268

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...

...

269

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

270

Task #4: Assessment Preparation

271
272
273

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

274 assessment can be deferred until a later iteration step (see Section 4.3) or inherited from
275 a previous exercise.

276 **Example**

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

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

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

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

287 3 Develop Detailed Privacy Analysis

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

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

293 3.1 Identify Participants and Systems, Domains and Domain Owners, 294 Roles and Responsibilities, Touch Points and Data Flows

295 Task #5: Identify Participants

296 **Objective** Identify Participants having operational privacy responsibilities.

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

299

300 **Example**

301 *Participants Located at the Customer Site:*

302 Registered Customer

303 *Participants Located at the EV's Location:*

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

305 *Participants Located within the Utility's domain:*

306 Service Provider (Utility)

307 Contractors and Suppliers to the Utility

308 Task #6: Identify Systems

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

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

314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329

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

330 **Task #7: Identify Privacy Domains and Owners**

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

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

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

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

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

344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359

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.

360

Task #8: Identify Roles and Responsibilities within a Domain

361
362

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

363
364
365

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.

366

Example

367

Role: EV Manufacturer Privacy Officer

368

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.

369
370

371

Task #9: Identify Touch Points

372
373

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

374
375

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

376
377

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.

378

Example

379

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

380

381

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.

382
383

384

Task #10: Identify Data Flows

385
386

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

387

Constraint Data flows may be multidirectional or unidirectional.

388
389
390
391
392
393
394

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.

395 **3.2 Identify PI in Use Case Privacy Domains and Systems**

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

398 **Task #11: Identify Incoming PI**

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

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

402 **Task #12: Identify Internally Generated PI**

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

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

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

408 **Task #13: Identify Outgoing PI**

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

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

413 **Example**
414 *Incoming PI:*
415 Customer ID received by Customer Communications Portal
416 *Internally Generated PI:*
417 Current EV location associated with customer information, and time/location information logged
418 by EV On-Board system
419 *Outgoing PI:*
420 Current EV ID and location information transmitted to Utility Load Scheduler System

421 **3.3 Specify Required Privacy Controls Associated with PI**

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

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

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

431 **Task #14: Specify Inherited Privacy Controls**

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

434 **Example:**

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

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

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

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

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

448 **Example**

449 **Use Limitation Internal Privacy Controls**

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

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

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

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

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

460 **Example**

461 The Utility exports Jane's privacy preferences associated with her PI to its third party partner, whose
462 systems are capable of understanding and enforcing these preferences. One of her privacy control
463 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.

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

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

512 The functions of one Service may invoke another Service. In other words, functions under one Service
 513 may “call” those under another Service (for example, pass information to a new function for subsequent
 514 action). In line with principles of Service-Oriented Architecture (SOA)³, the Services can thus interact in
 515 an arbitrary interconnected sequence to accomplish a privacy management task or set of privacy lifecycle
 516 requirements. Use cases will illustrate such interactions and their sequencing as the PMRM is used to
 517 solve a particular privacy problem. By examining and by solving multiple use cases, the PMRM can be
 518 tested for applicability and robustness.

519 The table below provides a description of each Service’s functionality and an informal definition of each
 520 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	View and propose changes to stored PI

³ See for example the [SOA-RM] and the [SOA-RAF]

	to their PI	
--	-------------	--

521

522 **4.2 Service Details and Function Descriptions**

523 **4.2.1 Core Policy Services**

524 **1. Agreement Service**

- 525 • Define and document permissions and rules for the handling of PI based on applicable policies,
526 individual preferences, and other relevant factors.
- 527 • Provide relevant Actors with a mechanism to negotiate or establish new permissions and rules.
- 528 • Express the agreements for use by other Services.

529 **Example**

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

535 **2. Usage Service**

- 536 • Ensure that the use of PI complies with the terms of any applicable permission, policy, law or
537 regulation,
- 538 • Including PI subjected to information minimization, linking, integration, inference, transfer,
539 derivation, aggregation, and anonymization,
- 540 • Over the lifecycle of the use case.

541 **Example**

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

545 **4.2.2 Privacy Assurance Services**

546 **3. Validation Service**

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

549 **Example**

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

553 **4. Certification Service**

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

558
559
560
561
562

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.

563

5. Enforcement Service

564
565
566

- 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).

567
568
569
570
571

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.

572

6. Security Service

573
574
575
576

- 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.

577
578
579
580

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.

581

4.2.3 Presentation and Lifecycle Services

582

7. Interaction Service

583
584
585
586

- 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.

587
588
589
590
591
592

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.

593

8. Access Service

594
595

- 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.

596
597
598

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.

599 **4.3 Identify Services satisfying the privacy controls**

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

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

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

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

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

611 **Examples:**

612 Based upon

613 **a) Internally Generated PI** (Current EV location logged by EV On-Board system), and

614 **b) Outgoing PI** (Current EV location transmitted to Utility Load Scheduler System),
615 convert to operational Services as follows:

616 **“Log EV location”:**

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

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

621 **Interaction** Communicate EV Location to EV On-Board System

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

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

625 **Interaction** Communication established between EV Location and ULSS

626 **Security** Authenticate the ULSS site; secure the transmission

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

628 **Validation** Validate the EV Location against accepted locations

629 **Usage** ULSS records the EV Location, together with agreements

630 **5 Define the Technical Functionality and Business**
631 **Processes Supporting the Selected Services**

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

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

637 **5.1 Identify Functions Satisfying the Selected Services**

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

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

643 **Examples**

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

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

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

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

6 Perform Risk and/or Compliance Assessment

650

651 Task #19: Conduct Risk Assessment

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

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

657 Examples

658 “Log EV location”:

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

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

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

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

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

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

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

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

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

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

678

679

7 Initiate Iterative Process

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

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

688 **Task #20: Iterate the analysis and refine.**

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

690 8 Operational Definitions for Fair Information 691 Practices/Principles (“FIPPs”) and Glossary

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

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

700 8.1 Operational FIPPs

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

704 **Accountability**

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

708 **Notice**

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

716 **Consent**

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

721 **Collection Limitation and Information Minimization**

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

725 **Use Limitation**

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

729 **Disclosure**

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

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

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

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

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

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

753 **Anonymity**
754 Functionality that prevents data being collected or used in a manner that can identify a specific
755 natural person.

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

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

762 **8.2 Glossary**

763 **Actor**
764 A system-level, digital 'proxy' for either a (human) Participant (or their delegate) interacting with a
765 system or a (non-human) in-system process or other agent.

766 **Audit Controls**
767 Processes designed to provide reasonable assurance regarding the effectiveness and efficiency of
768 operations and compliance with applicable policies, laws, and regulations.

769 **Boundary Object**
770 A sociological construct that supports productive interaction and collaboration among multiple
771 communities.

772 **Control**
773 A process designed to provide reasonable assurance regarding the achievement of stated objectives.

774 **Domain Owner**
775 A Participant having responsibility for ensuring that privacy controls and privacy constraints are
776 implemented and managed in business processes and technical systems in accordance with policy
777 and requirements.

778 **Incoming PI**
779 PI flowing into a Privacy Domain, or a system within a Privacy Domain.

780 **Internally Generated PI**
781 PI created within the Privacy Domain or System itself.

782 **Monitor**
783 To observe the operation of processes and to indicate when exception conditions occur.

784 **Outgoing PI**
785 PI flowing out of one system to another system within a Privacy Domain or to another Privacy Domain.

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

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

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

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

799 **Privacy Architecture**
800 A collection of proposed policies and practices appropriate for a given domain resulting from use of
801 the PMRM

802 **Privacy Constraint**
803 An operational mechanism that controls the extent to which PII may flow between touch points.

804 **Privacy Control**
805 An administrative, technical or physical safeguard employed within an organization or Privacy Domain
806 in order to protect PII.

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

809 **Privacy Management**
810 The collection of policies, processes and methods used to protect and manage PI.

811 **Privacy Management Analysis**
812 Documentation resulting from use of the PMRM and that serves multiple Stakeholders, including
813 privacy officers and managers, general compliance managers, and system developers

814 **Privacy Management Reference Model and Methodology (PMRM)**
815 A model and methodology for understanding and analyzing privacy policies and their management
816 requirements in defined use cases; and for selecting the technical services which must be
817 implemented to support privacy controls.

818 **(PMRM) Service**
819 A collection of related functions and mechanisms that operate for a specified purpose.

820 **System**
821 A collection of components organized to accomplish a specific function or set of functions having a
822 relationship to operational privacy management.

823 **Touch Point**
824 The intersection of data flows with Privacy Domains or Systems within Privacy Domains.

825 **Appendix A. Acknowledgments**

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

828 **Participants:**

829 Peter F Brown, Individual Member
830 Gershon Janssen, Individual Member
831 Dawn Jutla, Saint Mary's University
832 Gail Magnuson, Individual Member
833 Joanne McNabb, California Office of Privacy Protection
834 John Sabo, Individual Member
835 Stuart Shapiro, MITRE Corporation
836 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