



**PI lab**  
Privacy & Identity Lab

Radboud University

TILBURG UNIVERSITY  
Law School

university of groningen

# Privacy Seminar

## Basic Techniques

**Jaap-Henk Hoepman**

Privacy & Identity Lab  
Radboud University  
Tilburg University  
University of Groningen

✉ [jhh@cs.ru.nl](mailto:jhh@cs.ru.nl) // 🌐 [www.cs.ru.nl/~jhh](http://www.cs.ru.nl/~jhh) // 📝 [blog.xot.nl](http://blog.xot.nl) // @xotoxot

1

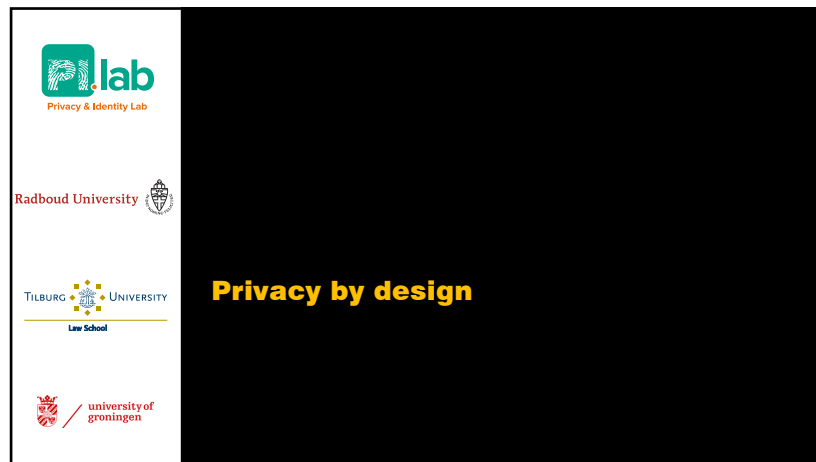


## Agenda

- **Privacy by Design**
  - Principles
  - Privacy Design Strategies
- **Privacy Enhancing Technologies I**

Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques

2



**PI lab**  
Privacy & Identity Lab

Radboud University

TILBURG UNIVERSITY  
Law School

university of groningen

# Privacy by design

3



## Privacy by design

- **Protect privacy when developing new technology:**
  - From concept...
  - ... to realisation

Throughout the system development cycle

- **Privacy is a quality attribute (like security, performance,...)**
- **Privacy by design is a process!**


Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques

4



5

**Common engineering misconceptions #1**


0/1 vs. 

Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques

6

6

**Common engineering misconceptions #2**

**Data controller =** 

Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques

7

7

**Common engineering misconceptions #3**

**Privacy = Data minimisation**

Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques

8

8

## Personal data?

(1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

- **So...**
  - Name
  - Social security number
  - Email address
- **But also...**
  - License plate
  - IP Address
  - Likes
  - Tweets
  - Search terms

Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques 9


9

## Aside: what is 'Data Processing'...


Action	Relevant GDPR Personal Data Processing Examples
<b>Operate</b>	Adaptation; Alteration; Retrieval; Consultation; Use; Alignment; Combination
<b>Store</b>	Organisation; Structuring; Storage
<b>Retain</b>	opposite to (Erasure; Destruction)
<b>Collect</b>	Collection; Recording
<b>Share</b>	Transmission; Dissemination; Making Available; opposite to (Restriction; Blocking)
<b>Change</b>	unauthorised third party (Adaptation; Alteration; Use; Alignment; Combination)
<b>Breach</b>	unauthorised third party (Retrieval; Consultation)

Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques 10

10



Radboud University

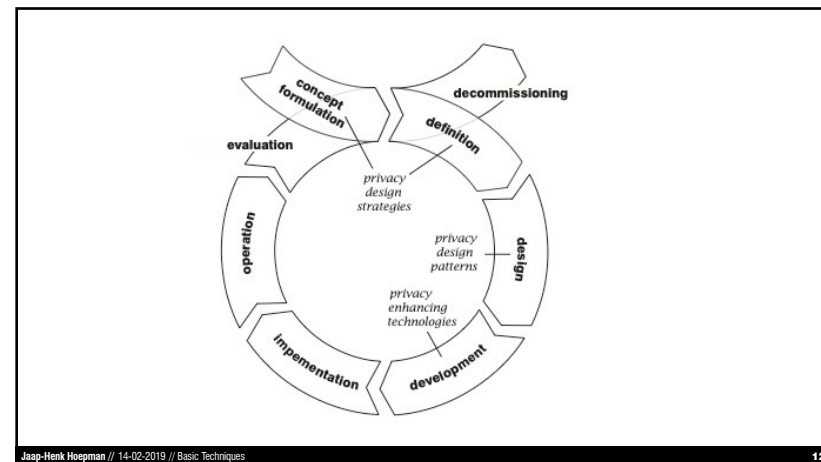


university of groningen

## Eight privacy design strategies

Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques 11

11



12

**Privacy design strategies map fuzzy legal concepts to concrete data protection goals to help control data processing**

Legal norms

(Technical) design requirements

Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques 13

13

**Levels of abstraction**

- **Design strategy**
  - “A basic method to achieve a particular design goal” - *that has certain properties that allow it to be distinguished from other basic design strategies*
- **Design pattern**
  - “Commonly recurring structure to solve a general design problem within a particular context”
- **(Privacy enhancing) technology**
  - “A coherent set of ICT measures that protects privacy” - *implemented using concrete technology*

Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques 14

14

**Design pattern: example**

Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques 15

15

**Privacy design patterns**

The “Aggregation over time” privacy design pattern

Jaap-Henk Hoepman

Name

Aggregation over time.

[Also Known As]

Summary

Instead of reporting immediately and continuously about resource consumption, a consumer of a resource keeps track of its consumption locally (using a trusted device) and periodically reports on its total consumption (over the last reporting period) to the provider of the resource. This prevents the provider to learn details about when exactly the consumer used the resource, while still informing the provider about the total amount of resources used by each individual consumer. Using *aggregation over time* protects the privacy of the consumer, while still allowing to charge consumers for their resource use (for example).

- **Describes a recurring pattern of communicating components that solve a general problem in a specific context**
  - Summary
  - Context
  - Problem
  - Solution
  - Structure
  - Consequences
  - Requirements
- <http://privacypatterns.org>
- <https://github.com/p4pnl/patterns>

Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques 16

16

### Sources for the design strategies

- **Standards**
  - ISO 29100 Privacy framework
- **Principles**
  - OECD guidelines
  - Fair Information Practices (FIPs)
- **Law**
  - General Data Protection Regulation

Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques 17

17

### Data protection law (core principles)

- **Legitimate Processing Grounds**
  - consent
  - necessity
- **Data Subject Rights**
  - Notification
  - Access
  - rectification
  - object to profiling
- **Data Protection Principles**
  - purpose limitation
  - data minimisation
  - duration of retention
  - accuracy of the data
- **Accountability**
  - risk based-approach
  - transparency of processing
  - data protection by design
  - data protection impact assessment

Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques 18

18

### IT system = essentially a database, so...

The diagram illustrates the transformation of a large database grid into a smaller, more manageable one. On the left, a grid with 'Individuals' on the vertical axis and 'Attributes' on the horizontal axis is shown. Below it are the labels 'minimise' and 'separate'. An arrow points to a smaller grid on the right, with labels 'abstract' and 'hide' below it.

Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques 19

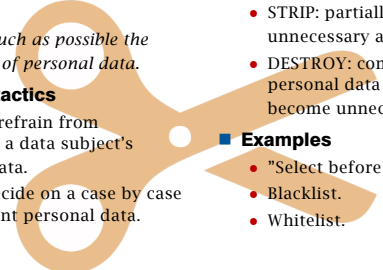
19

The diagram shows the interaction between a 'Data subject' and a 'Data controller'. The 'Data subject' is represented by an 'i' icon and a game controller icon, with arrows labeled 'inform' and 'control'. The 'Data controller' is represented by a shield icon and a document icon, with arrows labeled 'demonstrate' and 'enforce'. In the center, a large grid is being processed through several steps: 'minimise' (scissors icon), 'separate' (curved arrows), 'abstract' (magnifying glass icon), and 'hide' (eye with slash icon).

Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques 20

20

## #1 Minimize



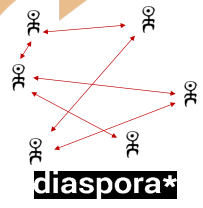
- Definition**
  - Limit as much as possible the processing of personal data.
- Associated tactics**
  - EXCLUDE: refrain from processing a data subject's personal data.
  - SELECT: decide on a case by case only relevant personal data.
- Examples**
  - STRIP: partially remove unnecessary attributes.
  - DESTROY: completely remove all personal data as soon as they become unnecessary.
  - "Select before you collect".
  - Blacklist.
  - Whitelist.

Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques 21

21

## #2 Separate

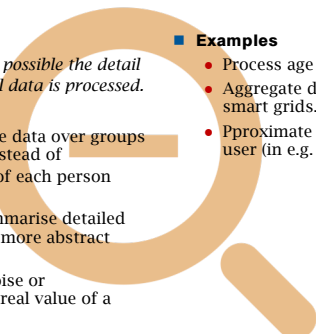
- Definition**
  - Separate the processing of personal data as much as possible, to prevent correlation.
- Associated tactics**
  - ISOLATE: process personal data (for different purposes) independently in (logically) separate databases or systems.
  - DISTRIBUTE: process personal data (for one task) in physically separate locations.
- Examples**
  - Edge computing: process data in the device of the user as much as possible.
  - Peer-to-peer, e.g. a social network.



Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques 22

22

## #3 Abstract



- Definition**
  - Limit as much as possible the detail in which personal data is processed.
- Associated tactics**
  - GROUP: aggregate data over groups of individuals, instead of processing data of each person separately.
  - SUMMARIZE: summarise detailed information into more abstract attributes.
  - PERTURB: add noise or approximate the real value of a data item.
- Examples**
  - Process age instead of date of birth.
  - Aggregate data over time, in e.g. smart grids.
  - Pproximate the real location of a user (in e.g. 10 km<sup>2</sup> resolution).

Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques 23

23

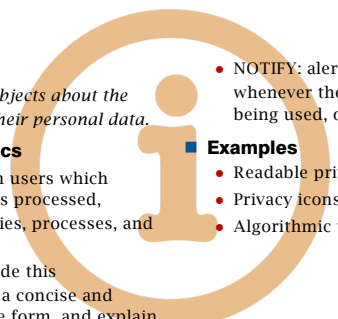
## #4 Hide

- Definition**
  - Prevent personal data to become public or known.
- Associated tactics**
  - RESTRICT: prevent unauthorized access to personal data.
  - ENCRYPT: encrypt data (in transit or when stored).
  - DISSOCIATE: remove the correlation between data subjects and their of personal data.
- Examples**
  - MIX: process personal data randomly within a large enough group to reduce correlation.
  - OBfuscate: prevent understandability of personal data, e.g. by hashing them.
  - Mix networks, Tor.
  - Pseudonimisation.
  - Differential privacy.
  - Access control.
  - Attribute based credentials.

Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques 24

24

## #5 Inform

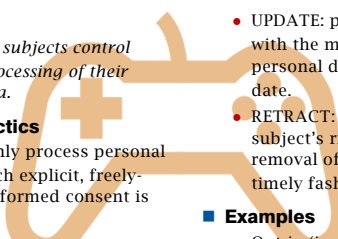


- Definition**
  - Inform data subjects about the processing of their personal data.
- Associated tactics**
  - SUPPLY: inform users which personal data is processed, including policies, processes, and potential risks.
  - EXPLAIN: provide this information in a concise and understandable form, and explain why the processing is necessary.
- Examples**
  - NOTIFY: alert data subjects whenever their personal data are being used, or get breached.
  - Readable privacy policy.
  - Privacy icons.
  - Algorithmic transparency.

Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques 25

25

## #6 Control

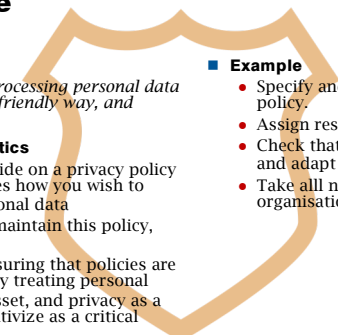


- Definition**
  - Provide data subjects control about the processing of their personal data.
- Associated tactics**
  - CONSENT: only process personal data for which explicit, freely-given, and informed consent is received.
  - CHOOSE: allow data subjects to select which personal data will be processed.
- Examples**
  - UPDATE: provide data subjects with the means to keep their personal data accurate and up to date.
  - RETRACT: honouring the data subject's right to the complete removal of any personal data in a timely fashion.
  - Opt-in (instead of opt-out).
  - Privacy dashboard.

Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques 26

26

## #7 Enforce

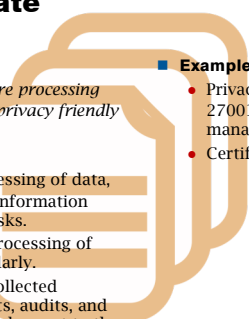


- Definition**
  - Commit to processing personal data in a privacy friendly way, and enforce this.
- Associated tactics**
  - CREATE: decide on a privacy policy that describes how you wish to protect personal data
  - MAINTAIN: maintain this policy, and
  - UPHOLD: ensuring that policies are adhered to by treating personal data as an asset, and privacy as a goal to incentivize as a critical feature.
- Example**
  - Specify and enforce a privacy policy.
  - Assign responsibilities.
  - Check that the policy is effective, and adapt where necessary.
  - Take all necessary technical and organisational measures.

Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques 27

27

## #8 Demonstrate



- Definition**
  - Demonstrate you are processing personal data in a privacy friendly way.
- Associated tactics**
  - LOG: track all processing of data, and reviewing the information gathered for any risks.
  - AUDIT: audit the processing of personal data regularly.
  - REPORT: analyze collected information on tests, audits, and logs periodically and report to the people responsible.
- Example**
  - Privacy management system (cf. ISO 27001 information security management systems).
  - Certification.

Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques 28

28

## Eight privacy design strategies

Data oriented	Process oriented
<ul style="list-style-type: none"> <li><b>MINIMIZE</b> <ul style="list-style-type: none"> <li>• Limit as much as possible the processing of personal data.</li> </ul> </li> <li><b>SEPARATE</b> <ul style="list-style-type: none"> <li>• Separate the processing of personal data as much as possible, to prevent correlation.</li> </ul> </li> <li><b>ABSTRACT</b> <ul style="list-style-type: none"> <li>• Limit as much as possible the detail in which personal data is processed.</li> </ul> </li> <li><b>HIDE</b> <ul style="list-style-type: none"> <li>• Prevent personal data to become public or known.</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li><b>INFORM</b> <ul style="list-style-type: none"> <li>• Inform data subjects about the processing of their personal data.</li> </ul> </li> <li><b>CONTROL</b> <ul style="list-style-type: none"> <li>• Provide data subjects control about the processing of their personal data.</li> </ul> </li> <li><b>ENFORCE</b> <ul style="list-style-type: none"> <li>• Commit to processing personal data in a privacy friendly way, and enforce this.</li> </ul> </li> <li><b>DEMONSTRATE</b> <ul style="list-style-type: none"> <li>• Demonstrate you are processing personal data in a privacy friendly way.</li> </ul> </li> </ul>

Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques 29

29

## Tensions

- Privacy vs. Utility
- Privacy vs. Security
- Privacy vs. Usability
- Data protection vs privacy as norm
- Perception of the data subject vs data controller ininterests

Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques 30

30

## Further information

- G. Danezis, J. Domingo-Ferrer, M. Hansen, J.-H. Hoepman, D. L. Metayer, R. Tirtea, and S. Schiffner. Privacy and Data Protection by Design - from policy to engineering. Technical report, ENISA, December 2014. ISBN 978-92-9204-108-3, DOI 10.2824/38623. <https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design>
- M. Colesky, J.-H. Hoepman, and C. Hillen. A Critical Analysis of Privacy Design Strategies. In 2016 International Workshop on Privacy Engineering - IWPE'16, San Jose, CA, USA, May 26 2016. <http://www.cs.ru.nl/~jhh/publications/iwpe-privacy-strategies.pdf>

Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques 31

31

## Questions?



[Monty Python's Argument Clinic sketch]

[jhh@cs.ru.nl](mailto:jhh@cs.ru.nl)   
 [www.cs.ru.nl/~jhh](http://www.cs.ru.nl/~jhh)   
 [blog.xot.nl](http://blog.xot.nl)   
 twitter: @xotoxot

Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques 32

32