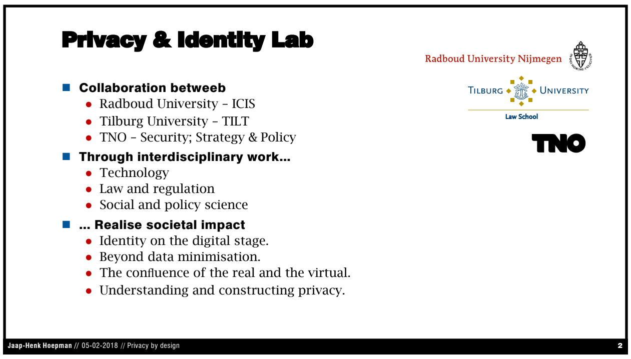
Privacy by Design

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



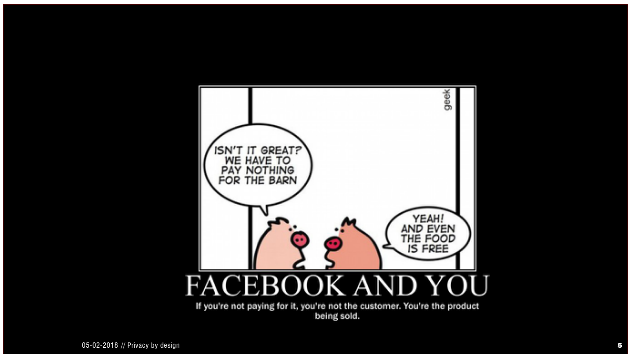
Privacy & Identity Lab

- **Collaboration betweeb**
  - Radboud University – ICIS
  - Tilburg University – TILT
  - TNO – Security; Strategy & Policy
- **Through interdisciplinary work…**
  - Technology
  - Law and regulation
  - Social and policy science
- **… Realise societal impact**
  - Identity on the digital stage.
  - Beyond data minimisation.
  - The confluence of the real and the virtual.
  - Understanding and constructing privacy.

Surveillance by the government

NATIONAL SECURITY AGENCY
at&t
NROL-39
NOTHING IS BEYOND OUR REACH

Jaap-Henk Hoepman // 05-02-2018 // Privacy by design 4

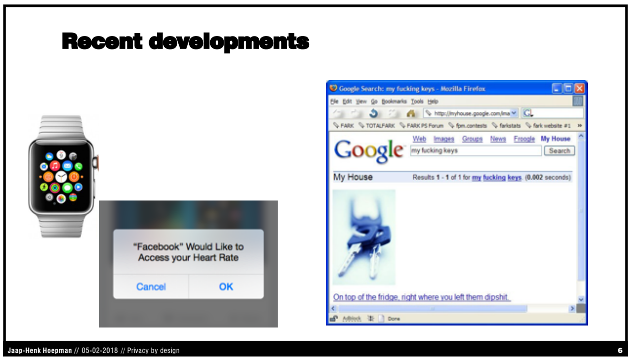


ISN'T IT GREAT? WE HAVE TO PAY NOTHING FOR THE BARN
YEAH! AND EVEN THE FOOD IS FREE
geek

FACEBOOK AND YOU

If you're not paying for it, you're not the customer. You're the product being sold.

05-02-2018 // Privacy by design 5



Recent developments

"Facebook" Would Like to Access your Heart Rate

Google Search: my fucking keys - Mozilla Firefox

File Edit View Go Bookmarks Tools Help
Web Images Groups News Froogle My House
Google
Search

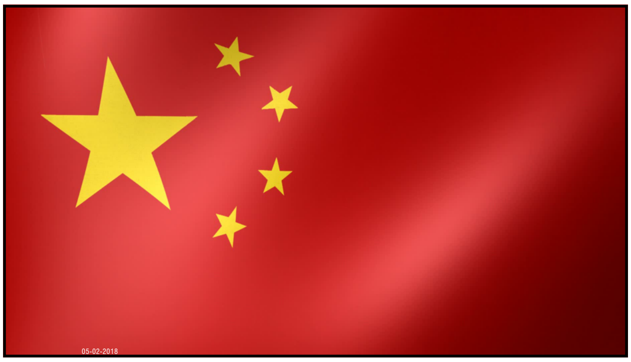
my fucking keys

My House

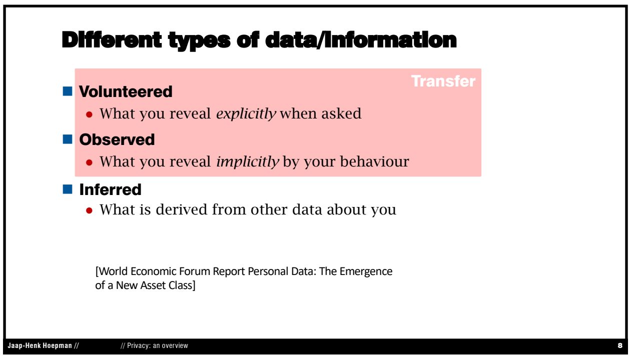
Results 1 - 1 of 1 for my fucking keys. (0.002 seconds)

On top of the fridge, right where you left them dipshit.

Jaap-Henk Hoepman // 05-02-2018 // Privacy by design 6



05-02-2018



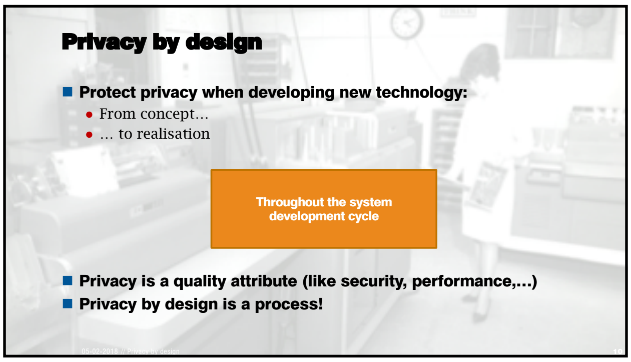
Different types of data/information

Transfer

- **Volunteered**
  - What you reveal *explicitly* when asked
- **Observed**
  - What you reveal *implicitly* by your behaviour
- **Inferred**
  - What is derived from other data about you

[World Economic Forum Report Personal Data: The Emergence of a New Asset Class]

Jaap-Henk Hoepman // // Privacy: an overview 8



Privacy by design

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

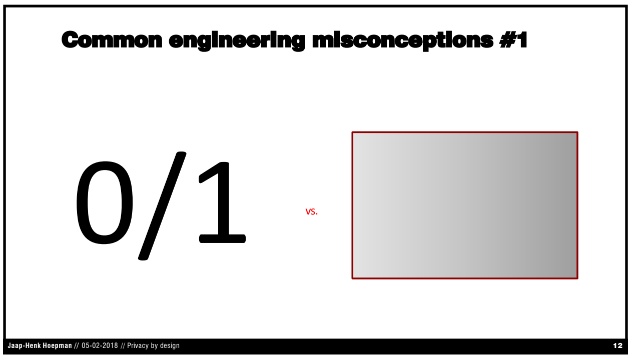
Throughout the system development cycle

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

05-02-2018 // Privacy by design 10

But how?

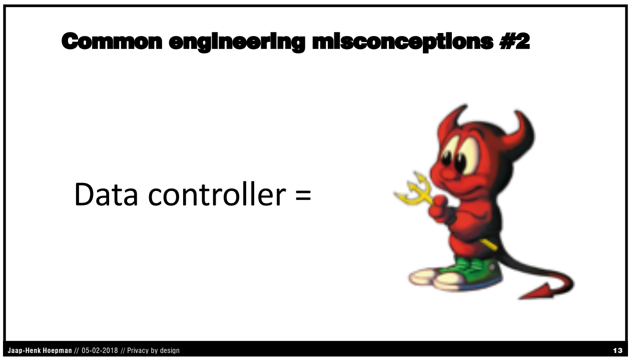
Jaap-Henk Hoepman // 05-02-2018 11



Common engineering misconceptions #1

0/1 vs.

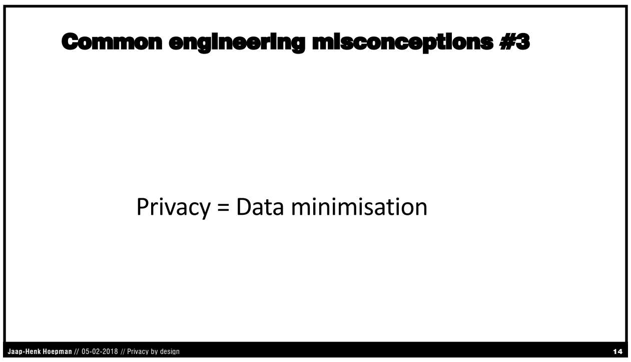
Jaap-Henk Hoepman // 05-02-2018 // Privacy by design 12



Common engineering misconceptions #2

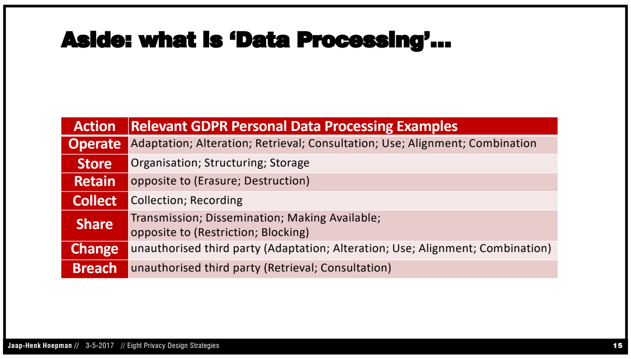
Data controller =

Jaap-Henk Hoepman // 05-02-2018 // Privacy by design 13



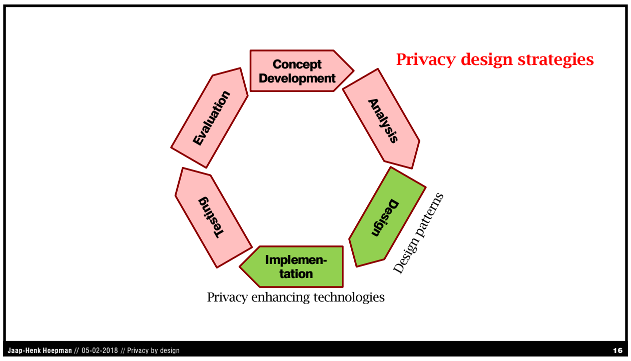
Common engineering misconceptions #3

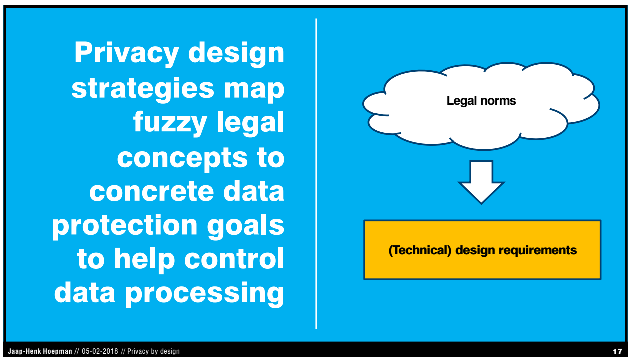
Privacy = Data minimisation



Aside: what is ‘Data Processing’…

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





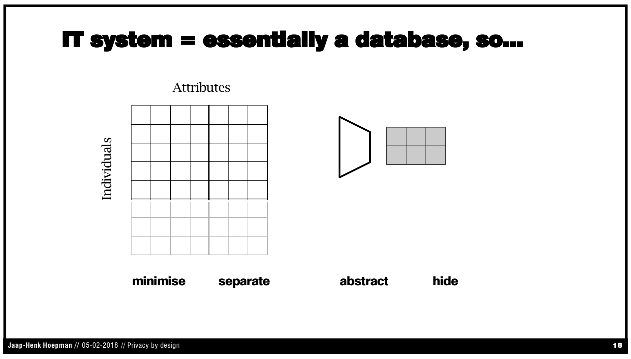
Privacy design strategies map fuzzy legal concepts to concrete data protection goals to help control data processing

Legal norms

(Technical) design requirements

Jaap-Henk Hoepman // 05-02-2018 // Privacy by design

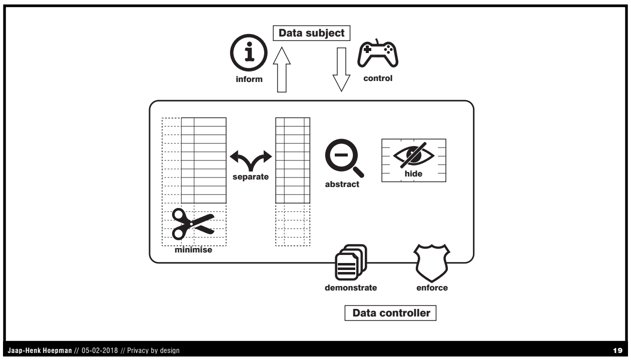
17



IT system = essentially a database, so...

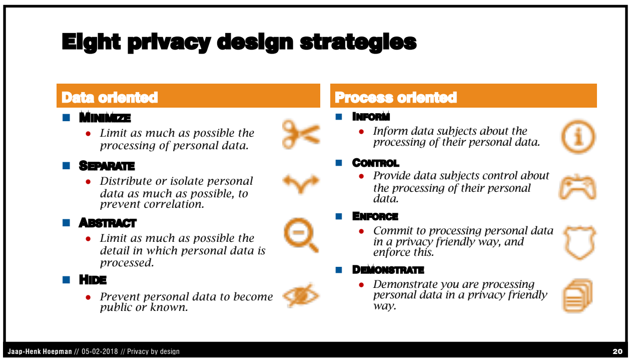
Jaap-Henk Hoepman // 05-02-2018 // Privacy by design

18



Jaap-Henk Hoepman // 05-02-2018 // Privacy by design

19



Eight privacy design strategies

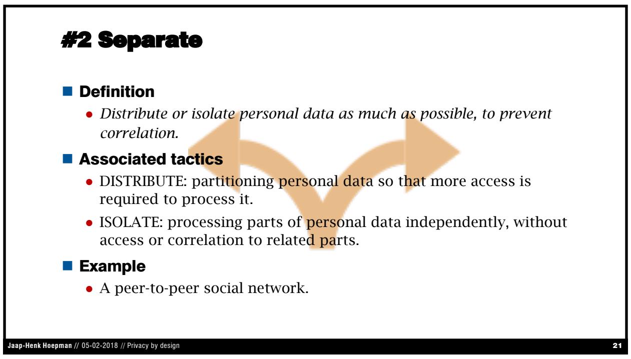
Data oriented

- **MINIMIZE**
  - *Limit as much as possible the processing of personal data.*
- **SEPARATE**
  - *Distribute or isolate personal data as much as possible, to prevent correlation.*
- **ABSTRACT**
  - *Limit as much as possible the detail in which personal data is processed.*
- **HIDE**
  - *Prevent personal data to become public or known.*

Process oriented

- **INFORM**
  - *Inform data subjects about the processing of their personal data.*
- **CONTROL**
  - *Provide data subjects control about the processing of their personal data.*
- **ENFORCE**
  - *Commit to processing personal data in a privacy friendly way, and enforce this.*
- **DEMONSTRATE**
  - *Demonstrate you are processing personal data in a privacy friendly way.*

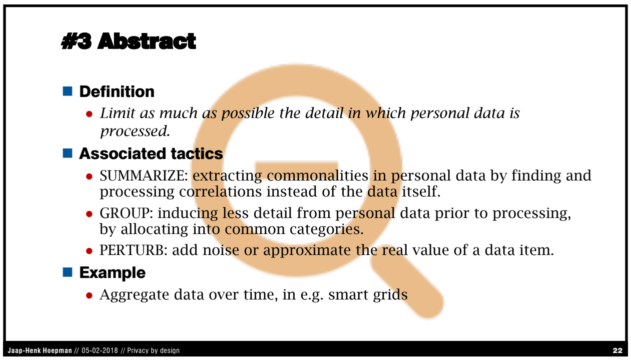
Jaap-Henk Hoepman // 05-02-2018 // Privacy by design 20



#2 Separate

- **Definition**
  - *Distribute or isolate personal data as much as possible, to prevent correlation.*
- **Associated tactics**
  - DISTRIBUTE: partitioning personal data so that more access is required to process it.
  - ISOLATE: processing parts of personal data independently, without access or correlation to related parts.
- **Example**
  - A peer-to-peer social network.

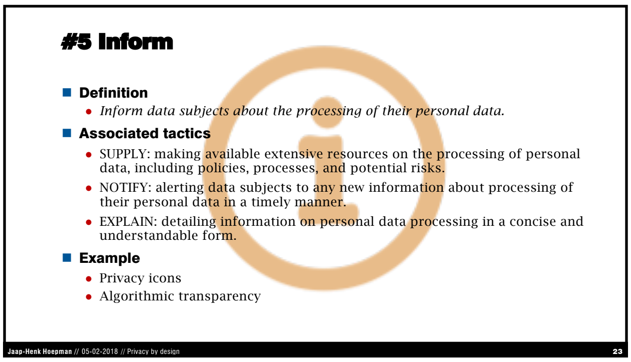
Jaap-Henk Hoepman // 05-02-2018 // Privacy by design 21



#3 Abstract

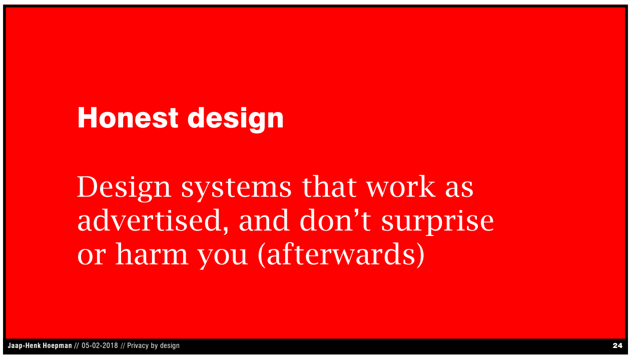
- **Definition**
  - *Limit as much as possible the detail in which personal data is processed.*
- **Associated tactics**
  - SUMMARIZE: extracting commonalities in personal data by finding and processing correlations instead of the data itself.
  - GROUP: inducing less detail from personal data prior to processing, by allocating into common categories.
  - PERTURB: add noise or approximate the real value of a data item.
- **Example**
  - Aggregate data over time, in e.g. smart grids

Jaap-Henk Hoepman // 05-02-2018 // Privacy by design 22



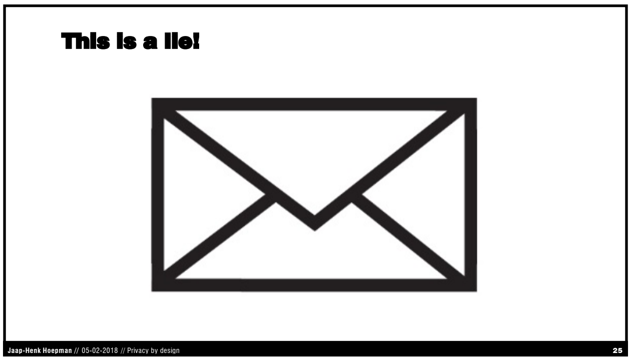
#5 Inform

- **Definition**
  - *Inform data subjects about the processing of their personal data.*
- **Associated tactics**
  - SUPPLY: making available extensive resources on the processing of personal data, including policies, processes, and potential risks.
  - NOTIFY: alerting data subjects to any new information about processing of their personal data in a timely manner.
  - EXPLAIN: detailing information on personal data processing in a concise and understandable form.
- **Example**
  - Privacy icons
  - Algorithmic transparency



Honest design

Design systems that work as advertised, and don't surprise or harm you (afterwards)



This is a lie!

Discussion

[Monty Python's Argument Clinic sketch]

jhh@cs.ru.nl www.cs.ru.nl/~jhh blog.xot.nl twitter: @xotoxot

Jaap-Henk Hoepman // 05-02-2018 // Privacy by design **26**