Privacy & Identity Lab

Radboud University

Tilburg University
Law School

university of groningen

# Privacy by Design

## De Toekomst

**Jaap-Henk Hoepman**

Privacy & Identity Lab
Radboud University
Tilburg University
University of Groningen

✉ *jhh@cs.ru.nl* // *www.cs.ru.nl/~jhh* // blog.xot.nl // @xotoxot

# Privacy & Identity Lab

Radboud University Nijmegen

Tilburg University
Law School

TNO

- Samenwerking tussen:
  - Radboud Universiteit – ICIS
  - Tilburg Universiteit – TILT
  - TNO – Security; Strategy & Policy
- Door interdisciplinair werk …
  - Technologie
  - Wet en regelgeving
  - Sociale- en beleidswetenschappen
- … maatschappelijke impact realiseren
  - Identity on the digital stage.
  - Beyond data minimisation.
  - The confluence of the real and the virtual.
  - Understanding and constructing privacy.

# Privacy by design

- Bescherm privacy gedurende het hele (technologische) ontwikkelproces
  - Van concept …
  - … tot en met realisatie.

Gedurende de hele systeem ontwikkelings cyclus

- Privacy is een software quality attribute (net zoals security, performance,…)
- Privacy by design is een proces!

# Waarom privacy by design?

- Het beperkt privacy risico's
  - En dus reputatieschade of herstelkosten
  - "Wat je niet hebt kun je ook niet verliezen"
- Het maakt nieuwe business mogelijk
  - E.g. Zorg, Internet of Things, Quantified self
  - Net zoals security by design internet bankieren mogelijk maakte
- Het is verplicht vanaf 2018!
  - De Algemene Verordening Gegevensbescherming (AVG)


Maar hoe?

# Wat de techneut denkt… #1

0/1

vs.

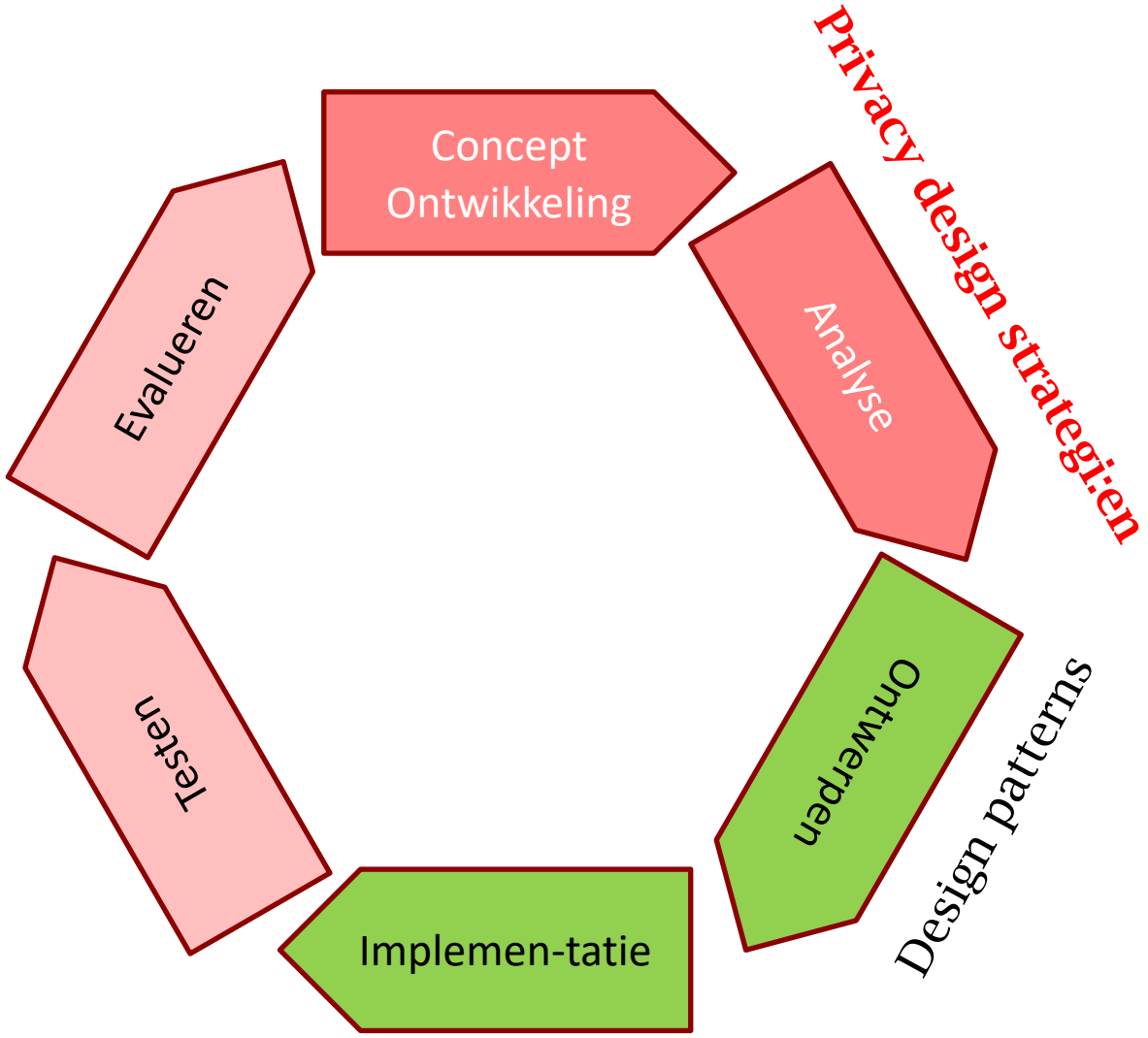
# Wat de techneut denkt… #2

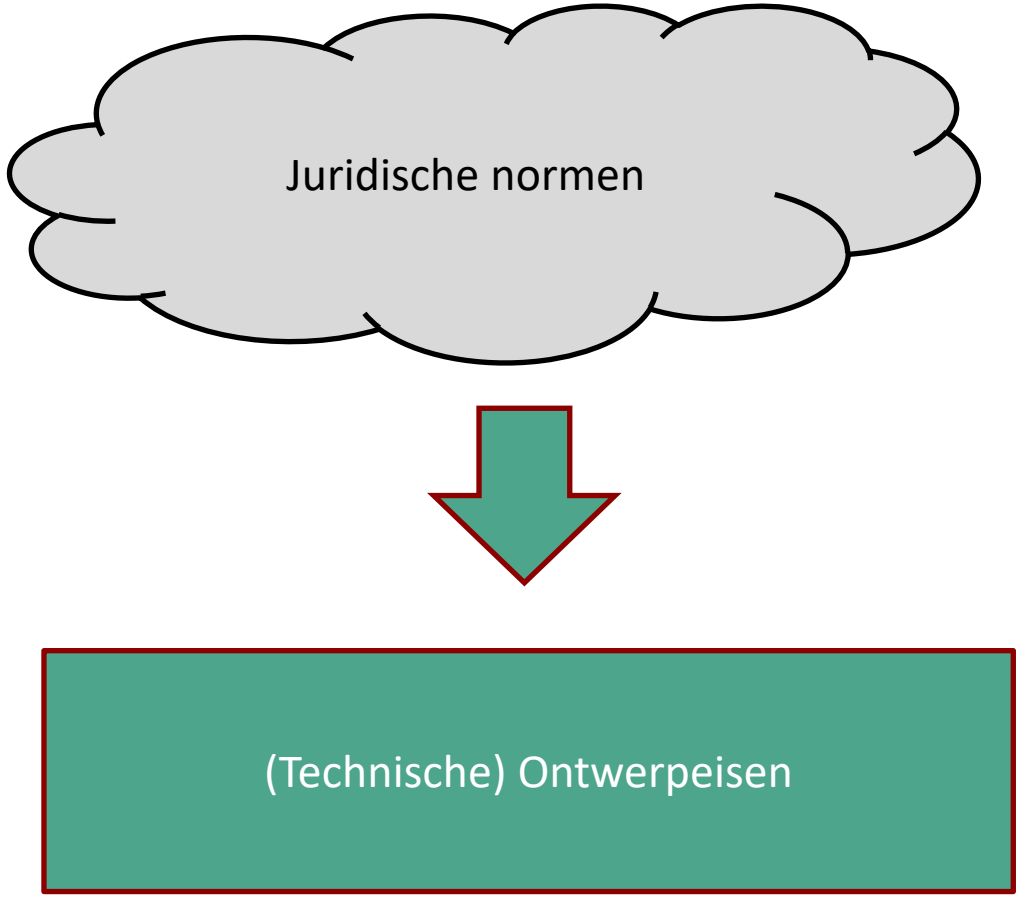
Data controller =

# Wat de techneut denkt… #3

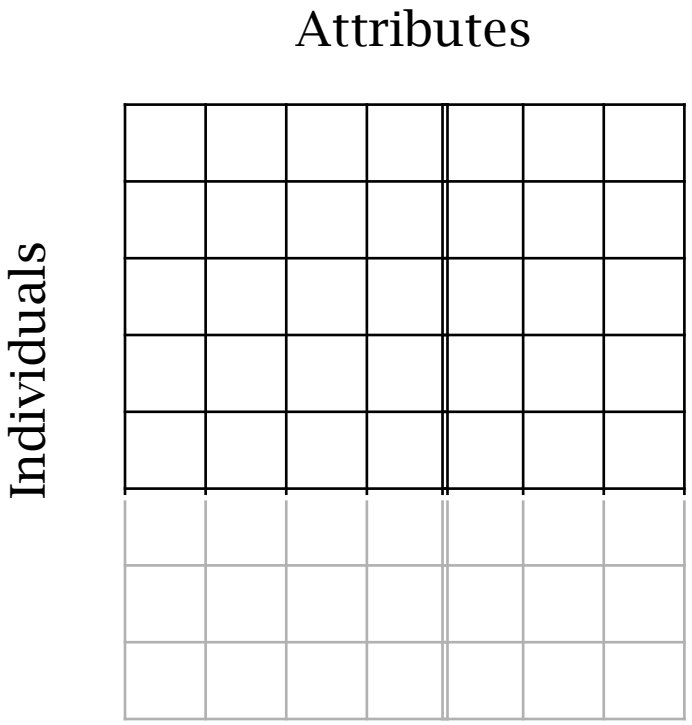
Privacy = Dataminimalisatie

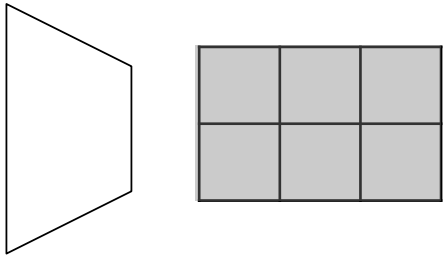
# Privacy design strategies



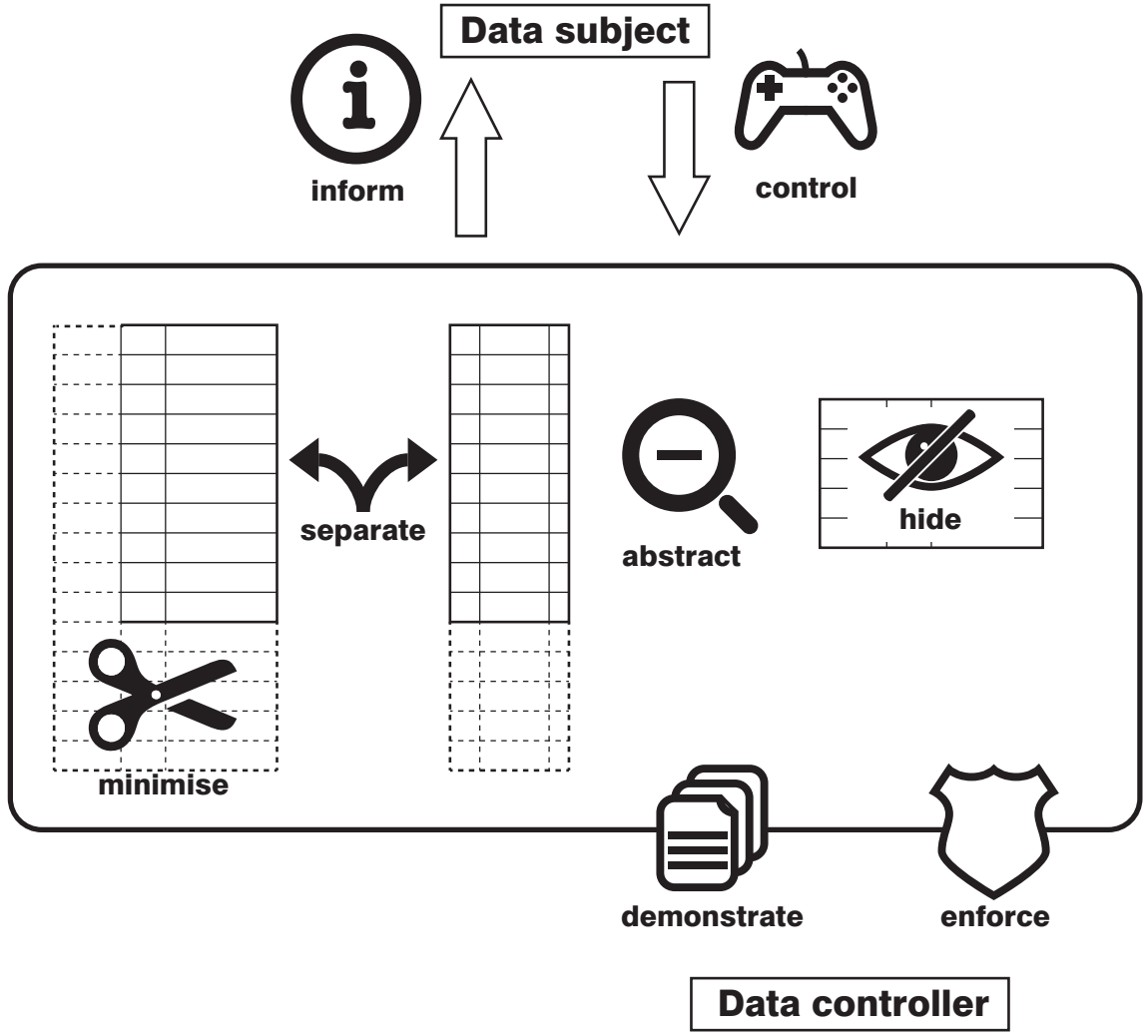
# 8 privacy design strategiën



minimise separate abstract hide

# 8 privacy design strategiën



# 8 privacy design strategiën

## Data oriented

- **Minimaliseer (Minimize)**
  - *Beperk zo veel mogelijk de verwerking van persoonsgegevens.*

- **Scheidt (Separate)**
  - *Scheidt persoonsgegevens zo veel mogelijk van elkaar, om correlatie te beperken.*

- **Abstraheer (Abstract)**
  - *Beperk zoveel mogelijk het detail waarin persoonsgegevens worden verwerkt.*

- **Bescherm, maak onherleidbaar (Hide)**
  - *Voorkom dat persoonsgegevens openbaar of bekend worden.*

## Process oriented

- **Informeer (Inform)**
  - *Informeer gebruikers over de verwerking van hun persoonsgegevens.*

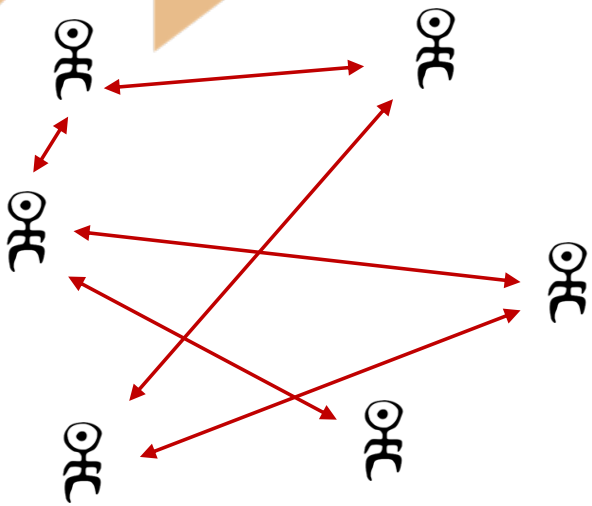
- **Controleer (Control)**
  - *Geef gebruikers controle over de verwerking van hun persoonsgegevens.*

- **Dwing af (Enforce)**
  - *Committeer je aan een privacy vriendelijke verwerking van persoonsgegevens, en dwing dit af.*

- **Toon aan (Demonstrate)**
  - *Toon aan dat je op een privacy vriendelijke wijze persoonsgegevens verwerkt.*

# Scheidt (Separate)

- Definitie
  - *Scheidt persoonsgegevens zo veel mogelijk van elkaar, om correlatie te beperken.*
- Geassocieerde taktieken
  - ISOLEER (ISOLATE): Verzamel of verwerk persoonsgegevens in verschillende databases of systemen.
  - DISTRIBUEER (DISTRIBUTE): Distribueer de verwerking over verschillende locaties.
- Voorbeelden
  - Peer-to-peer
  - Doe zoveel mogelijk in de apparatuur (PC, smartphone) van de eindgebruiker



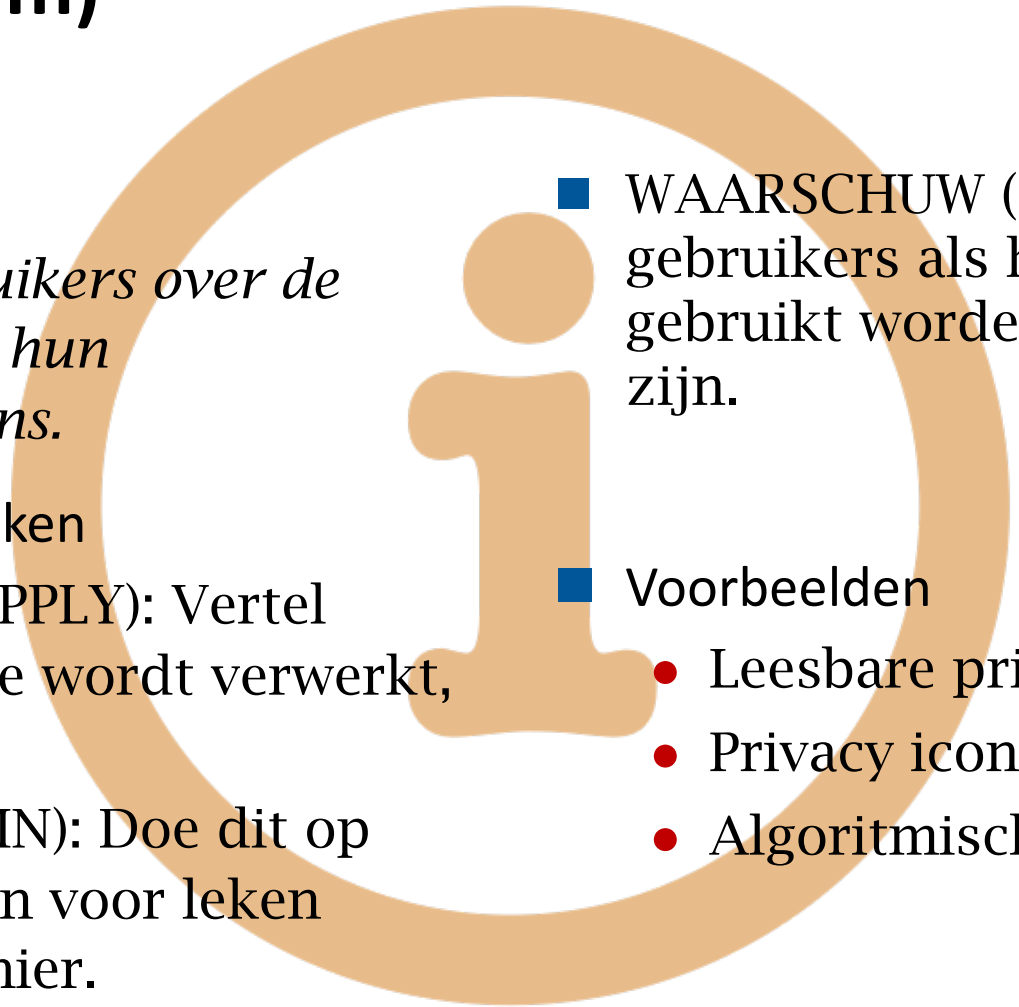
diaspora*

# Abstraheer (Abstract)

- Definitie
  - *Beperk zoveel mogelijk het detail waarin persoonsgegevens worden verwerkt.*
- Geassocieerde taktieken
  - GROEPEER (GROUP): Aggregeer informatie over categorieën personen in plaats van ieder individu.
  - VAT SAMEN, GENERALISEER (SUMMARIZE): Vat gedetailleerde informatie samen in meer algemene gegevens.

- Voorbeelden
  - Registreer leeftijd ipv geboortedatum
  - Verzamel het energieverbruik in een wijk ipv per huishouden
  - Attribuut gebaseerde credentials

# Informeer (Inform)



- Definitie
  - *Informeer gebruikers over de verwerking van hun persoonsgegevens.*
- Geassocieerde taktieken
  - INFORMEER (SUPPLY): Vertel welke informatie wordt verwerkt, en waarom.
  - LEG UIT (EXPLAIN): Doe dit op een duidelijke en voor leken begrijpbare manier.
  - WAARSCHUW (NOTIFY): Waarschuw gebruikers als hun persoonsgegevens gebruikt worden, of als deze gelekt zijn.
- Voorbeelden
  - Leesbare privacy policy
  - Privacy icons
  - Algoritmische transparantie

Privacy & Identity Lab

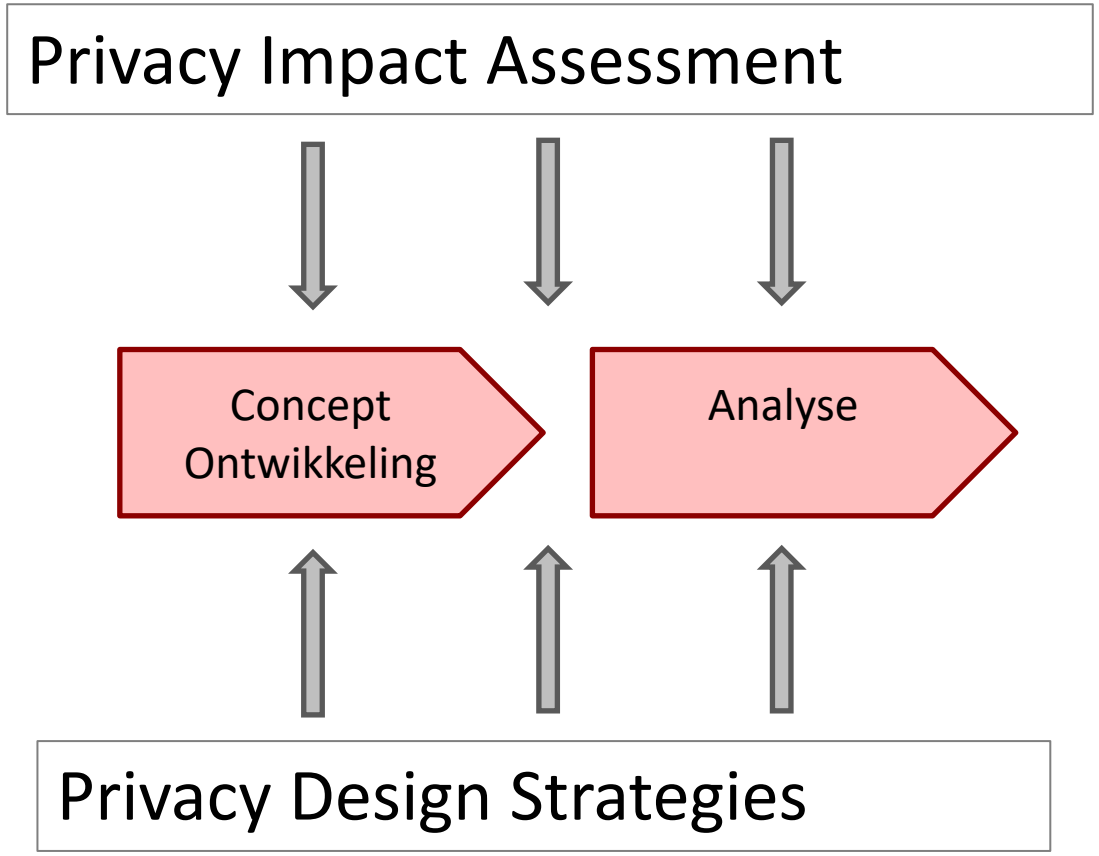
Radboud University

Tilburg University
Law School

university of groningen

# De toekomst

# Impact assessment & ontwerpstrategiën



# Methodologiën

# Privacy Engineering

# Tools

# Privacy design pattern

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).

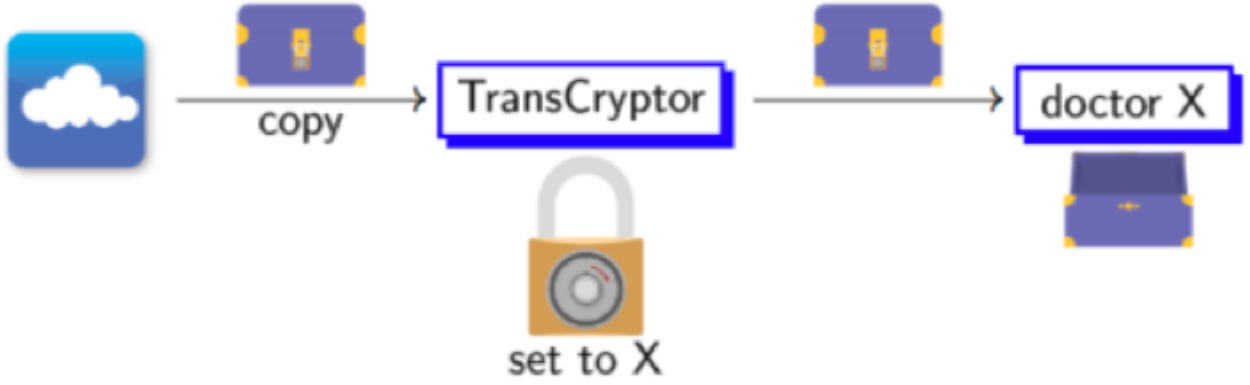
- Beschrijft een vaak terugkerend patroon van communicerende componenten waarmee een algemeen ontwerp probleem wordt opgelost binnen een bepaalde context
  - Samenvatting
  - Context
  - Probleem
  - Oplossing
  - Structuur
  - Consequenties
  - Randvoorwaarden

# De techniek kan veel meer dan je denkt

## Polymorphic encryption scenario (no pseudonyms yet)

- Sensitive device data are stored under polymorphic encryption

- Later on, device user gives doctor X access to the data:




The TransCryptor learns nothing about the data!

http://privacybydesign.foundation

# Vragen / discussie

[Monty Python's
Argument Clinic sketch]