

---

# Privacy Management Reference Model and Methodology (PMRM) Version 1.0

## Working Draft 05 – Edits to CSPRD01 of 12 April 2012

6 November 2012

### Technical Committee:

OASIS Privacy Management Reference Model (PMRM) TC

### Chairs:

John Sabo ([john.annapolis@verizon.net](mailto:john.annapolis@verizon.net)), **Individual**  
Michael Willett ([mwillett@nc.rr.com](mailto:mwillett@nc.rr.com)), Individual

**Comment [PFB1]:** Change of affiliation

### Editors:

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

**Comment [PFB2]:** Change of affiliation

### 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.

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.

# Table of Contents

1	Introduction .....	4
1.1	Context .....	4
1.2	Objectives.....	4
1.3	Target Audiences.....	5
1.4	Specification Summary.....	6
1.5	Terminology.....	8
1.6	Normative References.....	9
1.7	Non-Normative References .....	9
2	Develop Use Case Description and High-Level Privacy Analysis .....	10
2.1	Application and Business Process Descriptions .....	10
	Task #1: Use Case Description .....	10
	Task #2: Use Case Inventory.....	11
2.2	Applicable Privacy Policies .....	11
	Task #3: Privacy Policy Conformance Criteria .....	11
2.3	Initial Privacy Impact (or other) Assessment(s) [optional].....	12
	Task #4: Assessment Preparation .....	12
3	Develop Detailed Privacy Analysis.....	13
3.1	Identify Participants and Systems, Domains and Domain Owners, Roles and Responsibilities, Touch Points and Data Flows .....	13
	Task #5: Identify Participants .....	13
	Task #6: Identify Systems .....	13
	Task #7: Identify Privacy Domains and Owners.....	14
	Task #8: Identify Roles and Responsibilities within a Domain .....	15
	Task #9: Identify Touch Points.....	15
	Task #10: Identify Data Flows.....	16
3.2	Identify PI in Use Case Privacy Domains and Systems .....	16
	Task #11: Identify Incoming PI.....	16
	Task #12: Identify Internally Generated PI.....	16
	Task #13: Identify Outgoing PI.....	16
3.3	Specify Required Privacy Controls Associated with PI.....	17
	Task #14: Specify Inherited Privacy Controls .....	17
	Task #15: Specify Internal Privacy Controls .....	18
	Task #16: Specify Exported Privacy Controls.....	18
4	Identify Functional Services Necessary to Support Privacy Controls .....	19
4.1	Services Needed to Implement the Controls .....	19
4.2	Service Details and Function Descriptions .....	21
4.2.1	Core Policy Services .....	21
	1. Agreement Service .....	21
	2. Usage Service .....	21
4.2.2	Privacy Assurance Services .....	21
	3. Validation Service.....	21
	4. Certification Service .....	21
	5. Enforcement Service.....	22

6.	Security Service .....	22
4.2.3	Presentation and Lifecycle Services .....	22
7.	Interaction Service .....	22
8.	Access Service .....	22
4.3	Identify Services satisfying the privacy controls .....	23
	Task #17: Identify the Services necessary to support operation of identified privacy controls. ....	23
5	Define the Technical Functionality and Business Processes Supporting the Selected Services .....	24
5.1	Identify Functions Satisfying the Selected Services .....	24
	Task #18: Identify the Functions that satisfy the selected Services .....	24
6	Perform Risk and/or Compliance Assessment .....	25
	Task #19: Conduct Risk Assessment .....	25
7	Initiate Iterative Process .....	26
	Task #20: Iterate the analysis and refine. ....	26
8	PMRM Glossary, plus Operational Definitions for Fair Information Practices/Principles ("FIPPs") .....	27
	8.1 Operational FIPPs .....	27
	8.2 Glossary .....	28
Appendix A.	Acknowledgments .....	31
Appendix B.	Revision History .....	32

# 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)<sup>1</sup> 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 other 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.

Comment [JTS3]: Issue #1, part

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.

Comment [PFB4]: Issue #1, part

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.

<sup>1</sup> 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 Actors-Participants have  
48 regarding use and protection of PI. Even the definition of PI will vary. The PMRM attempts to address  
49 these issues. Because data can so easily migrate across jurisdictional boundaries, rights cannot be  
50 protected without explicit specification of what boundaries apply.

Comment [PFB5]: Issue #8

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 PMRM process output from using the PMRM, in contrast, should have direct and ongoing relevance  
71 for all Stakeholders and is less likely to suffer the above dynamic. This is because it should be considered  
72 as a “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.

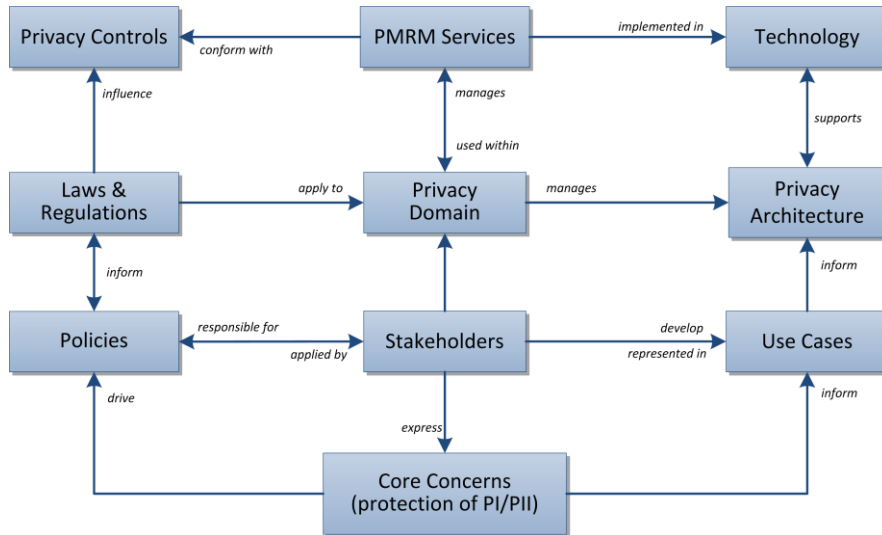
### 80 **1.3 Target Audiences**

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

Comment [JTS6]: Issue #1, part

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 and  
 103 principles (which both reflect and influence actual regulation and lawmaking); and on the other hand,  
 104 inform the use cases that are developed to address the specific architecture and solutions required by the  
 105 Stakeholders in a particular domain.

Comment [PFB7]: Issue #1, part

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/PIs), 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 actors-Participants
- 121 and 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.

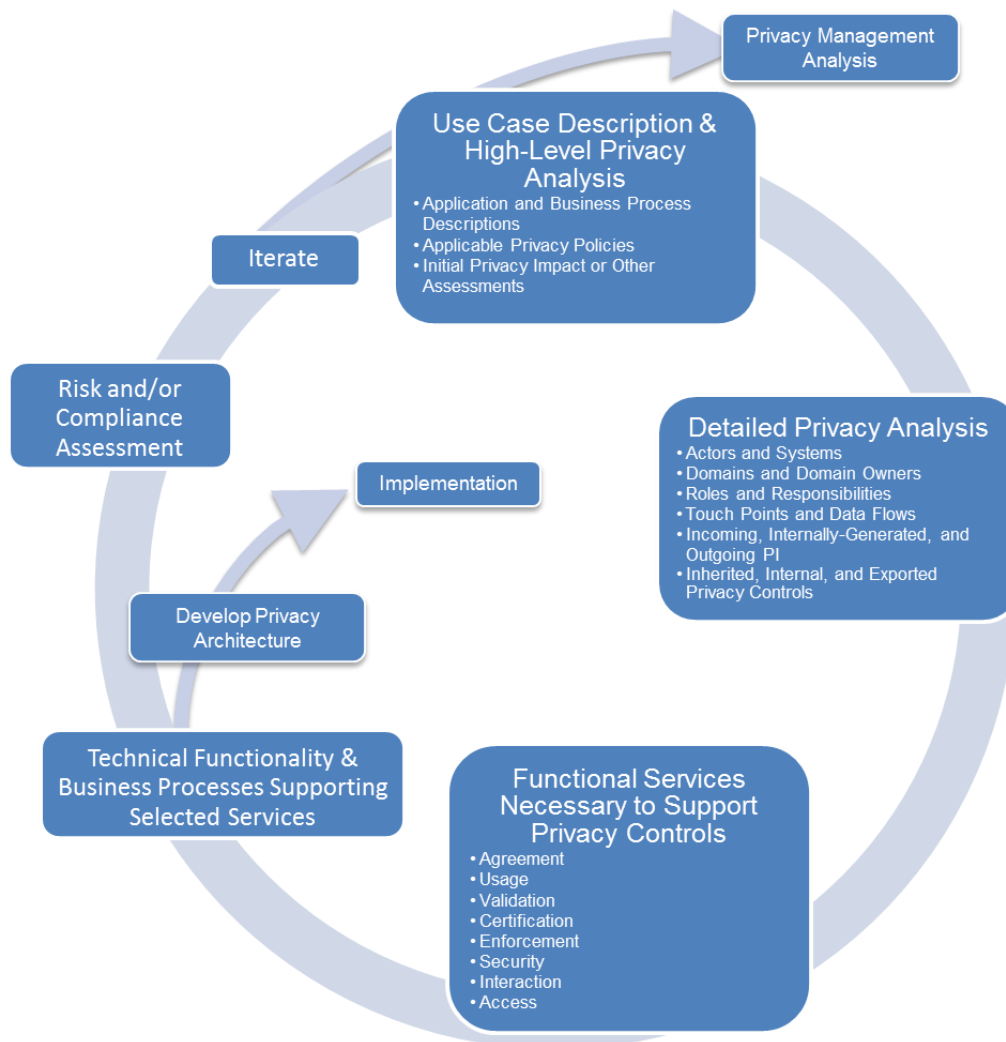
126 The specification also defines a set of Services deemed necessary to implement the management and  
127 compliance of detailed privacy requirements within a particular use case. The Services are sets of  
128 functions which form an organizing foundation to facilitate the application of the model 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  
139 ~~PMRM model~~ may choose to adopt some parts of the model and not others. However, a complete use of  
140 the model will contribute to a more comprehensive privacy management architecture for a given capability  
141 or 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*

**Comment [P8]:** Issue #2, Figure updated

## 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.

## 167 **1.6 Normative References**

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

## 170 **1.7 Non-Normative References**

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

173 **[SOA-RAF]** OASIS Specification, "SOA Reference Architecture Foundation 1.0" {Pending  
174 [Designated Cross-Reference](#)}

175 **[NIST 800-53]** "Security and Privacy Controls for Federal Information Systems and  
176 Organizations – Appendix J: Privacy Controls Catalog", NIST Special Publication  
177 800-53 Draft Appendix J, July 2011.

178  
179  
180  
181  
182  
183  
184  
185  
186  
187  
188  
189  
190  
191  
  
192  
  
193  
194  
195  
196  
197  
198  
199  
200  
201  
202  
203  
204  
205  
206  
207  
208  
209  
210  
211  
212  
213  
214  
215  
216  
217

## 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 entity utilizing 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 the user of the PMRM. 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 ~~now~~ 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 person/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.

Comment [PFB9]: Issue #4, part

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

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

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

Comment [PFB10]: Issue #4, part

232 **Example**

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

234 Legal and Regulatory Jurisdictions:

235 California Constitution, Article 1, section 1 gives each citizen an "inalienable right" to  
 236 pursue and obtain "privacy."  
 237 Office of Privacy Protection - California Government Code section 11549.5.  
 238 Automobile "Black Boxes" - Vehicle Code section 9951.  
 239 ...

240 Personal Information Collected on Internet:

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

242 The California Public Utilities Commission, which "serves the public interest by protecting  
 243 consumers and ensuring the provision of safe, reliable utility service and infrastructure at  
 244 reasonable rates, with a commitment to environmental enhancement and a healthy  
 245 California economy"...

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

247

248 Customer: The Data Subject-Customer's selected settings for policy options presented via customer-  
 249 facing interfaces or customize the settings.

Comment [PFB11]: Issue #4, part

250 **2.2 Applicable Privacy Policies**

251 **Task #3: Privacy Policy Conformance Criteria**

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

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

260 **Example**

261 Privacy Policy Conformance Criteria:

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

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

264 (a) Identity authentication

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

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

267 ...

268 **2.3 Initial Privacy Impact (or other) Assessment(s) [optional]**

269 **Task #4: Assessment Preparation**

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

275 **Example**

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

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

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

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

**Comment [PFB12]:** Issue #4, part

**Comment [PFB13]:** Issue #4, part

**Comment [PFB14]:** Issue #4, part

286

### 3 Develop Detailed Privacy Use Case Analysis

287

**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.

288

289

290

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

291

292

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

293

294

##### Task #5: Identify Participants

295

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

296

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

297

298

~~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.~~

299

300

Comment [PFB15]: Issue #4, part

301

##### Example

302

Participants Located at the Customer Site:

303

Registered Customer

304

Participants Located at the EV's Location:

305

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

306

Participants Located within the Utility's domain:

307

Service Provider (Utility)

308

Contractors and Suppliers to the Utility

309

##### Task #6: Identify Systems

310

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

311

312

**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.

313

314

315	<b>Example</b>
316	<u>System Located at the Customer Site(s):</u>
317	Customer Communication Portal
318	EV Physical Re-Charging and Metering System
319	<u>System Located in the EV(s):</u>
320	EV: Device
321	EV On-Board System: System
322	<u>System Located within the EV manufacturer's domain:</u>
323	EV Charging Data Storage and Analysis System
324	<u>System Located within the Utility's domain:</u>
325	EV Program Information System (includes Rates, Customer Charge Orders, Customers enrolled
326	in the program, Usage Info etc.)
327	EV Load Scheduler System
328	Utility Billing System
329	Remote Charge Monitoring System
330	Partner marketing system for transferring usage pattern and location information

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

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

334 **Definition** A "Domain" covers both physical areas (such as a customer site or home) and logical  
 335 areas (such as a wide-area network or cloud computing environment) that are subject to  
 336 the control of a particular domain owner. ~~Privacy Domains are the physical or logical~~  
 337 ~~areas within the use case subject to control by Domain Owners.~~

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

**Comment [PFB16]:** Issue #4, part

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

**Comment [PFB17]:** Issue #4, part

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

346 **Example**

347 *Utility Domain:*

348 The physical premises located at... which includes the Utility's program information system, load

349 scheduling system, billing system, and remote monitoring system

350 This physical location is part of a larger logical privacy domain, owned by the Utility and extends

351 to the Customer Portal Communication system at the Customer's site, and the EV On-Board

352 software application System installed in the EV by the Utility, together with cloud-based services

353 hosted by....-

354 *Customer Domain:*

355 The physical extent of the customer's home and adjacent land as well as the EV, wherever

356 located, together with the logical area covered by devices under the ownership and control of the

357 customer (such as mobile devices).

358 **Example**

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

360 The EV (with its ID Number) belongs to the Customer Domain Owner and the Vehicle

361 Manufacturer Domain Owners, but the EV ID may be accessed by the Utility.

362 **Task #8: Identify Roles and Responsibilities within a Domain**

363 **Objective** For any given use case, identify the roles and responsibilities assigned to specific

364 Participants and Systems ~~actors~~ within a specific privacy domain

**Comment [PFB18]:** Issue #4, part

365 **Rationale** Any Participant ~~individual or position~~ may carry multiple roles and responsibilities and

366 these need to be distinguishable, particularly as many functions involved in processing of

367 PI are assigned to ~~a person or other actor~~ functional roles, ~~according to~~ with explicit roles

368 and authority to act, rather to ~~a specific participant~~ person or actor as such.

**Comment [PFB19]:** Issue #4, part

**Comment [PFB20]:** Issue #4, part

**Comment [PFB21]:** Issue #4, part

369 **Example**

370 **Role:** EV Manufacturer Privacy Officer

371 **Responsibilities:** Ensure that all PI data flows from EV On-Board System conform both with

372 contractual obligations ~~towards associated with~~ the Utility and vehicle owner as well

373 as the Collection Limitation and Information Minimization FIP/P. in its privacy

374 policies.

**Comment [PFB22]:** Editorial

375 **Task #9: Identify Touch Points**

376 **Objective** Identify the touch points at which the data flows intersect with Privacy Domains or

377 Systems within Privacy Domains.

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

379 Privacy Domains.

380 **Rationale** The main purpose for identifying touch points in the use case is to clarify the data flows

381 and ensure a complete picture of all Privacy Domains and Systems in which PI is used.

382 **Example**  
383 ~~The Communication Interfaces whereby actors send and receive data are touch points. For instance~~  
384 ~~the The Customer Communication Portal provides an interface via through which the Customer~~  
385 ~~communicates a charge order to the Utility. This interface is a touch point.~~  
386 When the customer plugs into the charging station, the EV On-Board System ~~also embeds~~  
387 communication functionality ~~that acts as its touch point~~ to send EV ID and EV Charge Requirements to  
388 the Customer Communication Portal. ~~This functionality provides a further touch point.~~

389 **Task #10: Identify Data Flows**

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

392 **Constraint** Data flows may be multidirectional or unidirectional.

393 **Example**  
394 When a charging request event occurs, the Customer Communication Portal sends Customer  
395 information, EV identification, and Customer Communication Portal location information to the EV  
396 Program Information System managed by the Utility.  
397 This application uses metadata tags to indicate whether or not customer' identification and location data  
398 may be shared ~~(and then, only~~ with authorized third parties), and ~~to prohibits~~ the sharing of data that  
399 provides customers' movement history, if derived from an aggregation of transactions.

400 **3.2 Identify PI in Use Case Privacy Domains and Systems**

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

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

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

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

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

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

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

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

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

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

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



418 **Example**

419 *Incoming PI:*

420 Customer ID received by Customer Communications Portal

421 *Internally Generated PI:*

422 Current EV location associated with customer information, and time/location information logged

423 by EV On-Board system

424 *Outgoing PI:*

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

426 **3.3 Specify Required Privacy Controls Associated with PI**

427 **Goal** For Incoming, Internally Generated and Outgoing PI, specify the privacy controls required

428 to enforce the privacy policy associated with the PI. Privacy controls may be pre-defined

429 or may be derived. In either case, privacy controls are typically associated with specific

430 Fair Information Practices Principles (FIP/Ps) that apply to the PI.

431 **Definition** Control is a process designed to provide reasonable assurance regarding the

432 achievement of stated objectives.

433 **Definition** Privacy Controls are administrative, technical and physical safeguards employed within

434 an organization or Privacy Domain in order to protect PI. They are the means by which

435 privacy policies are satisfied in an operational setting.

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

437 **Objective** Specify the required Privacy Controls which are inherited from Privacy Domains or

438 Systems within Privacy Domains.

439 **Example:**

440 The utility inherits a Privacy Control associated with the Electric Vehicle's ID (EVID) from the vehicle

441 manufacturer's privacy policies.

442 The utility inherits the consumer's Operational Privacy Control Requirements, expressed as privacy

443 preferences, via a link with the customer communications portal when she plugs her EV into friend

444 Rick's charging station.

445 The utility must apply Jane's privacy preferences to the current transaction. The Utility accesses Jane's

446 privacy preferences and learns that Jane does not want her association with Rick exported to the

447 Utility's third party partners. Even though Rick's privacy settings differ around his PI, Jane's non-

448 consent to the association being transmitted out of the Utility's privacy domain is sufficient to prevent

449 commutative association. Thus if Rick were to charge his car's batteries at Jane's, the association

450 between them would also not be shared with third parties.

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

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

453 **Example**

454 **Use Limitation Internal Privacy Controls**

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

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

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

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

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

465 **Example**

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

469 **4 Identify Functional Services Necessary to Support**  
 470 **Privacy Controls**

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

Comment [PFB23]: Issue #4, part

476 **4.1 Services Needed to Implement the Controls**

477 A set of operational Services is the organizing structure which will be used to link the required Privacy  
 478 Controls specified in Section 4.3 to operational mechanisms necessary to implement those requirements.  
 479 Eight Privacy Services have been identified, based on the mandate to support an arbitrary set of privacy  
 480 policies, but at a *functional level*. The eight Services can be logically grouped into three categories:

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

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

<b>Core Policy Services</b>	<b>Privacy Assurance Services</b>		<b>Presentation &amp; Lifecycle Services</b>
Agreement	Validation	Certification	Interaction
Usage	Security	Enforcement	Access

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

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

Comment [PFB24]: Issue #4, part

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

Comment [PFB25]: Issue #4, part

506 | As used here,  
 507 - A "Service" is defined as a collection of related functions and mechanisms that operate for a specified  
 508 purpose;  
 509 - An "Actor" is defined as a system-level, digital 'proxy' for either a (human) Participant or an (non-  
 510 human) system-level process or other agent.

Comment [PFB26]: Issue #4, part

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

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

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

SERVICE	FUNCTIONALITY	PURPOSE
<b>AGREEMENT</b>	Define and document permissions and rules for the handling of PI based on applicable policies, individual 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
<b>USAGE</b>	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
<b>VALIDATION</b>	Evaluate and ensure the information quality of PI in terms of Accuracy, Completeness, Relevance, Timeliness and other relevant qualitative factors	Check PI
<b>CERTIFICATION</b>	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 of that Actor, Domain, System or system component against defined policies and assigned roles.	Check credentials
<b>ENFORCEMENT</b>	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
<b>SECURITY</b>	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
<b>INTERACTION</b>	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
<b>ACCESS</b>	Enable data-subjects, Actors, as required and/or allowed by permission, policy, or regulation, to review their PI that is held within a Domain and propose changes and/or corrections to their PI	View and propose changes to stored PI

Comment [PFB27]: Issue #4, part

Comment [PFB28]: Issue #4, part

Comment [PFB29]: Issue #4, part

<sup>2</sup> See for example the [SOA-RM] and the [SOA-RAF]

526

## 527 4.2 Service Details and Function Descriptions

### 528 4.2.1 Core Policy Services

#### 529 1. Agreement Service

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

#### 534 Example

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

Comment [PFB30]: Issue #6, part

#### 540 2. Usage Service

- 541 • Ensure that the use of PI complies with the terms of any applicable permission, policy, law or  
542 regulation,
- 543 • Including PI subjected to information minimization, linking, integration, inference, transfer,  
544 derivation, aggregation, and anonymization,
- 545 • Over the lifecycle of the use case.

#### 546 Example

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

Comment [PFB31]: Issue #4, part

### 550 4.2.2 Privacy Assurance Services

#### 551 3. Validation Service

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

#### 554 Example

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

Comment [PFB32]: Issue #6, part

#### 558 4. Certification Service

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

563  
564  
565  
566  
567

**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.

Comment [PFB33]: Issue #6, part

568  
569  
570  
571

### 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).

572  
573  
574  
575  
576

**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 person (the organization's privacy officer), who takes appropriate action.

Comment [PFB34]: Issue #4, part

577  
578  
579  
580  
581

### 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.

582  
583  
584  
585

**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 confidentiality-security policies.

Comment [PFB35]: Issue #6, part

## 4.2.3 Presentation and Lifecycle Services

587  
588  
589  
590  
591

### 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.

592  
593  
594  
595  
596  
597

**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.

Comment [PFB36]: Issue #6, part

598  
599  
600

### 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.

601  
602  
603

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

604 **4.3 Identify Services satisfying the privacy controls**

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

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

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

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

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

616 **Examples:**

617 Based upon

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

621 **“Log EV location”:**

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

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

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

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

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

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

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

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

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

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

**Comment [PFB37]:** Issue #9

**Comment [PFB38]:** Issue #6, part

---

635 **5 Define the Technical Functionality and Business**  
636 **Processes Supporting the Selected Services**

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

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

642 **5.1 Identify Functions Satisfying the Selected Services**

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

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

648 **Examples**

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

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

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

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



655

## 6 Perform Risk and/or Compliance Assessment

656

### Task #19: Conduct Risk Assessment

657

**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

658

659

**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.

660

661

662

#### Examples

663

#### “Log EV location”:

664

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

665

666

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

667

668

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

669

670

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

671

672

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

673

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

674

675

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

676

677

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

678

679

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

680

681

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

682

683

684

## 7 Initiate Iterative Process

685

### Goal

A 'first pass' through the Tasks above ~~could 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 ~~well-understood~~ developed.

686

687

688

689

690

691

692

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.

Comment [PFB39]: Issue #3

693

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

694

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

## 695 8 Operational Definitions for Fair Information 696 Practices/Principles (“FIPPs”) and Glossary

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

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

### 705 8.1 Operational FIPPs

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

#### 709 **Accountability**

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

Comment [PFB40]: Issue #4, part

#### 713 **Notice**

714 Functionality providing Information, in the context of a specified use, regarding ~~an entity’s privacy~~  
715 policies and practices ~~exercised within a Privacy Domain~~ including: definition of the Personal  
716 Information collected; its use (purpose specification); its disclosure to parties within or external to the  
717 ~~entitydomain~~; practices associated with the maintenance and protection of the information; options  
718 available to the ~~individual data subject~~ regarding the ~~collector processor’s~~ privacy practices; retention  
719 and deletion; changes made to policies or practices; and other information provided to the ~~individual~~  
720 ~~data subject~~ at designated times and under designated circumstances.

Comment [PFB41]: Issue #4, part

Comment [PFB42]: Issue #4, part

Comment [PFB43]: Issue #4, part

Comment [PFB44]: Issue #4, part

#### 721 **Consent**

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

Comment [PFB45]: Issue #4, part

#### 726 **Collection Limitation and Information Minimization**

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

Comment [PFB46]: Issue #4, part

#### 730 **Use Limitation**

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

Comment [PFB47]: Issue #4, part

Comment [PFB48]: Issue #4, part

#### 735 **Disclosure**

736 Functionality ~~that~~ enables the ~~release~~, transfer, provision of access to, use for new purposes, or  
737 ~~divulging-release~~ in any ~~other~~ manner, of Personal Information ~~held by an entity-managed within a~~  
738 ~~Privacy Domain~~ in accordance with notice and consent permissions and/or applicable laws and

739 | functionality making known the information ~~collector processor's~~ policies to external parties receiving  
740 | the information.

Comment [PFB49]: Issue #4, part

#### 741 | **Access and Correction**

742 | Functionality ~~that allows an adequately identified data subject individuals having adequate proof of~~  
743 | ~~identity to discover, from an entity, or discover and/or correct or delete, their~~ Personal Information  
744 | ~~managed within a Privacy Domain, at specified costs and within specified time constraints; and~~  
745 | functionality providing notice of denial of access; and options for challenging denial when specified.

Comment [PFB50]: Issue #4, part

Comment [P51]: Not relevant for the definition

#### 746 | **Security/Safeguards**

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

#### 750 | **Information Quality**

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

#### 753 | **Enforcement**

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

Comment [PFB52]: Issue #4, part

#### 757 | **Openness**

758 | Functionality, ~~available to data subjects, making availability to individuals the~~ that allows access to an  
759 | information ~~collector's or information user processor's~~ policies and practices relating to their  
760 | management of ~~their~~ Personal Information and ~~that~~ establishes the existence, nature, and purpose of  
761 | use of Personal Information held about the ~~individuals data subject~~.

Comment [PFB53]: Issue #4, part

Comment [PFB54]: Issue #4, part

#### 762 | **Anonymity**

763 | Functionality ~~that prevents data being collected or used in a manner that can identify a specific~~  
764 | ~~natural person renders personal information anonymous so that an individual is no longer identifiable.~~

#### 765 | **Information Flow**

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

#### 768 | **Sensitivity**

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

## 771 | **8.2 Glossary**

### 772 | **Actor**

773 | ~~A system-level, digital 'proxy' for either a (human) Participant (or their delegate) interacting with a~~  
774 | ~~system or a (non-human) in-system process or other agent. A data subject or a human or a non-~~  
775 | ~~human agent or (sub)system interacting with PI within Privacy Domain or System.~~

Comment [PFB55]: Issue #4, part

### 776 | **Audit Controls**

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

Comment [PFB56]: Issue #7

### 779 | **Boundary Object**

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

### 782 | **Control**

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

784 **Domain Owner**

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

Comment [PFB57]: Issue #4, part

788 **Incoming PI**

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

790 **Internally Generated PI**

791 PI created within the Privacy Domain or System itself.

792 **Monitor**

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

Comment [PFB58]: Issue #7

794 **Outgoing PI**

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

796 **Participant**

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

799 **PI**

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

Comment [PFB59]: Issue #4, part

802 **PII**

803 Personally identifiable information – any (set of) data that can be used to uniquely identify a natural  
804 person distinguish or trace an individual's identity.

Comment [PFB60]: Issue #4, part

805 **Policy**

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

Comment [PFB61]: Issue #1, part

809 **Privacy Architecture**

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

Comment [PFB62]: Issue #13, part

812 **Privacy Constraint**

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

814 **Privacy Control**

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

817 **Privacy Domain**

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

819 **Privacy Management**

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

821 **Privacy Management Analysis**

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

Comment [PFB63]: Issue #13, part

824 **Privacy Management Reference Model and Methodology (PMRM)**

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

828 **(PMRM) Service**

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

830 **System**

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

833 **Touch Point**

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

---

835 **Appendix A. Acknowledgments**

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

838 **Participants:**

839 Peter F Brown, Individual Member  
840 Gershon Janssen, Individual Member  
841 Dawn Jutla, Saint Mary's University  
842 Gail Magnuson, Individual Member  
843 Joanne McNabb, California Office of Privacy Protection  
844 | John Sabo, [Individual MemberCA Technologies](#)  
845 Stuart Shapiro, MITRE Corporation  
846 Michael Willett, Individual Member

**Comment [PFB64]:** Change of affiliation

---

## 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