Privacy Engineering: We Need New Tools and Practices to Deliver and Manage Privacy/Data Protection in Networked Systems and Applications

John Sabo, Chair OASIS IDTrust Member Section
Chair, PMRM Technical Committee
John.sabo711@yahoo.com
Data Privacy - The Appeal of Abstraction
# 30+ Years of Policies/Fair Information Practices

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>● Collection Limitation</td>
<td>○ Accountability</td>
<td>■ Preventing Harm</td>
</tr>
<tr>
<td>● Data Quality</td>
<td>○ Identifying Purposes</td>
<td>■ Notice</td>
</tr>
<tr>
<td>● Purpose Specification</td>
<td>○ Consent</td>
<td>■ Collection Limitation</td>
</tr>
<tr>
<td>● Use Limitation</td>
<td>○ Limiting Collection</td>
<td>■ Uses of Personal Information</td>
</tr>
<tr>
<td>● Security Safeguards</td>
<td>○ Limiting Use, Disclosure and Retention</td>
<td>■ Choice</td>
</tr>
<tr>
<td>● Openness</td>
<td>○ Accuracy</td>
<td>■ Integrity of Personal Information</td>
</tr>
<tr>
<td>● Individual Participation</td>
<td>○ Safeguards</td>
<td>■ Security Safeguard</td>
</tr>
<tr>
<td>● Accountability</td>
<td>○ Openness</td>
<td>■ Access and Correction</td>
</tr>
<tr>
<td></td>
<td>○ Individual Access</td>
<td>■ Accountability</td>
</tr>
<tr>
<td></td>
<td>○ Challenging Compliance</td>
<td></td>
</tr>
</tbody>
</table>

# Contemporary Principles

<table>
<thead>
<tr>
<th>GDPR Article 5</th>
<th>ISO/IEC -29100</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Lawfulness, fairness and transparency</td>
<td>• Consent and choice</td>
</tr>
<tr>
<td>• Purpose limitation</td>
<td>• Purpose legitimacy and specification</td>
</tr>
<tr>
<td>• Data minimisation</td>
<td>• Collection limitation</td>
</tr>
<tr>
<td>• Accuracy</td>
<td>• Data minimization</td>
</tr>
<tr>
<td>• Storage limitation</td>
<td>• Use, retention and disclosure limitation</td>
</tr>
<tr>
<td>• <strong>Security</strong> – confidentiality, integrity, availability and resilience</td>
<td>• Accuracy and quality</td>
</tr>
<tr>
<td></td>
<td>• Openness, transparency and notice</td>
</tr>
<tr>
<td></td>
<td>• Individual participation and access</td>
</tr>
<tr>
<td></td>
<td>• Accountability</td>
</tr>
<tr>
<td></td>
<td><strong>Information security</strong></td>
</tr>
<tr>
<td></td>
<td>• Privacy compliance</td>
</tr>
</tbody>
</table>
Privacy by Design
Foundational Principles

• 1. **Proactive** not **Reactive** - Preventative, not Remedial
• 2. Privacy as the **Default** setting
• 3. Privacy **Embedded** into Design
• 4. **Full** Functionality - Positive-Sum, not Zero-Sum
• 5. End-to-End **Security** - Full Lifecycle Protection
• 6. Visibility **and** Transparency - Keep it Open
• 7. Respect for User Privacy - **Keep it User-Centric**

Source: https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf
But...Applying Abstract Principles in Complex Systems – A Hard Problem
High Level View - US Health Information Exchange Roles Diagram

Providers
- Physicians
- Hospitals
- Clinics
- Labs
- Pharmacy
- Other

EMRs and PHRs

Intermediaries
- Health Plans
- Service Bureaus
- Partnerships
- Other

Health Information Exchange (HIE)
Operated by State Designed Entity (SDE)

Standards

Messaging

Applications
- System
- Database

Services
- Partner Management
- Security/HIPAA
- Privacy/HIPAA
- System Management
- Governance

Members
- Google Health
- Microsoft Health Vault
- Web MD
- Smart Devices (Stakaris)
- Other

Organizations
- BC/BS Association
- World Health Congress
- Healthcare Leadership Council
- Other

Payers
- Blues
- Medicare
- Medicaid
- Private Pay
- Self-Pay
- Other

Government
- WHO
- CMS
- CDC
- NIH
- Data Mining
US Healthcare On-Site Care Business Processes

Figure 2.2.4.1-1 On-Site Care Scenario Perspective Business Sequence Diagram

Legend
- Bold Red: Interoperability Specification (IS) Required
- Narrow Orange: Standards Gap or Overlap
- Narrow Blue: Internal Information Exchange

6.1 SCENARIO: On-site Care Perspective
6.1.1 EVENT: On-Site Mgmt and Coordination
6.1.2 EVENT: Start collection of on-site care information
6.1.3 EVENT: Assess additional patient health information
6.1.4 EVENT: Assess, treat and transport patient
6.1.5: Update on-site care information
6.1.6: Transport Patient
6.1.7: Provide Information

On-site information requests (e.g., ECON, PIX/PDO, EHR, PHR) may be direct or via the Emergency Communications System.
NIST Smart Grid Conceptual Model

Source: 27 NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0
‘Simple’ On-line System Enabling Residents to Report Issues to Town Council for Action
Moving from Abstract to Concrete
GDPR Article 25
Data Protection by Design and by Default

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks ... the controller shall... implement appropriate technical and organisational measures... which are designed to implement data-protection principles... in an effective manner and to integrate the necessary safeguards into the processing....

2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.
• From Macro to Micro:
Data Privacy/Data Protection in [*] Systems and Applications

• **Macro /Abstract**
  - Aspirations
  - Principles
  - Policies
  - Standards
  - Risk Assessment Models

• **Micro/ Concrete**
  - Business Processes
  - Systems
  - Technologies
  - Operational Environment and Risk Management
  - Risk Assessment

Orders of Magnitude
More Complexity at Functional Implementation Level

Complexity Increases with Scale of System and App Integration
GDPR Attempts to Bridge Data Protection Policies with Associated Technical Functionality

• Are organizations able to put in place comprehensive controls over how they use and manage personal data?
• Do organizations understand how to implement technical and business process functionality across systems that will deliver promised data protections and demonstrate compliance?
• Do software developer/technical teams – including third party data partners – have the tools to understand and implement data protection requirements?
• Can they quickly address rapidly changing systems, technologies and business objectives?
• Is operational compliance in vast, interconnected applications and systems achievable today?
The GDPR and the Need for New Tools and Approaches to Data Protection Delivery

• The GDPR’s mandates are global - will cover 510 million people (including Britain) and have International impact

• To effectively meet its mandates, we must
  o Develop tools that leverage existing technical and policy standards
  o foster the development and adoption of new standards and data protection practices and tools where there are gaps
  o take the next steps towards building a Privacy Engineering capability
OASIS Privacy by Design Documentation for Software Engineers (PbD-SE)

- OASIS Privacy by Design Documentation for Software Engineers (PbD—SE)
- [http://docs.oasis-open.org/pbd-se/pbd-se/v1.0/csd01/pbd-se-v1.0-csd01.pdf](http://docs.oasis-open.org/pbd-se/pbd-se/v1.0/csd01/pbd-se-v1.0-csd01.pdf)

  The PbD-SE TC published a specification and a separate committee note addressing the information sources and documentation necessary for software developers to ensure that they are applying Privacy by Design principles to particular software development projects.

- **But .. Software engineers represent only one stakeholder group impacting the delivery of data protection functionality in networked systems**
Integrating the “macro” with the “micro”
Privacy Engineering
Why Privacy Engineering? – An Analogy

Civil engineering is a professional engineering discipline that deals with the design, construction, and maintenance of the physical and naturally built environment, including works like roads, bridges, canals, dams, and buildings.

- Materials science and engineering
- Coastal engineering
- Construction engineering
- Earthquake engineering
- Environmental engineering
- Geotechnical engineering
- Structural engineering
- Surveying
- Transportation engineering
- Forensic engineering
- Municipal or urban engineering
- Control engineering
- Water resources engineering

Building One World Trade Center

Images: Wikipedia Commons
Current Definitions of *Privacy Engineering*?

**NIST NISTIR 8062**

- “A specialty discipline of systems engineering focused on achieving freedom from conditions that can create problems for individuals with unacceptable consequences that arise from the system as it processes PII.” *An Introduction to Privacy Engineering and Risk Management in Federal Systems*“
  

**PRIPARE**


-
Further Definitions

MITRE

• “Privacy Engineering is a systemic, risk-driven process that operationalizes the privacy by design (PbD) framework within IT systems.” The privacy engineer or a designated individual is the individual that performs privacy engineering.”  

ISO 27550 Privacy Engineering Working definition

• "Privacy engineering deals with the integration of privacy in the engineering of information and communication technology (ICT) systems."
Privacy Engineering Resources

- Privacy Engineering Models/Methodologies
- Privacy Engineering Publication
- Risk Management Privacy Engineering Methodologies
- Privacy Engineering Automated Tools
- Privacy Engineering Conferences and Workshops
- Privacy Controls Design Strategies, Patterns Libraries
- Privacy Engineering Education and Curricula
- Formal and de-facto standards

Source: “Privacy Engineering...It’s Time to Take the Next Steps towards Standards and Automated Tools,” Gail Magnuson, LLC

ISO/IEC Standards

- ISO/IEC 29100 - a high-level, general organizational, technical, and procedural framework for the protection of PII within ICT systems.
- ISO/IEC 29134 - guidelines for a process on privacy impact assessments (PIA)
- ISO/IEC 29151 which establishes risk management control objectives for Personal Information
- ISO/IEC 27018 - a code of practice for the protection of personal information in public clouds
- Other standards on security and security management relevant to privacy management
Academic Programs/Courses

• Carnegie Mellon University “Master of Science in Information Technology—Privacy Engineering,” one-year graduate program for computer scientists and engineers
  o addressing technology and integrating perspectives that span product design, software development, cyber security, human computer interaction, business and legal considerations.

• Oxford University Department of Computer Science course, February 2019, “Data Security and Privacy,” addressing:
  o **Context:** the changing landscape, privacy, data security and the law
  o **Access control:** theory and practice; mandatory policies; role-based access control; policy languages
  o **Privacy:** balancing privacy and utility; statistical database security; k-anonymity and related techniques; privacy languages
• Johns Hopkins University “Privacy Engineering Course 595.672,” online course, Fall 2018; course objectives:

  o Identify and explain the diverse technology, business and legal rules, domestic and international, that govern how privacy solutions must be engineered.
  o Understand and use an integrated engineering design process for building and governing privacy solutions to meet legal, technology, and business requirements.
  o Acquire and use new tools to create visual data flow models expressing use cases and requirements for privacy solutions.
Common Elements

- Privacy Engineering as a discipline can analyze, document, visualize and provide integrated *technical and business process solutions* to data protection requirements

  - Address the delivery of data protection/privacy principles, regulations, and business policies
  - Set in the context of a rigorous privacy management analysis specific to a use case/implementation
  - Extensible to associated use cases
  - Translated into Privacy Controls and Specific Requirements
  - Defined in required privacy services and functionality
  - Implemented in technical and procedural mechanisms
  - Using visualisation tools
  - Reporting tools that allow a privacy engineer to demonstrate compliance
Important Common Objective: Managing the Complexity of Data Privacy/Protection

• A system is a combination of interacting elements organized to achieve one or more stated purposes. The interacting elements that compose a system include hardware, software, data, humans, processes, procedures, facilities, materials, and naturally occurring entities [ISO/IEC/IEEE 15288]

• To deliver privacy in IT systems, privacy control requirements must be functionally built into the “interacting elements that compose a system.”

Why a Standardized Methodology to Support Privacy Engineering?

- a disciplined and comprehensive, and reusable analytic methodology supporting engineered compliance and accountability
- management of layers of detail for a complete analysis
- support for an automated tool that retains data/linkages to minimize manual work and speeds analysis of linked use cases
- Access by all relevant subject matter experts, their disciplines and tools
- interfaces with other external standards and practices (e.g. DPIAs/PIAs) for efficiency and accuracy
Supports Iterative Analysis, SDLC Management and Reporting

- Changing application/system requirements and conditions are a constant reality
- A methodology that supports Iterative analysis enables privacy engineers to integrate all aspects of privacy delivery, end to end and across domains - resulting in a comprehensive engineered design
- As each analytic task is executed, data are categorized and linkable
- Supports updates, new categories, detail and annotations – reusability
- Documents how given mechanisms meet their control requirements - demonstrates accountability and regulatory compliance
- Make use of existing tools to ensure common data collection and reporting
The PMRM Methodology

The PMRM V1.0 CS02 - A methodology and analytic tool developed to:

- enable the structured analysis of “use cases” in which personal information (PI) and PII are used, generated, communicated, processed and stored and erased
  - Support for applications, IoT, Cloud, complex hyper-connected systems, as well as smaller components of a system
- show the linkages among data, data flows, PI, privacy [including security] policies, privacy controls, privacy-enabling Services/ functionality, supporting mechanisms and risk
- Integrate with and support existing privacy standards
- achieve data protection by design requirements and compliance across policy and system boundaries
- support multiple stakeholders

http://docs.oasis-open.org/pmrm/PMRM/v1.0/cs02/PMRM-v1.0-cs02.html
The PMRM Model Reflects the Complexity of Data Protection/Privacy
The PMRM Privacy Management Analysis Methodology is the Analytic Tool Supporting Privacy Engineering
Privacy Management Analysis is complicated
- Multiple Stakeholders
- Overlapping responsibilities
- Policy
- Business Processes
- Technical Functionality
- Risk Management at all levels
- Need for Iterative analyses
PMRM – Privacy Engineering Methodology

Privacy Engineering Generalists

### High Level Privacy Use Case Analysis

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

### Detailed Privacy Use Case Analysis

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

### PI in Use Case Systems

<table>
<thead>
<tr>
<th>System 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Incoming/Internally Generated/Outgoing</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>System …n</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incoming/Internally Generated/Outgoing</td>
</tr>
</tbody>
</table>
Operational Privacy Control Requirements

| Inherited | Internal | Exported |

Services Required for Operationalized Controls

| Agreement | Usage | Validation | Certification | Enforcement | Security | Interaction | Access |

Technical and Process Functionality and Mechanisms

Risk Assessment

Privacy Engineering Specialists

Iterative Process
## PMRM Service Descriptors

<table>
<thead>
<tr>
<th>Core Policy Services</th>
<th>Privacy Assurance Services</th>
<th>Presentation &amp; Lifecycle Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agreement</td>
<td>Validation</td>
<td>Interaction</td>
</tr>
<tr>
<td>Usage</td>
<td>Security</td>
<td>Access</td>
</tr>
<tr>
<td></td>
<td>Certification</td>
<td></td>
</tr>
<tr>
<td>PMRM SERVICE</td>
<td>SERVICE FUNCTIONALITY</td>
<td>INFORMAL DEFINITION</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>AGREEMENT</td>
<td>Defines and documents permissions and rules for the handling of PI based on applicable policies, data subject preferences, and other relevant factors; provides relevant Actors with a mechanism to negotiate, change or establish new permissions and rules; expresses the agreements such that they can be used by other Services</td>
<td>Manage and negotiate permissions and rules</td>
</tr>
<tr>
<td>USAGE</td>
<td>Ensures that the use of PI complies with the terms of permissions, policies, laws, and regulations, including PI subjected to information minimization, linking, integration, inference, transfer, derivation, aggregation, anonymization and disposal over the lifecycle of the PI</td>
<td>Control PI use</td>
</tr>
<tr>
<td>VALIDATION</td>
<td>Evaluates and ensures the information quality of PI in terms of accuracy, completeness, relevance, timeliness, provenance, appropriateness for use and other relevant qualitative factors</td>
<td>Ensure PI Quality</td>
</tr>
<tr>
<td>CERTIFICATION</td>
<td>Ensures that the credentials of any Actor, Domain, System, or system component are compatible with their assigned roles in processing PI and verifies their capability to support required Privacy Controls in compliance with defined policies and assigned roles.</td>
<td>Ensure appropriate privacy management credentials</td>
</tr>
<tr>
<td>ENFORCEMENT</td>
<td>Initiates monitoring capabilities to ensure the effective operation of all Services. Initiates response actions, policy execution, and recourse when audit controls and monitoring indicate operational faults and failures. Records and reports evidence of compliance to Stakeholders and/or regulators. Provides evidence necessary for Accountability.</td>
<td>Monitor proper operation, respond to exception conditions and report evidence of compliance where required for accountability</td>
</tr>
<tr>
<td>SECURITY</td>
<td>Provides the procedural and technical mechanisms necessary to ensure the confidentiality, integrity, and availability of PI; makes possible the trustworthy processing, communication, storage and disposition of PI; safeguards privacy operations</td>
<td>Safeguard privacy information and operations</td>
</tr>
<tr>
<td>INTERACTION</td>
<td>Provides generalized interfaces necessary for presentation, communication, and interaction of PI and relevant information associated with PI, encompassing functionality such as user interfaces, system-to-system information exchanges, and agents</td>
<td>Information presentation and communication</td>
</tr>
<tr>
<td>ACCESS</td>
<td>Enables 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, corrections or deletion for their PI</td>
<td>View and propose changes to PI</td>
</tr>
</tbody>
</table>
PMRM Use Case Analysis Development Architecture
PMRM Individual Use Case Exemplar Architecture

Use Case Executive Sponsors selects

Use Case Stakeholders & Experts to define

Use Case Definition, Inventory & Relevant Studies

Privacy Conformance Criteria (Policies and Requirements)

Participants, Domains, Business Processes, Systems, Touch Points and Personal Data;

Source:
Gail Magnuson, PMRM Technical Committee
Privacy Conformance Criteria and Controls

Privacy Conformance Criteria

Inherited Privacy Controls

Privacy Controls

Risk Assessment

Functions & Services Definition for Privacy Controls

Mechanisms

Exported Privacy Controls

Packaged into Business Processes and Controls

Source: Gail Magnuson, PMRM Technical Committee
Use Case Operations

Use Case Operations Defines

Participants

Domains

Business Processes

Systems

Touch Points

Personal Data

All Packaged into Domains defining Incoming, Generated and Outgoing Personal Data

Including the Privacy Mechanisms designed to implement Privacy Controls

Risk Assessment

Source: Gail Magnuson, PMRM Technical Committee
Use Case Executive Sponsors selects

Use Case Stakeholders & Experts to define

Use Case Definition, Inventory & Relevant Studies

Privacy Conformance Criteria (Policies and Requirements)

Participants, Domains, Business Processes, Systems, Touch Points and Personal Data;

Privacy Conformance Criteria

Inherited Privacy Controls

Privacy Controls

Risk Assessment

Functions & Services Definition for Privacy Controls

Mechanisms

Packaged into Business Processes and Controls

All Packaged into Domains defining Incoming, Generated and Outgoing Personal Data

Including the Privacy Mechanisms designed to implement Privacy Controls

Risk Assessment

Source:
Gail Magnuson, PMRM Technical Committee
Two Follow-on PMRM Projects

- PMRM “Quick Start Guide” – to simplify utility of the PMRM Methodology for practitioners
  - drafts now under review by PMRM TC

- Privacy Management Analysis (PMA) Open Source Tool Project
Open Source Privacy Management Analysis Tool Project Based on PMRM

Content developed for EIC 2017 by ChiljonJanssen
Principal Software Engineer
chiljon.janssen@gmail.com
Architecture of PMRM PMA Tool

Stakeholders provide analytic inputs for analysis

Content provided by Chiljon Janssen
Across Organizations/Domains

Content provided by Chiljon Janssen
Building Data and Datasets for Integration, Analysis and Reporting

Content provided by Chiljon Janssen
Capturing Increasing Complexity

Content provided by Chiljon Janssen
Objectives:

- Capture, integrate and build all analytic data associated with use case
- Enable iterative add, deletes, links
- Visualisation of all PMRM elements – such as data flows, control requirements etc.
- Click on objects to drill into details
- Support multiple data capture options: API’s for Tablet-collected data, spreadsheet data, structured and unstructured data, etc.

Content provided by Chiljon Janssen
To View The Complete Video Presentation

• Chiljon Janssen: “Demonstrating a Software Solution to Support GDPR Privacy Delivery and Compliance” - Building a Code Base for an Open Source Privacy Management Analysis Tool

• Videos available on Youtube
  o OASIS Open Standards
  o https://youtube.com/user/OASISopen/playlists

• Playlist: Data Protection-Privacy-IDTrust
PMA Tool Roadmap

Design and development of the User Interface that allows for data entry:

• Easy
• Understandable
• Support for structuring of data
• Support of iterative PMA process
• Design and development of the API layer:
  • Standardization
  • Extend and further develop the Visualization Engine
• import / export options
PMRM Open Source Privacy Management Analysis Tool

- **PMRM TC Documents-resources:**

- **Software Implementation Presentation by Chiljon Janssen, EIC 2017, Munich**
Outline of approach:

• Design and develop specifications for an open source PMRM-Privacy Management Analysis tool(s) using an agile approach

• To accomplish this the PMRM TC seeks input from interested academic institutions and practitioners

• Goal is to achieve a Minimum Viable Product (MVP) that allows for basic support of the PMRM methodology, initially focusing on the areas where most benefit and added value are expected:
  
  o visualization of relationships
  o data entry and data acquisition
  o data persistence and data integration

• A small amount of OASIS funding may be available to seed for this work.
Closing Thoughts

• Structured privacy management analysis of applications and systems is essential
• Integration of “macro” with “micro” – include all relevant stakeholders
• Accept that this effort is iterative and time-consuming
• A robust analysis is complex and hard
• Delivering valuable analytic products will require automated tools to overcome time and effort barriers and support scalability
• Academic focus – pure and applied research can be invaluable in assured privacy management a reality
For More Information

Privacy Engineering…It's Time to Take the Next Steps towards Standards and Automated Tools by Gail Magnuson, LLC

OASIS Privacy Management Reference Model and Methodology (PMRM)
http://docs.oasis-open.org/pmrn/PMRM/v1.0/cs02/PMRM-v1.0-cs02.pdf

OASIS Privacy by Design Documentation for Software Engineers (PbD—SE)
http://docs.oasis-open.org/pbd-se/pbd-se/v1.0/csd01/pbd-se-v1.0-csd01.pdf

Companion committee Note:
http://docs.oasis-open.org/pbd-se/pbd-se-annex/v1.0/cnd01/pbd-se-annex-v1.0-cnd01.html

OASIS Online GDPR/PMRM/Privacy Engineering Workshop Videos
https://www.youtube.com/watch?v=afKSgq-MURg&list=PLaYKtNo_BitYphf94ctTgjS40-sTDMDCS
Thank You

john.sabo711@yahoo.com

www.oasis-open.org