# Privacy Data Envelops for Moving Privacy-sensitive Data

## Keeping Control over the propagation of your personal data

*Armen Aghasaryan, Stéphane Betgé-Brezetz, Marie-Pascale Dupont, and Guy-Bertrand Kamga*

Alcatel-Lucent Bell Labs France

# Monitoring the Privacy sensitive data across a network

## Motivation

Today privacy sensitive data are not just stored at central servers or at end-devices, but continuously travel across a network of interconnected applications: various social networks, content sharing and communication tools.

Users have increasingly strong concerns about their personal data "traveling" over such a global infrastructure without having means to control their disclosure.

## Problem definition

Provide a mechanism *to monitor* the lifecycle of privacy-sensitive data entities and *to notify* the interested parties on the application of the appropriate privacy rules & strategies.

## The proposed approach

Identify the privacy-sensitive information entities and embed them in a Privacy Data Envelop allowing:

- the data owner or the administrator to specify which actions are authorized on each of this these data entities, possibly keeping these entities within an hierarchical structure
- the owner or administrator to be informed of actions executed with this data entities,
- (optionally) a software client to enforce these privacy policies set by the data owner or his representative.

# Privacy Data Envelop (PDE)

## definition

### Privacy-sensitive entities (or sensitive entities)

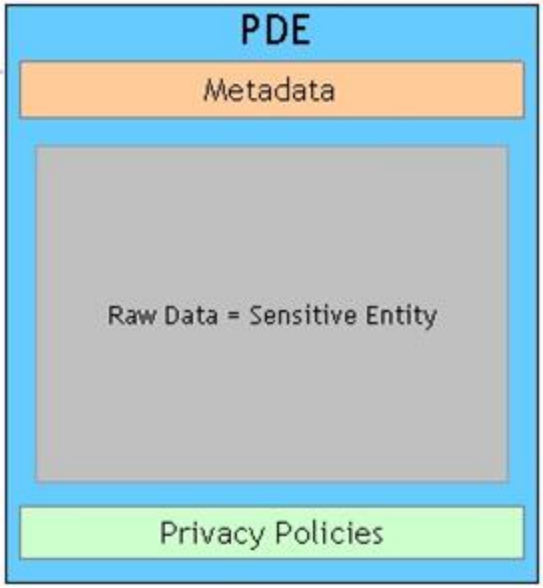
define the parts of raw data that are different from the privacy point of view; each such part is characterized by its individual properties.

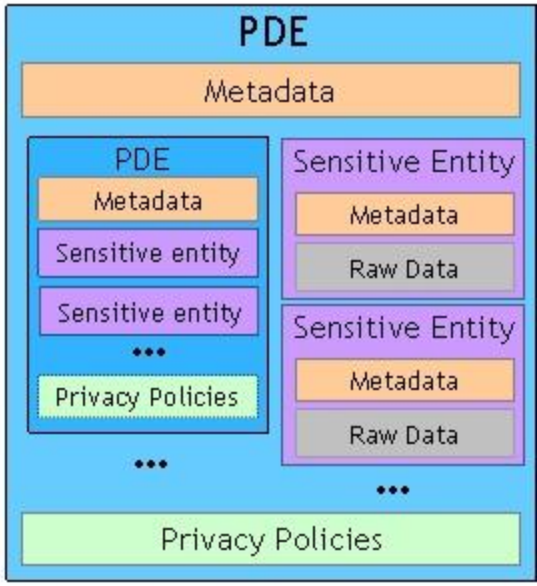
### Properties (or metadata)

specify some semantics on the respective data entities, e.g. the data category, owner, date of creation/publication.

### Privacy policies

indicate the authorized actions (e.g., access control, data handling and disclosure policies) and which obligations must be fulfilled (e.g., data deletion after a certain time period, notification or consent request to the owners).




***Composite PDE***

# Privacy Data Envelop (PDE)

## sensitive data entities and the privacy-related properties

| *Privacy-sensitive information entities* | *Metadata* |
|---|---|
| **User profile**<br>- demographic data (age, sex, marital status, …)<br>- different identifiers (names, social security, e-mail address, credit card number, …)<br>- preferences (video or music preferences, …)<br>- group affiliations<br>-… | **User profile properties**<br>- Category<br>- TTL (time-to-live)<br>- Exposure level<br>- Owner |
| **Messages (intentional)**<br>- e-mail messages (including attachments: forwarded/replied message, or other types of files)<br>- IM<br>- User-generated multimedia contents<br>- … | **Message properties**<br>- Category<br>- TTL<br>- Exposure level<br>- Owner<br>- Sender<br>- Receiver<br>- Subject |
| **Interaction traces (residual)**<br>- purchase logs<br>- click-trough traces<br>- video streaming logs<br>- … | **Interaction traces properties**<br>- Category<br>- TTL<br>- Exposure level<br>- Owner<br>- Object (interacted with) |

# Privacy Data Envelop (PDE)

## categories of privacy policies

### System-wise configuration of default properties

*If type=email then*

*exposureLevel=1*

*TTL = unlimited*

*If type=IM then*

*exposureLevel=2*

*TTL = 12 hours*

### Exposure level interpretation policies

*If exposureLevel = 0 then*

*The data are accessible without any restriction*

*If exposureLevel = 1 then*

*The data are accessible only to owner and receiver*

*The PDE properties are accessible without restriction*

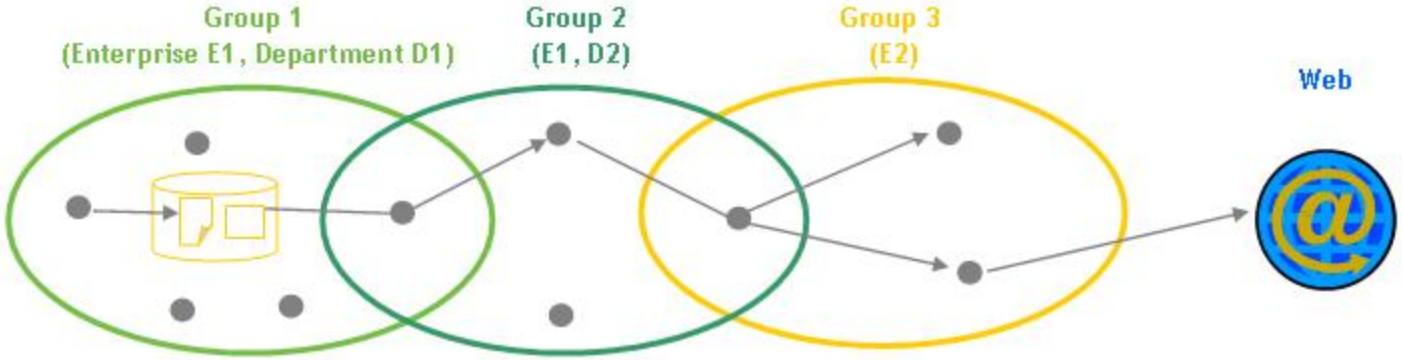
### Individual configuration of PDE properties

*If owner = Mr X and type=email then*

*exposureLevel = 3*

# Privacy Data Envelop (PDE)

## examples of group privacy policies in enterprise context




**Group Privacy Policy 1 (sender inside the group 1):**

*If sender* ∈ E1 ∧ D1, *then check recipient*

*If recipient* ∈ E1\D1, *then authorize sending and keep log;*

**Group Privacy Policy 2 (sender inside the group 2):**

*If the sender* ∈ E1\D1, *then check recipient*

*If recipient* ∈ E1-partners, *then ask consent from the original sender, wait time T*

*If positive consent received, then authorize sending under conditions*

*Else deny sending*

**Group Privacy Policy 3 (sender inside the group 3):**

*If the sender* ∈ E1-partners, *then check recipient*

*If recipient* ∉ E1 ∧ E1-partners, *then ask consent from all* D1 *members, wait time T*

*If all positive consent received, then authorize sending under conditions*

*Else deny sending*

# Conclusions

## Guiding users' privacy-aware behavior

Provide for a data structure for Privacy Data Envelops (PDE) that can be integrated with the existing communication tools (e.g. e-mail, IM, Wiki, Blog, or SN apps)

- Definition of different data properties and policy categories that can be carried by a PDE
- Realization of a mechanism for PDE communication between different processing entities

## Industry-focused API specification

Provide application programmers a standard for guiding the development of PDE-aware applications

- Facilitate the development of various add-ons over existing communication tools

## Security and enforcement

Investigate security mechanisms that enforce PDE policies

- Time-to-live enforcement
- Data encryption and signing

## Expected Benefits

Increase trust in privacy sensitive applications

Promote a privacy-responsible behaviour within a user/application network

- Reduce risk of data misuse and user mistakes in complex operations