PRIPARE

PReparing Industry to Privacy-by-design by supporting its Application in REsearch

Teaching Privacy-by-design

Some issues

Fanny Coudert, Daniel Le Métayer

ICRI – KU Leuven – iMinds, INRIA

fanny.coudert@law.kuleuven.be, daniel.le-metayer@inria.fr

First issue

WHAT IS PRIVACY BY DESIGN?

PbD: enforcing privacy

- Approach to privacy that uses **technology as a way to enforce legal obligations**

- **Goal**: **identify and mitigate privacy risks** from the very beginning, when the means for the processing of data are determined and throughout the lifecycle of the processing

“By design”?

“By design” suggests the initial phase in the life cycle of a product but consideration for privacy should not be limited to this phase:

it should cover all the life cycle of a product.

- Before design: PIA
- After design: accountability, reaction in case of privacy breach, etc.)

“By design”?

“By design” suggests technical considerations but technology is intimately related to organization, and also to economy, to law.

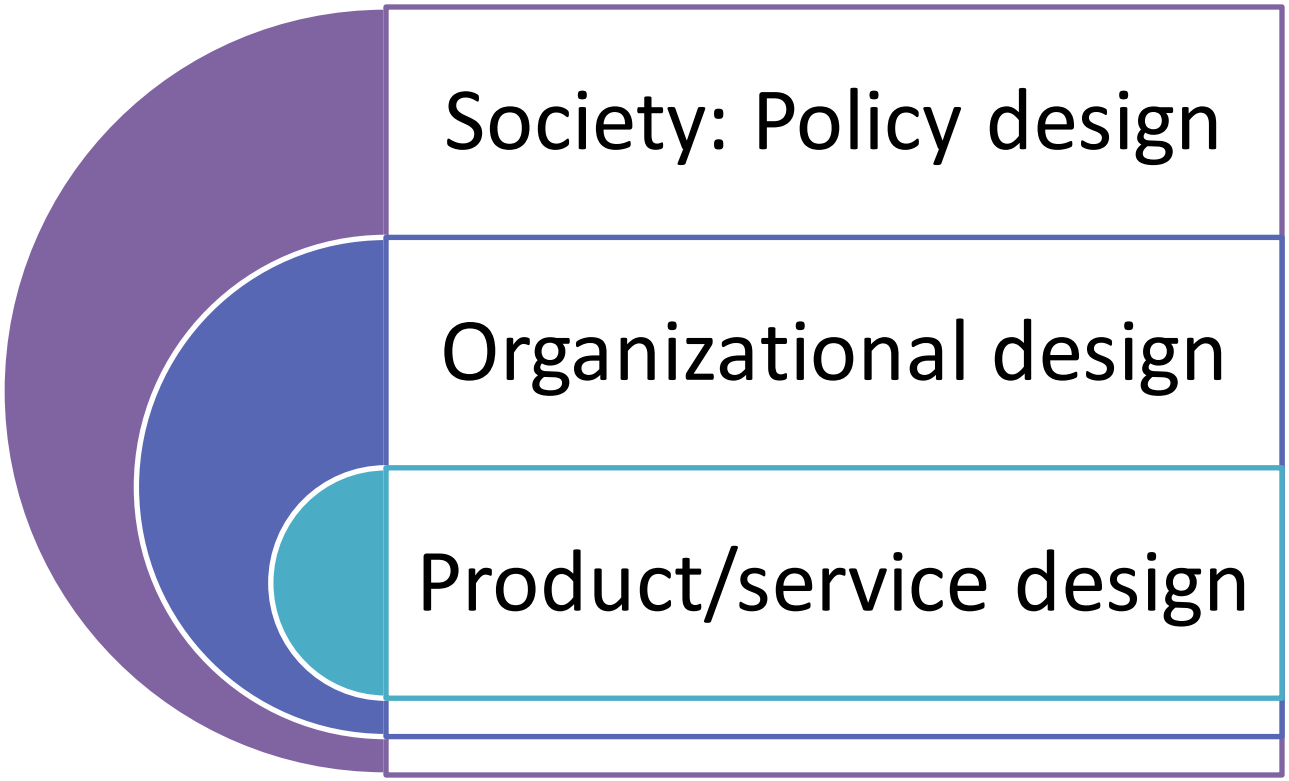
Towards a holistic approach to PbD?

A holistic approach to PbD?

Privacy by Design as a holistic concept that may be applied to operations throughout an organization, end-to-end, including its information technology, business practices, processes, physical design and networked infrastructure

(Resolution on PbD, 32nd International Conference of Data Protection and Privacy Commissioners, 2010)

A holistic approach to PbD?



Creating a culture of privacy

Draft Regulation

The principle of data protection by design require data protection to be embedded within the entire life cycle of the technology, from the very early design stage, right through to its ultimate deployment, use and final disposal. This should also include the responsibility for the products and services used by the controller or processor.

(Recital 61)

Draft Regulation

The protection of the rights and freedoms of data subjects with regard to the processing of personal data require that appropriate technical and organizational measures are taken, both at the time of the design of the processing and at the time of the processing itself, to ensure that the requirements of this Regulation are met.

(Recital 61)

Issue in PbD training

Where should we draw the line in a PbD training?

How do all these dimensions articulate ?

Should we set up targeted PbD courses (for decision makers, for engineers, for operators, data protection officers, lawyers, etc.)?

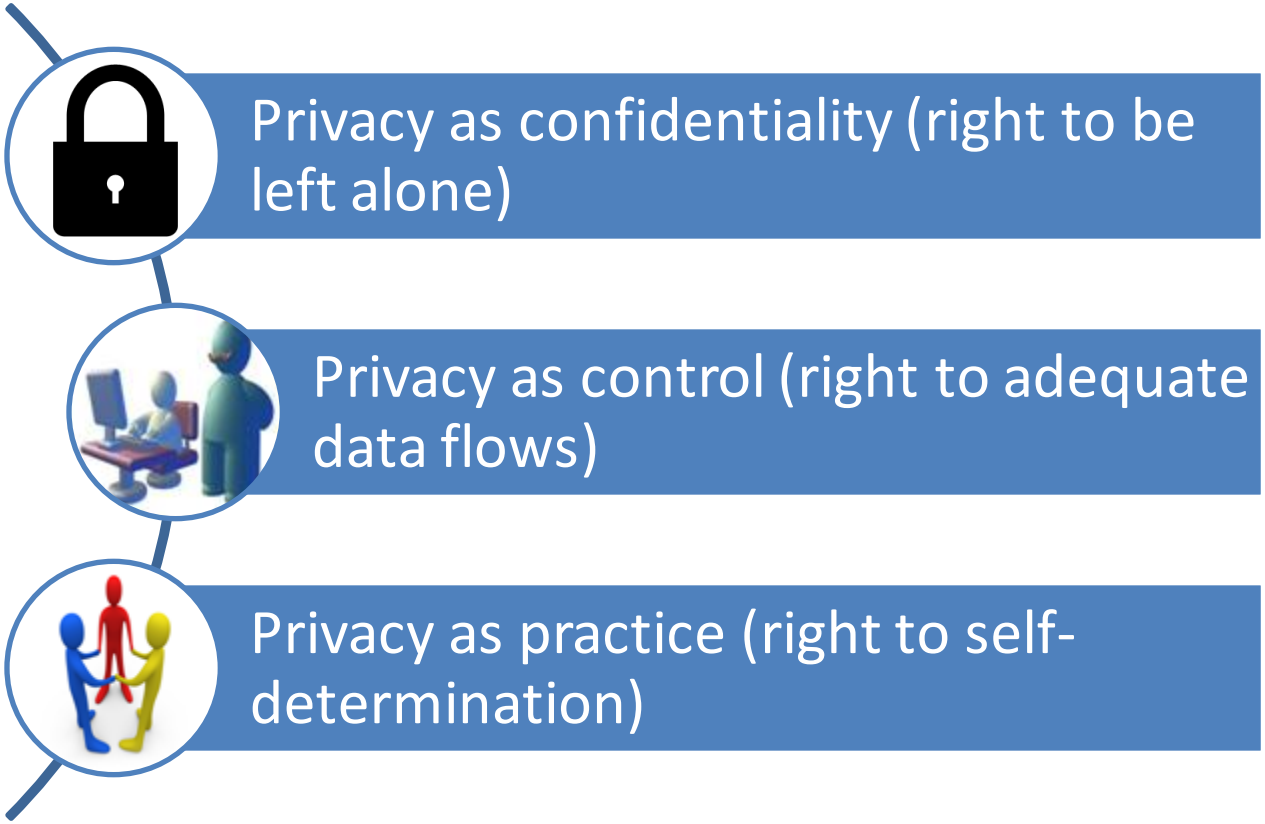
Second issue

WHAT HAS TO BE ACHIEVED?

Challenges

- The different of dimensions of privacy
- The variety of stakeholders involved
- The variety of other (sometimes conflicting) requirements that designers have to take into account (functional, usability, performances, etc.)

Different dimensions of privacy



Variety of stakeholders

Example: Two types of security system designers.

- **System owners** (requirement level):
  - Responsible for system's requirements
  - Obligation to comply with regulation
  - Protection of goods and persons
  - Political motivation: public satisfaction / privacy optimization
- **Developers** (realization level)
  - Compliance with requirements at minimum cost
  - Within the frame of applicable regulations
  - Optimization of long-term fruitful collaboration
  - Differenciation towards other actors on the market

Conflicting requirements

- *System design functionality vs. Privacy*

"A coherent system of ICT measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, all without losing functionality of the information systems " (EC, Opinion on PETs, 2007)

- *Privacy vs. other competing values (e.g. security, growth in a data driven economy, etc)*

Issues in PbD Training

Need to teach ways to:

- Define precisely all requirements and tools to reason about them
- Deal with different privacy risks

Third issue

HOW CAN IT BE ACHIEVED?

Which tools for which purposes?

"Privacy by design" involves the use of Privacy Enhancing Technologies (but goes beyond that) and a variety of PETs are available today (many more tomorrow)

- How to select the appropriate combination of tools to address the needs of a particular system ?

- How to combine them together and with further organizational or legal measures ?

Issues in PbD training

Need to **teach strategies**:

- To go from requirements to architectures, products and procedures
- To set up the right organizational structure that will support/ promote legal compliance

Fourth issue

WHAT ARE THE LIMITATIONS?

Limits of the PbD approach

Privacy by Design is not a bullet proof solution to enforce the legal framework

Raise awareness of all stakeholders on the advantages and limits of the process

Sustain continuous awareness of all stakeholders (and above all the subject himself) about privacy: Foster a culture of privacy at organizational/societal level

PRIPARE

PReparing **I**ndustry to **P**rivacy-by-design by supporting its **A**pplication in **RE**search

Thank you for your attention

Questions?

Website: www.pripareproject.eu

Project Co-ordinator
Antonio Kung (Trialog)

Technical Co-ordinator
Christophe Jouvray (Trialog)