iHub

Privacy Seminar

Privacy - An Introduction

Jaap-Henk Hoepman

iHub
Radboud University
Karlstad University

jhh@cs.ru.nl // www.cs.ru.nl/~jhh // blog.xot.nl
@xot@someone.elses.computer // @xotoxot.bsky.social

Radboud University

Contents

- **Privacy under threat**
  - Government
  - Business
  - People
- **What is privacy?**
- **The value of privacy**
  - Individual liberty
  - Social value
- **How the law protects privacy**

iHub

Government surveillance

Radboud University

Snowden


Support The Guardian
Available for everyone, funded by readers
Contribute
Subscribe
Search jobs
Sign in
Search
The Guardian
International edition
News
Opinion
Sport
Culture
Lifestyle
More
World
Europe
US
Americas
Asia
Australia
Middle East
Africa
Inequality
Global development
The NSA files
NSA files decoded / Edward Snowden's surveillance revelations explained
All stories

Fraud detection, policing

de Volkskrant

Columns & Opinie Video Wetenschap Mensen De Gids Cultuur

NIEUWS STAKING FRAUDEONDERZOEK

Rotterdam stopt omstreden fraudeonderzoek met SyRI

Rotterdam stopt met het fraudeonderzoek met het risico-indicatiesysteem SyRI in de wijken Bloemhof en Hillesluis. De gemeente krijgt de opzet van het onderzoek niet rond vanwege de juridische onduidelijkheid of het gewenste onderzoek niet in strijd is met privacywetten.

Charlotte Huisman 3 juli 2019, 20:32

Trouw

Gemeente Amsterdam

Politie Amsterdam loerde onterecht in data van milieucamera's

Belastingdienst

Data driven governance

Use location data to make policy decisions on if/when/how to invest in certain (commercial) areas.

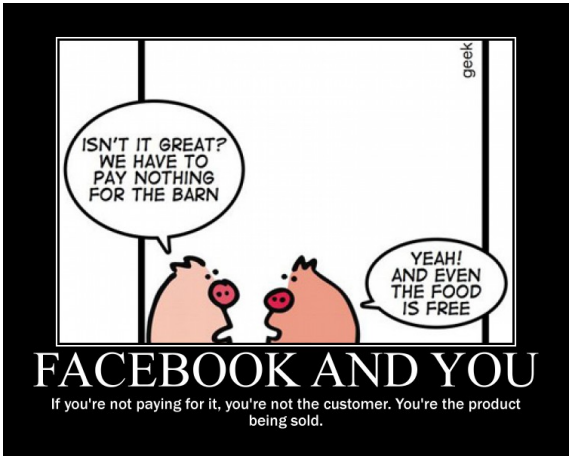
- **measure number of visitors per hour**
- **measure returning visitors**
- **determine origin of visitors**
  - postal code
  - municipality
- **determine cross-visits (% of people that visited A also visit B)**
  - if A is a border, you can measure foreign visitors.

More examples?

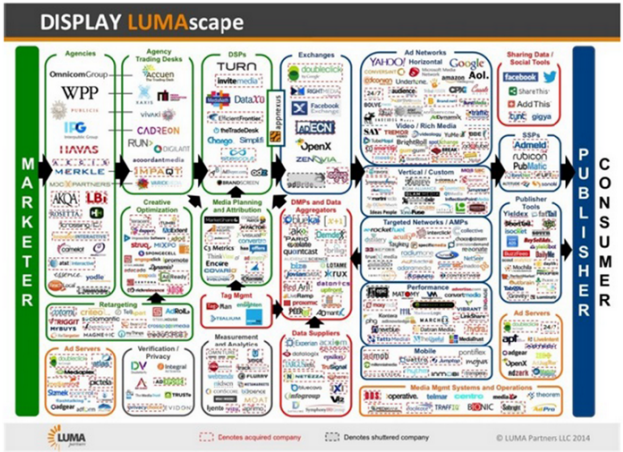
iHub

Commercial surveillance

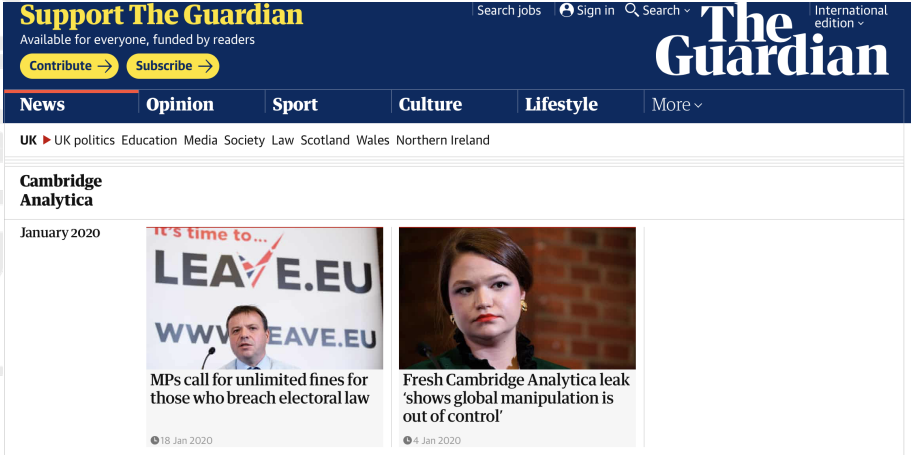
Radboud University


geek
ISN'T IT GREAT? WE HAVE TO PAY NOTHING FOR THE BARN
YEAH! AND EVEN THE FOOD IS FREE
FACEBOOK AND YOU
If you're not paying for it, you're not the customer. You're the product being sold.

Advertising (cookies, fingerprinting and more)



Cambridge Analytica



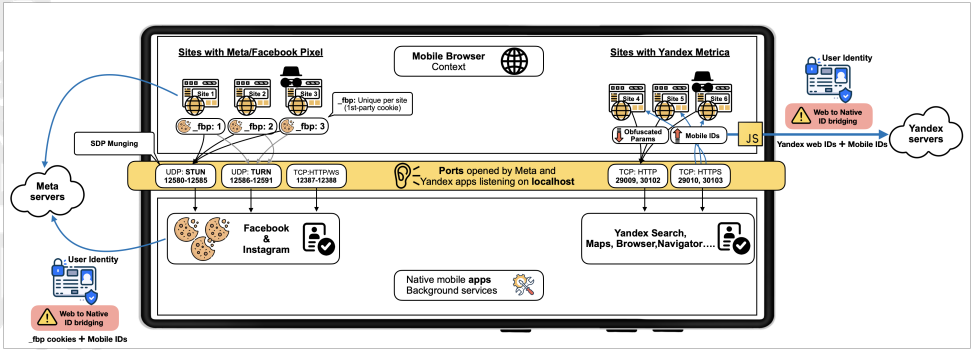
https://www.theguardian.com/uk-news/cambridge-analytica

Targetted campaigning, Dutch 2021 elections

https://www.nrc.nl/nieuws/2021/02/22/de-rode-roos-maakt-plaats-voor-het-online-filmpje-a4032842

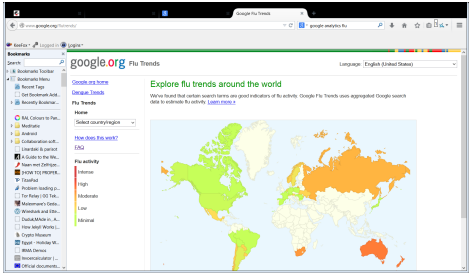
https://www.volkskrant.nl/nieuws-achtergrond/politieke-partijen-willen-liever-niet-dat-u-dit-weet-de-geruisloze-strijd-om-uw-stem-via-facebook~bcdbf993/

Localmess (Vlummens et al. 2026)



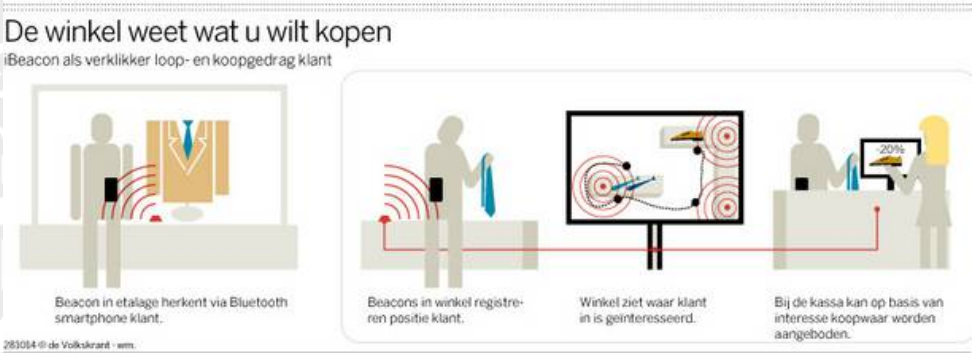
More examples?

They know things before you yourself do ??



TARGET

They track you even in real shops



iHub

People

Radboud University

People

People

- **Online 24 hours/day**
- **Do many things over the Internet**
  - Social networking
  - Communications
  - Reading
  - Video
  - Finance
  - Maps
  - Platforms (Airbnb, Uber)

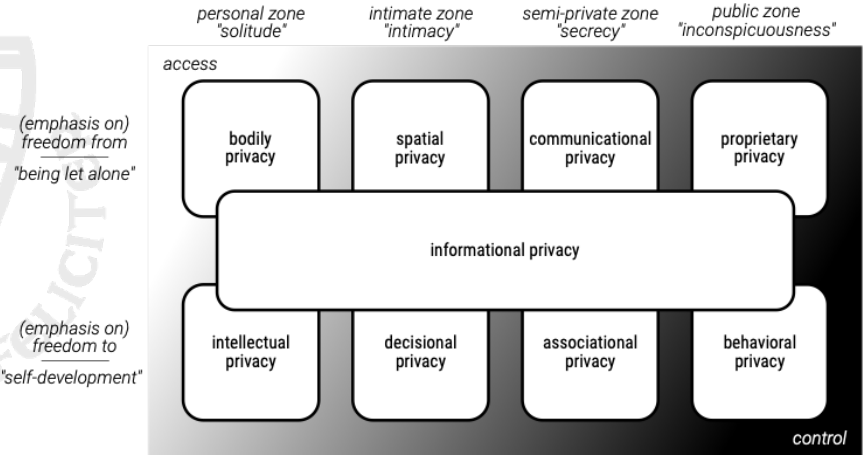
iHub

Privacy

Radboud University

What is privacy according to you?

Privacy typology (Koops et al. 2017)



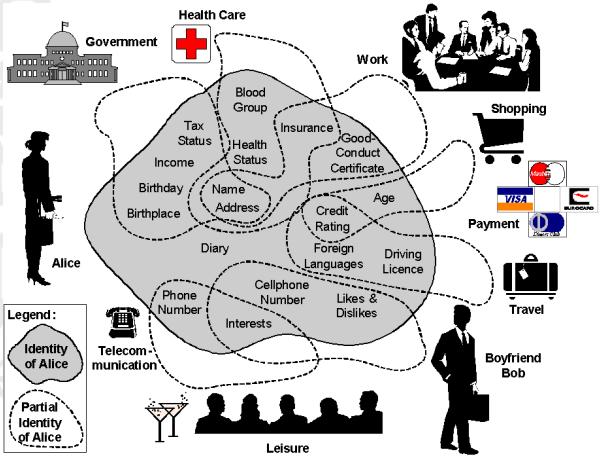
Technology impacted privacy

- **computing (1950-)**
  - searching becomes efficient
  - data kept forever
- **networking (1980-)**
  - datasharing becomes easy
  - data accessible on-line
  - “network effect”

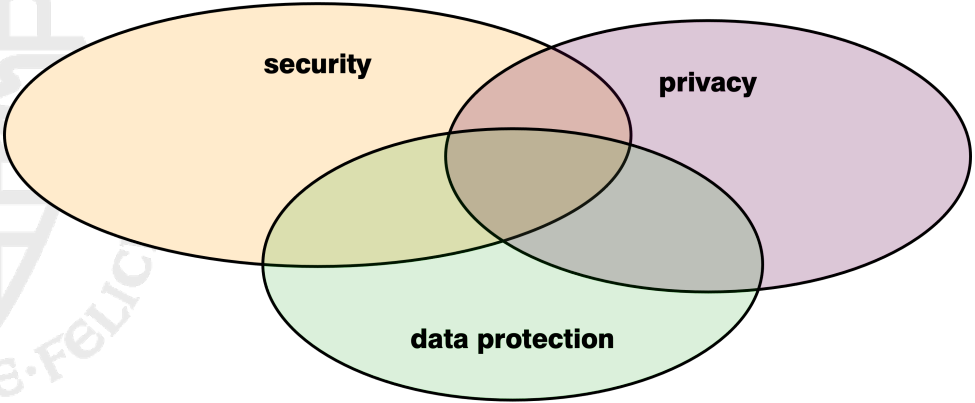
Different definitions

- **The right to be let alone**
  - (Warren and 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 one's identity**
  - (Agre and Rotenberg 1998)
- **Contextual integrity: the right to prevent information to flow from one context to another**
  - (Nissenbaum 2004)

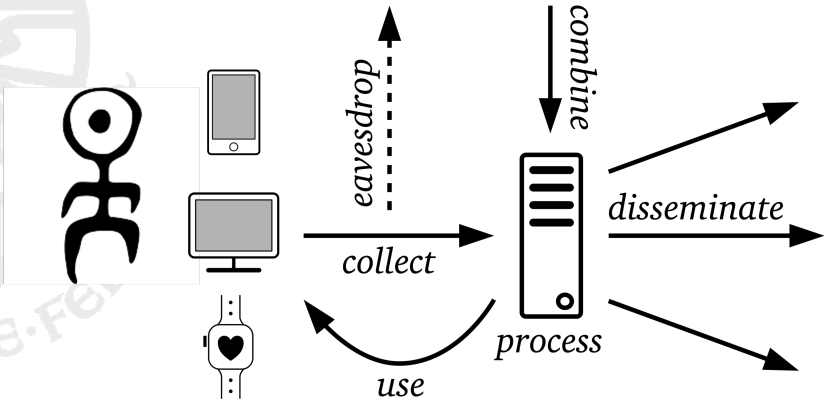
Contextual integrity: beyond context separation



Don’t confuse these concepts!



Privacy invasions (Solove 2006)



Different types of data/information (WEF 2011)

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

The dangers of metadata

- **Collected surreptitiously**
  - The systems we use rediate personal data continually
- **Small, structured, pieces of data**
  - Easy to collect, store, process and analyse
- **Relate to behaviour**
  - “Don’t listen to what a man says; look at what he does”


HOBBES, DO YOU THINK OUR MORALITY IS DEFINED BY OUR ACTIONS, OR BY WHAT'S IN OUR HEARTS?
I THINK OUR ACTIONS SHOW WHAT'S IN OUR HEARTS.
© 1990 Universal Press Syndicate

Why is privacy important

In the late 20th century Romania was ruled by the dictator Nicolae Ceaușescu, with the help of his brutal secret police, the Securitate, and its half a million informers. In the 1980's there was a big shortage of food and fuel in Romania. As a result the Romanians suffered from hunger and cold. The Romanians feared the Securitate so much, that the were afraid to even talk among each other about the fact that they were hungry and cold. The risk that an informant would hear them and accuse them of criticising the government was simply too high. A study by a Romanian psychologist Radu Clit later found that the Romanians suffered most from the fact that the couldn't even talk about the fact that they were hungry and cold. Even more than that they suffered from being hungry and cold itself!
(Zanfir-Fortuna 2012)

Moral basis for data protection (Hoven and Vermaas 2007)

- **prevention of information-based harm**
  - Like guns, information may kill people
- **prevention of informational inequality**
  - The “market” of information
  - Non-discrimination
- **prevention of informational injustice**
  - Spheres of privacy must be protected
- **respect for moral autonomy.**
  - People change

The value of privacy

As a personal right

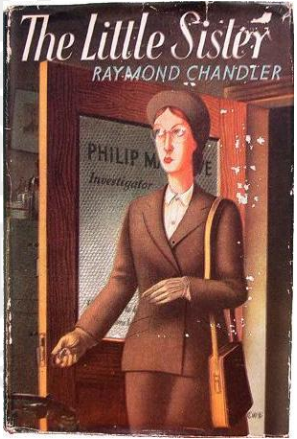
- **Protect**
  - Personal freedom
  - Autonomy
- **Restore power balance**
  - Kafka's "The Trial"

As a societal need

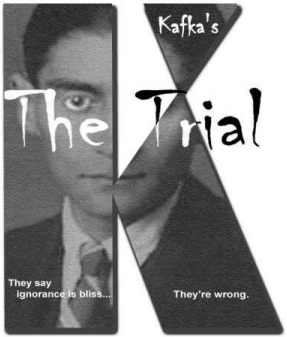
- **Protect democratic process**
  - Prevent meddling with elections
  - Freedom to vote without interference
  - Consistent public political campaign
- **Debate status quo**
  - Labour rights
  - Women voting rights
  - Gay rights

”Privacy is essential for freedom, democracy, psychological well-being, individuality and creativ-ity"
(Solove 2008)

Searching for the right metaphor



orwell / big brother



chandler / little sister

kafka / the trial

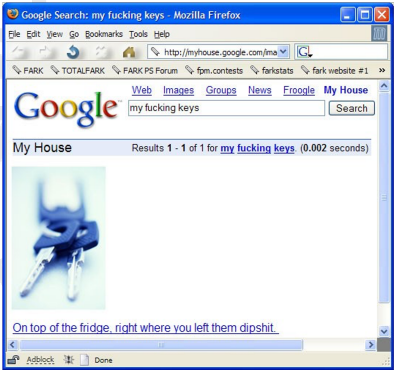
You've got nothing to hide

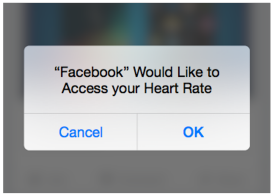
Have you!!??

I have nothing to hide…. (Solove 2007)

- **Hiding is natural**
  - There is no “I”, no self, without privacy
  - It is impossible to be fully transparent
- **Freedom of thought**
  - That job offer looks interesting...
  - That woman looks “interesting”...
- **Necessary to build relationships**
  - Contexts matter!
- **What is the data used for: investigation, anti-terrorism, or …??**
  - Function creep
- **Everybody has something to be embarrassed about**
  - And everybody breaks the law a lot of times
- **Assumes that the problem is data you want to hide**
  - even “innocent” data can harm you
- **No distinction between illegal (legal) vs disgraceful (moral) vs …:**
  - data is data
- **Norms change**
  - Pedophilia in NL

Beyond privacy: autonomy





iHub

The GDPR in 5 minutes

Radboud University

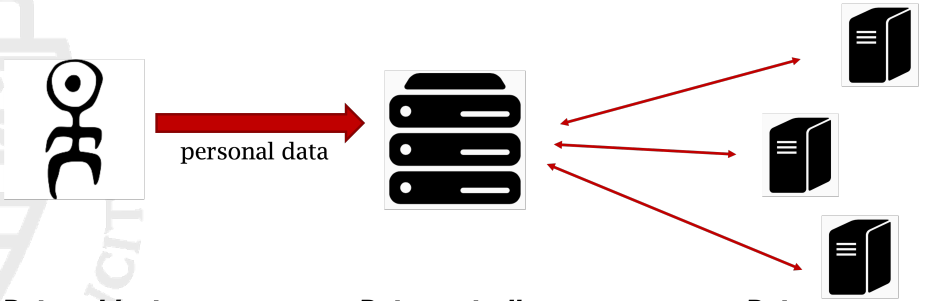
Applies when you process personal data?

(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

(2) ‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

Subject / controller / processor



(7) 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

GDPR principles (art 5.)

1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

GDPR principles (art 5.)

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

GDPR lawfulness (art. 6)

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

GDPR and automated decision making

Article 22

Automated individual decision-making, including profiling

1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

2. Paragraph 1 shall not apply if the decision:

(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;

(b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

(c) is based on the data subject's explicit consent.

3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

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

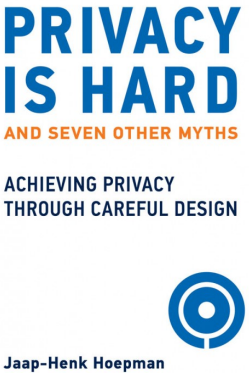

And no, I am not a luddite

”

Technology is neither good nor bad; nor is it neutral.
--- *Melvin Kranzberg, 1985*

Architecture is politics.
--- *Mitch Kapor, 1991*

Resources



- **Websites**
  - `http://wiki.science.ru.nl/privacy/`
  - https://www.eff.org/
  - https://www.bof.nl
  - My blog `https://blog.xot.nl`
- **Books**
  - Ilija Trojanow, Juli Zeh “Aanslag op de vrijheid”, de Geus,2010
  - Bart de Koning “Alles onder controle”, Uitgeverij Balans, 2008.
  - Jaap-Henk Hoepman “Privacy Is Hard And Seven Other Myths”, MIT Press, October 2021

See also references below

Questions / discussion

[Monty Python's Argument Clinic sketch]

References

Agre, P. E. and M. Rotenberg (1998). *Technology and Privacy: The New Landscape.* Cambridge: MIT Press.

Hoven, J. van den and P. E. Vermaas (2007). "NanoTechnology and Privacy: On Continuous Surveillance Outside the Panopticon". In: *Journal of Medicine and Philosophy* 32.3, pp. 283–297.

Koops, B.-J. et al. (2017). "A Typology of Privacy". In: *University of Pennsylvania Journal of International Law* 38, pp. 483–575.

Nissenbaum, H. (Feb. 2004). "Privacy as Contextual Integrity". In: *Washington Law Review* 79.1, pp. 119–158.

Solove, D. J. (2006). "A Taxonomy of Privacy". In: *University of Pennsylvania Law Review* 154.3, pp. 477–564.

Solove, D. J. (2007). ""I've Got Nothing to Hide" and Other Misunderstandings of Privacy". In: *San Diego Law Review* 44, p. 745.

— (2008). *Understanding Privacy*. Cambridge: Harvard University Press.

Vlummens, T. et al. (2026). “Bridges to Self: Silent Web-to-App Tracking on Mobile via Localhost”. In: *35th USENIX Security Symposium*.
Warren, S. D. and L. D. Brandeis (Dec. 15, 1890). “The Right to Privacy. The Implicit Made Explicit”. In: *Harvard Law Review* IV.5, pp. 193–220.
Westin, A. F. (1967). *Privacy and Freedom*. New York: Atheneum.
World Economic Forum (Jan. 2011). *Personal Data: The Emergence of a New Asset Class*. Report. World Economic Forum.
Zanfir-Fortuna, G. (2012). “’Big Brother’ in a Post-Communist Era - A Radiography of the Protection of Private Life in an European Romania”. In: *Revue des Sciences Politiques* 35, pp. 330–351.