On Parametric Obligation Policies:
Enabling Privacy-aware
Information Lifecycle Management in Enterprises

IEEE Policy Workshop 2007
Marco Casassa Mont
(marco.casassa-mont@hp.com)
Hewlett-Packard Labs
Presentation Outline

• Background on Privacy Obligation Management
• Addressed Problem and Related Work
• Scalable Obligation Management
• Conclusions
Presentation Outline

• Background on Privacy Obligation Management
• Addressed Problem and Related Work
• Scalable Obligation Management
• Conclusions
Privacy: Impact on Users and Enterprises

Privacy Legislation
(EU Laws, HIPAA, COPPA, SOX, GLB, Safe Harbour, ...)

Customers’ Expectations

Internal Guidelines

Applications & Services

Personal Data

Regulatory Compliance

Customers’ Satisfaction

Positive Impact on Reputation, Brand, Customer Retention

People

Enterprise

Positive Impact on Reputation, Brand, Customer Retention
Privacy Obligation Policies

- **Privacy Obligations** are Policies that describe **Duties** and **Expectations** on how Personal Data (PII) Should be Managed in Enterprises (e.g. Data Deletion, Retention, Notifications, Data Transformation, …)
- They dictate **“Privacy-aware (Identity) Information Lifecycle Management”**
- They can be defined by Privacy Laws, Data Subjects (Users’) Preferences and Enterprise Guidelines
Privacy Obligations: A Complex Topic …

Obligation Constraints:
- Notice Requirements
- Enforcement of opt-in/opt-out options
- Limits on reuse of Information and Information Sharing
- Data Retention limitations …

“Notify User via e-mail If his/her Data is Accessed”
“Delete Data XYZ after 7 years”
Presentation Outline

• Background on Privacy Obligation Management
• Addressed Problem and Related Work
• Scalable Obligation Management
• Conclusions
Key Research Problems

• How to Help Enterprises to Handle Obligation Policies:
  – How to Represent Privacy Obligations?
  – How to “Stick” them to Data?
  – How to Manage, Enforce and Monitor Them?
  – How to Leverage Current Identity Management Solutions?

• How to Achieve this in a **Scalable Way**, with **Very Large Sets** of Managed Personal Data (>100K, usually million of records ...)
Technical Work in this Space (Privacy Obligation Management)

- **P3P (W3C):**
  - Definition of User’s Privacy Expectations
  - Explicit Declaration of Enterprise Promises
  - No Definition of Mechanisms for their Enforcement

- **Data Retention Solutions, Document Management Systems, Ad-hoc Solutions for Vertical Markets**
  - Limited in terms of expressiveness and functionalities.
  - Focusing more on documents/files not personal data

- **IBM Enterprise Privacy Architecture, EPAL, XACML …**
  - No Refined Model of Privacy Obligations
  - Privacy Obligations Subordinated to AC. Incorrect …
  - No Focus on Scalability Issue …
Presentation Outline

• Background on Privacy Obligation Management
• Addressed Problem and Related Work
• Scalable Obligation Management
• Conclusions
Our Approach (EU PRIME Project)

- Privacy Obligations are "First-Class Entities": No Subordination to Access Control/Authorization View
  → Explicit Representation, Management and Enforcement of Privacy Obligation Policies

- Allow Users to Express their Privacy Preferences that are Mapped into Enterprises’ Obligation Policies

- Scalability to Large data sets (>100K) by means of Parametric Obligation Policies

- Provide a Solution to Enterprises to Automate the Management and Enforcement of Privacy Obligation Policies
Our Model: Obligation Management Framework [1/2]
Our Model: Obligation Management Framework [2/2]
Parametric (Privacy) Obligation Policies

- **Parametric Obligation**: contains a “parametric definition” of Obligation’s Target, Events, Actions (and On-Violation Actions …)
- Structure based on Predefined Obligation Templates. Once Instantiated, it contains References to Personal Data and Privacy Preferences
- References are Resolved at Runtime by OMS

---

**Parametric Obligation (Reactive Rule)**

FOR: Target

WHEN Events(Refs)

THEN EXECUTE [Actions(Refs)]

ON VIOLATION:

EXECUTE [Violation-Actions(Refs)]
Parametric Obligation: “Simple” XML-based Example

Target with the references description of the databases

Target with

<br><br>

Timeout Event using the explicit reference

Actions involving the Notification and Data Deletion

On Violation Actions using the direct value

FOR ALL TARGETED PII DATA + RELATED_PREFS
WHEN Deletion_Time (Ref)
THEN EXECUTE [DELETE CreditCard (Ref) & Notify (Ref)]
ON VIOLATION: EXECUTE [Notify(admin)]

15 13 June, 2007
Parametric Obligation: Working with References …

- **Target**
  - Data Model Definition (PII Data, Preferences, etc.)
  - Uses Alias to identify each data model

- **Events**
  - Uses the “Alias + References” to get the data to trigger the action

- **Actions**
  - Uses the “Alias + References” to acquire additional information to enforce the action
Obligation Processing Workflow (Run-time ...)

External Events Happen

- Identify Relevant Personal Data and Privacy Preferences

Parametric Obligation Policy

- Target
- Events
- Actions
- OnViolation Actions

Solving the Events References by building dynamically SQL queries

Scalable Obligation Database

- Update Stateful Events

Event Trigger a parametric obligation on a given piece of data?

- Yes
- No

Enforce the Actions by solving the Actions References building dynamical SQL queries
Scalable OMS High-Level Architecture

Current Status
- Full working prototype. Tested with Large data sets (>100K)
- Integrated with HP OpenView Identity Management Solution (HP Select Identity)
- Working on further Tests and Analysing them …
Presentation Outline

• Background on Privacy Obligation Management
• Addressed Problems and Related Work
• Scalable Obligation Management

• Conclusions
Conclusions

- Privacy Management is Important for Enterprises
- Need to Provide Scalable Solutions to Handle Privacy Obligations
- Proposed a Scalable Obligation Management Framework and Solution
  - Explicit Modelling and Management of Obligation Policies
  - Concept of Parametric Obligation Policies
- It Works!! Handling Obligations on Large set of PII Data (>100k)
- Collecting Test Results and more Formal Analysis …
- R&D Work in Progress:
  - Stickiness of Obligation Policy to Data (subject to change of locations)
  - Management of Obligation Policies in Federated Identity Management Contexts
  - …