



Privacy by Design: a Matter of Choice

Daniel Le Métayer

CPDP, Brussels, January 2009

INSTITUT NATIONAL
DE RECHERCHE
EN INFORMATIQUE
ET EN AUTOMATIQUE



Privacy by Design

Main Challenges:

1. First and foremost: political

Need to restore the balance of power

2. Secondly: technical (law and information technology)

Need to cope with both generality and particularity

Privacy by Design: What do we mean ?

1. Some examples of privacy by design:

- User friendly interface for data subjects to exercise their rights (request for access, rectification, deletion, etc.)
- Electronic commerce protocol which does not require one actor (e.g. the seller) to get access to all the information disclosed by the customer
- Electronic health record system with personal data stored on a smart card under the control of the patient rather than on a central server
- Access control system using anonymous credentials rather than identity

2. Privacy by design is not just PETs

3. The first obstacle to privacy by design is not technical, it is political (matter of choice)

Political Choice

Today:

1. Non privacy by design (deliberate infringement)
2. Non privacy by non design (lack of care)
3. Non privacy by bad design (lack of competency)

Position:

- **First step:** Avoid 1 and 2 (political choices)
- **Second step:** Avoid 3 (technical choices)

Avoiding non privacy by bad design is a more realistic goal than trying to achieve privacy by design (no bullet proof solution: technology alone cannot solve the problem)

Technical Challenges

Privacy is both

- **Very general** : fundamental right, protects social and public life as well as individual life, etc.
- **Very personal** : different perceptions among individuals, requires room for individual choices

Reconciling generality and individuality is a challenge:

- **For law** : where to draw the line between the protection of the weakest and the right to individual freedom ?
- **For technology** : the design must allow for a high level of parameterization or customization without encouraging individuals to make choices that they do not understand or to go systematically for the less protective options

From a vicious circle to a virtuous circle

- Computer scientists :

- **User-friendliness** and proper information to the data subject are more important than highly sophisticated functionalities
- **Transparency** tools are as important as obscurity tools, **a posteriori** is as important as a priori, : accountability, liability, simple means to exercise the rights of the subject, etc.

- Lawyers, legislators :

- Principles may need to be revisited (where to put the red line) but **effectiveness** is the most important
- Stronger **incentives** are required
- Mandatory and/or voluntary **privacy certification schemes** can be a way to favour the development of privacy by design (need for “**Privacy Profiles**” akin to the “**Security Profiles**” of the Common Criteria for security)
- Accompanying measure: more **publicity about privacy breaches**
- Increase general **awareness**

- Industry:

- Develop **standards**

- Individuals:

Necessary conditions for a real choice

- Awareness
- Proper information
- Range of “non privacy invasive” products and services