



## Designing Privacy by Design

Jaap-Henk Hoepman  
 RU Nijmegen  
[jhh@cs.ru.nl](mailto:jhh@cs.ru.nl) / @xotoxot / [www.xot.nl](http://www.xot.nl)



### Introductie



- **PI.lab: samenwerking tussen:**

- Radboud Universiteit – ICIS
- Tilburg Universiteit – TILT
- TNO – Security; Strategy & Policy
- SIDN



- **Ikzelf:**

- Wetenschappelijk directeur PI.lab
- Universitair Hoofddocent Radboud Universiteit
- Onderzoek: privacy & identity, toegepaste cryptografie, Internet of Things

3 | Designing Privacy by Design / Jaap-Henk Hoepman / 1310-2014

[www.pilab.nl](http://www.pilab.nl)

### Wat is privacy?



- **The right to be let alone**  
 – [Warren & Brandeis, 1890]
- **Informational self-determination: The right to determine for yourself when, how and to what extend information about you is communicated to others**  
 – [Westin, 1967]
- **The freedom from unreasonable constraints on the construction of ones identity**  
 – [Agre & Rottenberg, 2001]
- **Contextual integrity: the right to prevent information to flow from one context to another**  
 – [Nissenbaum, 2004]

4 | Designing Privacy by Design / Jaap-Henk Hoepman / 1310-2014

[www.pilab.nl](http://www.pilab.nl)

### Persoonlijke informatie



- **Data bronnen**

- Vrijwillig gegeven data
- Geobserveerde data
- Daar van afgeleide gegevens

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

- **Metadata (= gegevens over gedrag)**

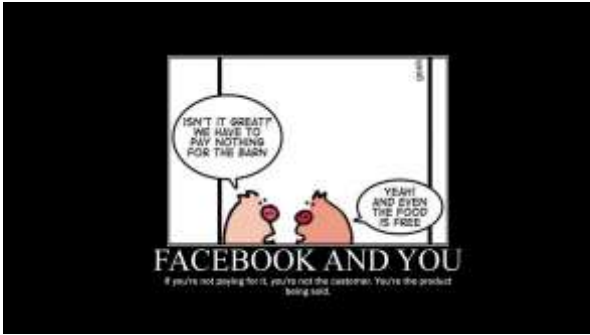
- Gecondenseerd: rijk aan informatie, makkelijk te verwerken
- "Waar(devoller)": *beoordeel een man niet op wat hij zegt maar op wat hij doet.*



5 | Designing Privacy by Design / Jaap-Henk Hoepman / 1310-2014

[www.pilab.nl](http://www.pilab.nl)

[www.pilab.nl](http://www.pilab.nl)



**Ze weten dingen eerder dan jij zelf!**

**TARGET**

8 | Designing Privacy by Design / JaapHenk Hoepman / 13-10-2014 [www.pilab.nl](http://www.pilab.nl)

**Een metafoor voor het belang van privacy**

orwell / big brother    chandler / little sister    kafka / the trial    the matrix

9 | Designing Privacy by Design / JaapHenk Hoepman / 13-10-2014 [www.pilab.nl](http://www.pilab.nl)

**FORKE & SUKKE**  
WISDEN MET DE ERG ZEKERHOUDE

"AAN DE BENCHERS  
WAL PFF BENOED"

"HIE WAREN LE  
GAE MOU NEEG TI"

10 | Designing Privacy by Design / JaapHenk Hoepman / 13-10-2014 [www.pilab.nl](http://www.pilab.nl)

**Privacy by design**

- **Protect privacy during technology development:**
  - From conception...
  - ... to realisation.

Through the full product development lifecycle

11 | Designing Privacy by Design / JaapHenk Hoepman / 13-10-2014 [www.pilab.nl](http://www.pilab.nl)

**Software development cycle**

Concept Development    Analysis    Design (Design patterns)    Implementation (Privacy enhancing technologies)    Review    Evaluation

12 | Designing Privacy by Design / JaapHenk Hoepman / 13-10-2014 [www.pilab.nl](http://www.pilab.nl)

## Approaches

- **Minimise**
  - Select before you collect
- **Hide**
  - TOR
- **Aggregate**
- **Separate**
  - Distribueer data; verwerk lokaal; P2P
- **Inform**
- **Control**
- **Enforce**
- **Demonstrate**

13 Designing Privacy by Design / JaapHenk Hoepman / 13-10-2014

www.pillab.nl

## Privacy-vriendelijk 'appen'



14 Designing Privacy by Design / JaapHenk Hoepman / 13-10-2014

www.pillab.nl

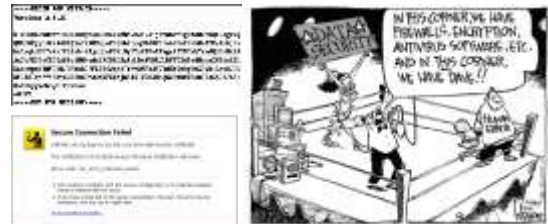
## Privacy-vriendelijk identiteitsbeheer



15 Designing Privacy by Design / JaapHenk Hoepman / 13-10-2014

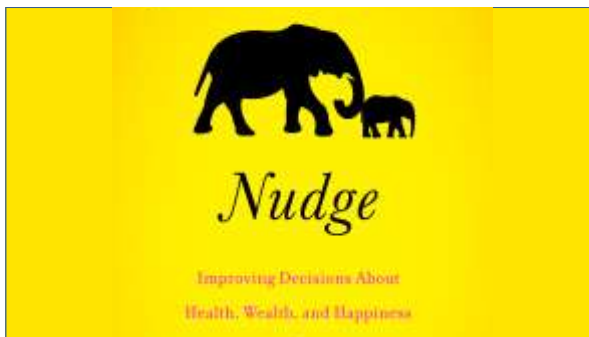
www.pillab.nl

## PGP (en veel ander spul) sucks



16 Designing Privacy by Design / JaapHenk Hoepman / 13-10-2014

www.pillab.nl



## Het "Internet der dingen"



18 Designing Privacy by Design / JaapHenk Hoepman / 13-10-2014

www.pillab.nl

## Nieuwe risico's



- **Het system is onzichtbaar**
  - Geen interface.
- **Het system omvat**
  - niet alleen sensoren
  - maar ook actuatoren

19 | Designing Privacy by Design / JaapHenk Hoepman / 13-10-2014

[www.pilab.nl](http://www.pilab.nl)

## Ik heb maar 1 vraag...



- **hoe maak je privacyvriendelijke systemen ook gebruikersvriendelijk (en dus bruikbaar)?**

20 | Designing Privacy by Design / JaapHenk Hoepman / 13-10-2014

[www.pilab.nl](http://www.pilab.nl)

## Discussie



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

21 | Designing Privacy by Design / JaapHenk Hoepman / 13-10-2014

[www.pilab.nl](http://www.pilab.nl)