Privacy - the what & why

GÉANT eHealth Training

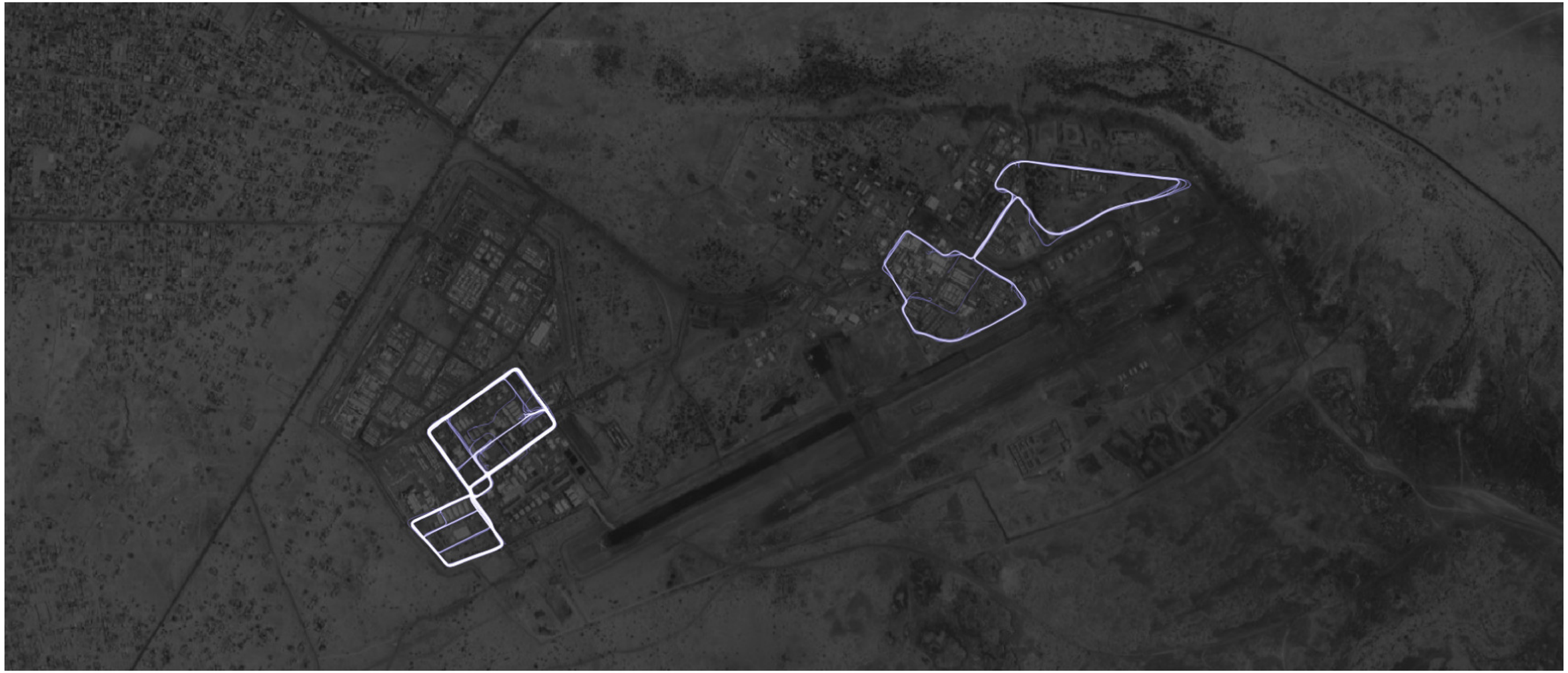
Arnout Terpstra
Product Manager Trust & Identity, SURF
(External) PhD student, Tilburg University (TILT)

Outline

1. Privacy: what's wrong?
2. What is privacy and why is it important to protect
3. Crash course GDPR and Privacy by Design
4. My own research: how design can help people think about privacy

Dima Yarovinsky, I Agree
https://www.dimayarovinsky.com/#/i-agree/

Rebecca Ricks, How PayPal Shares Your Data
https://rebecca-ricks.com/paypal-data/

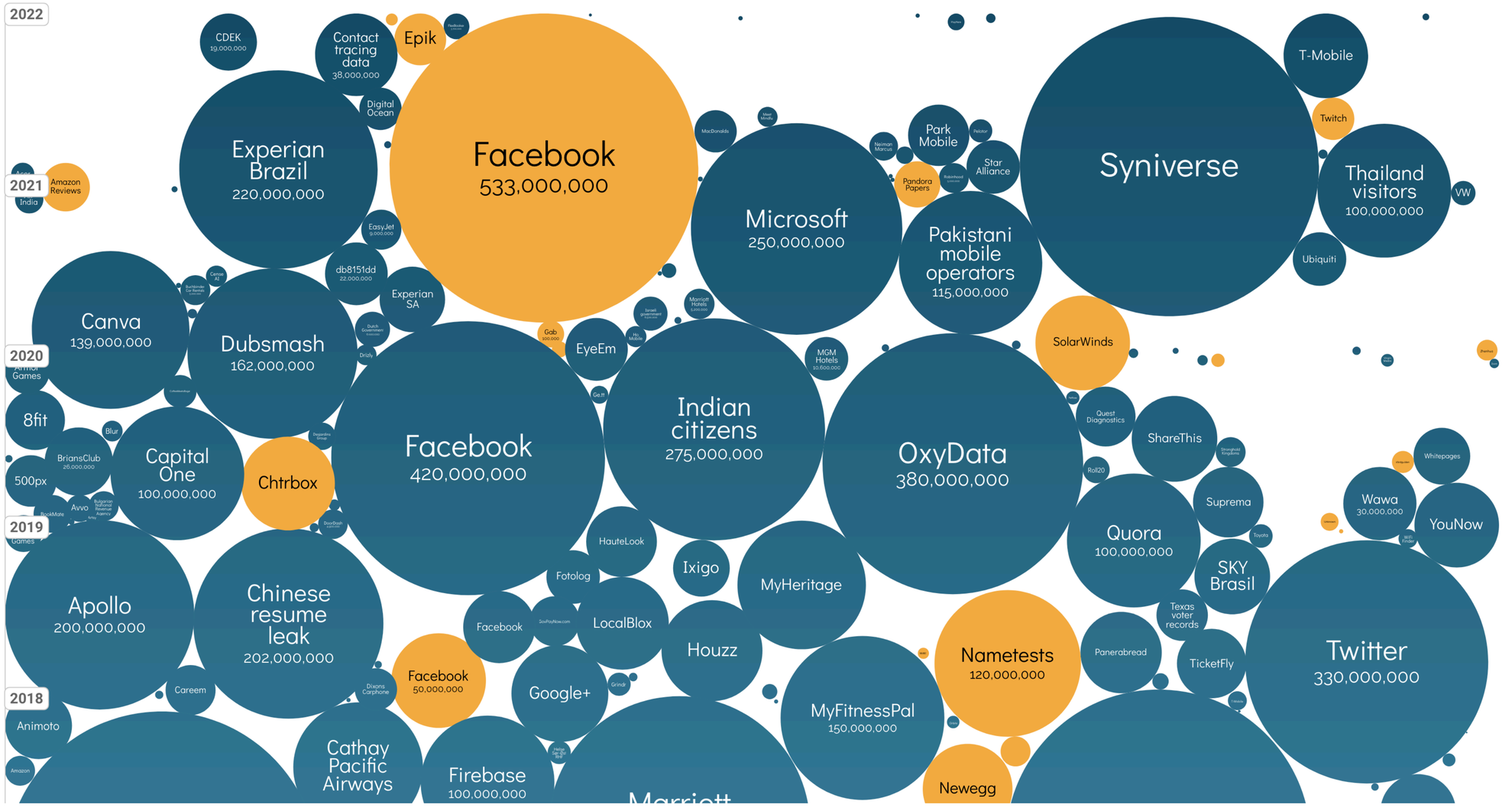


Project Polar, The Correspondent
https://decorrespondent.nl/collectie/project-polar-english

World's Biggest Data Breaches & Hacks

Selected events over 30,000 records

UPDATED: May 2022

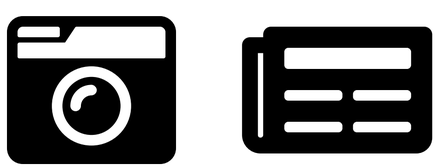


https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

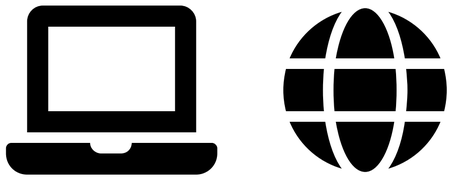
Privacy problems

- People are (partly) responsible for **managing their own privacy**, but...
  - Privacy policies do not inform people (too much + too long + too complicated)
  - Decisions are complex (unintended consequences) + require mental effort and time
  - There is no real / meaningful choice
- Organisations which have your data **'lose' it all the time**
- Privacy is... **complex**
  - Technological developments are moving faster than we can keep up with

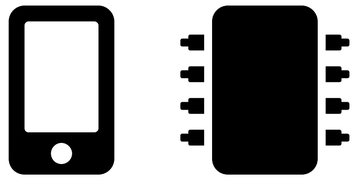
Defining privacy...



1890



1990



2010

What is (informational) privacy?

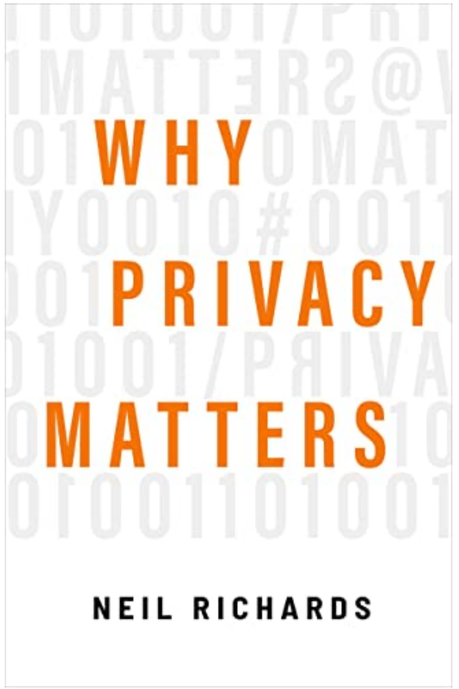
"Privacy is the degree to which human information is neither known nor used"

1. *information* about

2. humans that is

3. used as well as known and is

4. a matter of *degree*



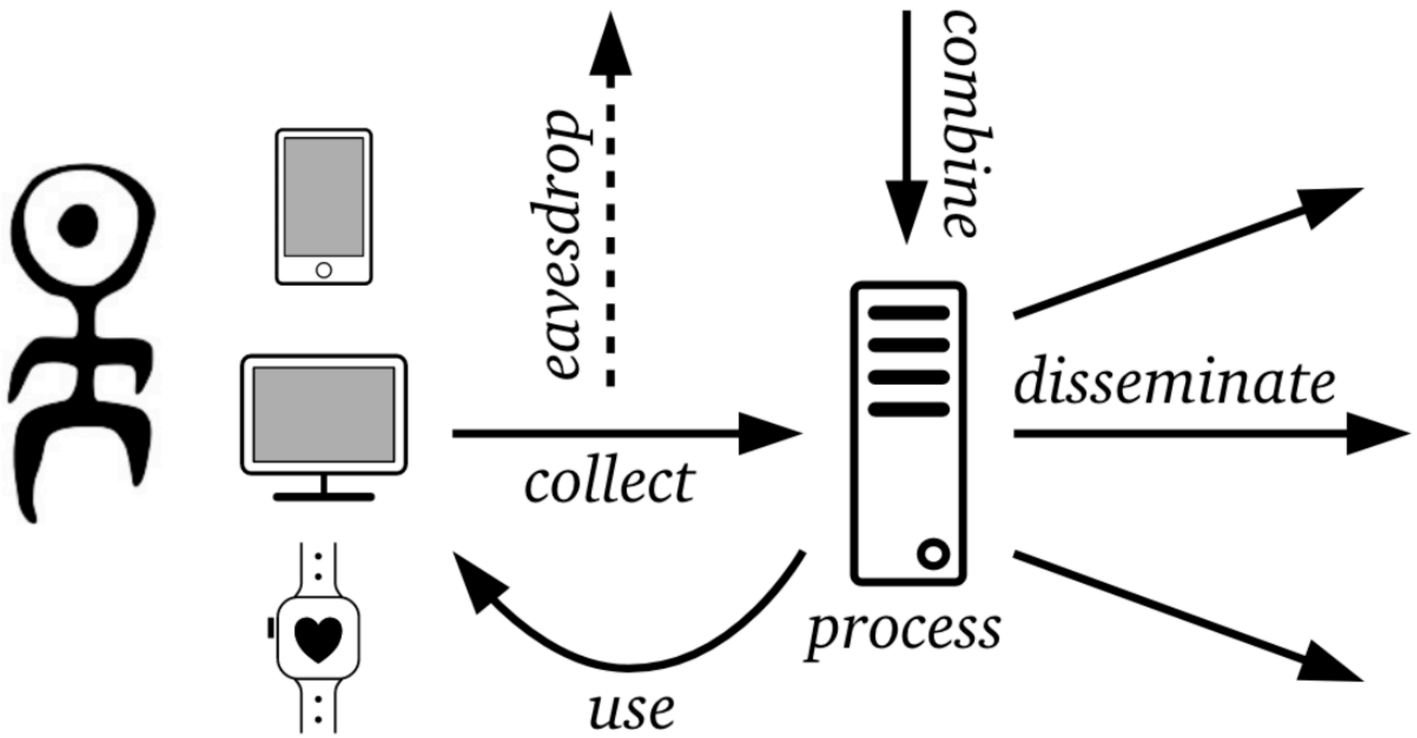
(Neil Richards, "Why Privacy Matters", 2022)

Types of Personal Data

1. **Volunteered**
    - E.g. your name or age
2. **Observed**
    - Time, voice, location, etc.
    - Exhaust data (Zuboff, 2019)
3. **Inferred**
    - E.g. your sex, age, sleeping patterns

World Economic Forum, "Personal Data: The Emergence of a New Asset Class"
http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf

Processing personal data



(Image credit: Jaap-Henk Hoepman, "Privacy Seminar Introduction")

Privacy as Contextual Integrity

- Society is built on **appropriate information flows**
- **Context-specific norms** prescribe what is considered appropriate
- A privacy violation is a **breach of the norm**

- Information flows consist of **5 parameters**:
  1. Sender
  2. Recipient
  3. Information type
  4. Subject
  5. Transmission principle

(Helen Nissenbaum, "Privacy in Context", 2009)

Why privacy matters

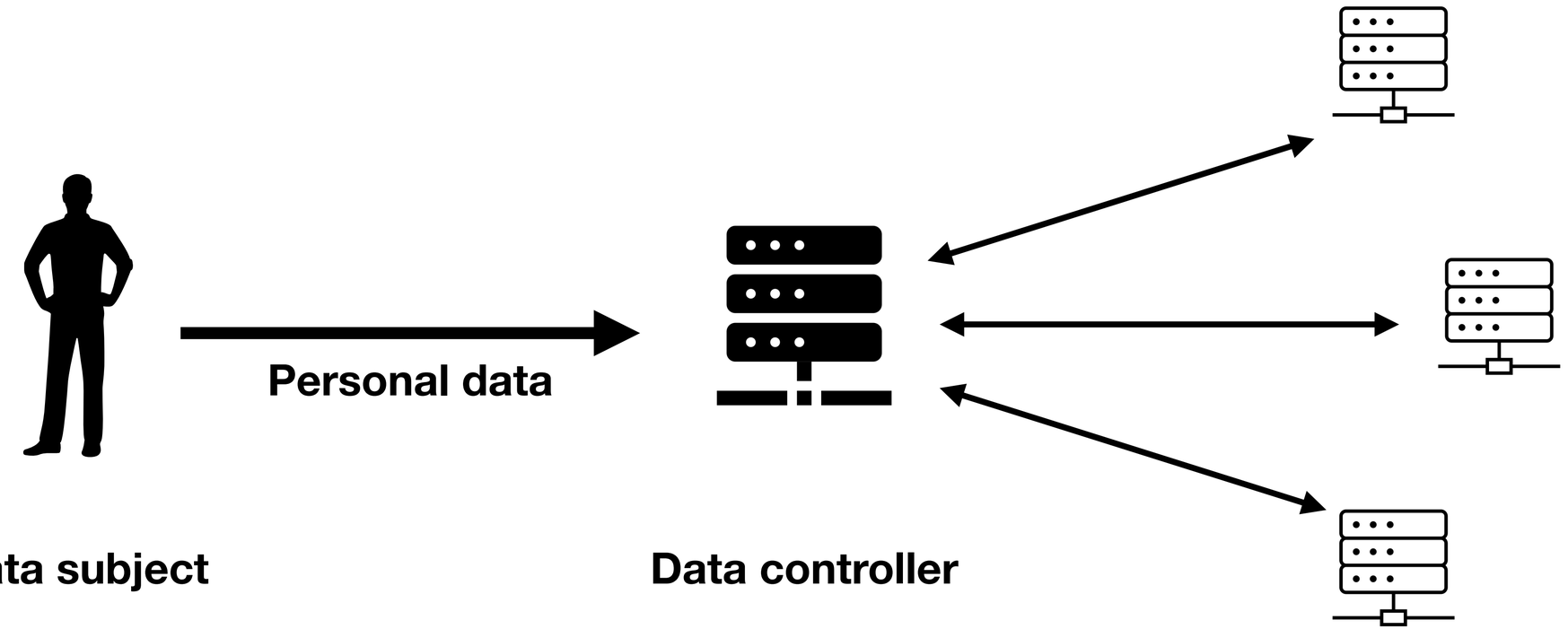
1. Identity
2. Freedom
3. Protection

(Neil Richards, "Why Privacy Matters", 2022)

Regulating personal data: GDPR

- Applies for **processing personal data**...
  - "*'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.*"
  - "*'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.*"

Controller / processor / data subject



- ‘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;

- ‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data **on behalf of the controller**;

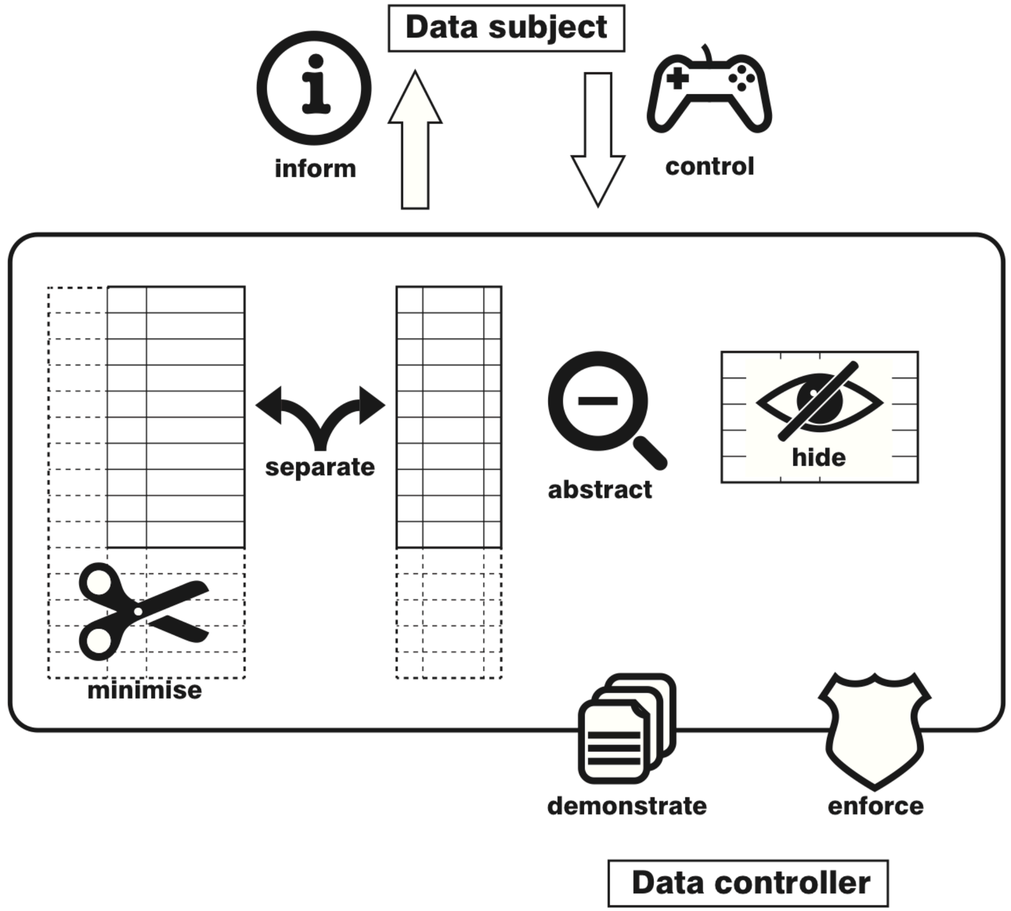
GDPR core principles

- Lawfulness, fairness, transparency
  - Consent, contract, legal obligation, vital interests, public task, legitimate interest
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

Data subject rights

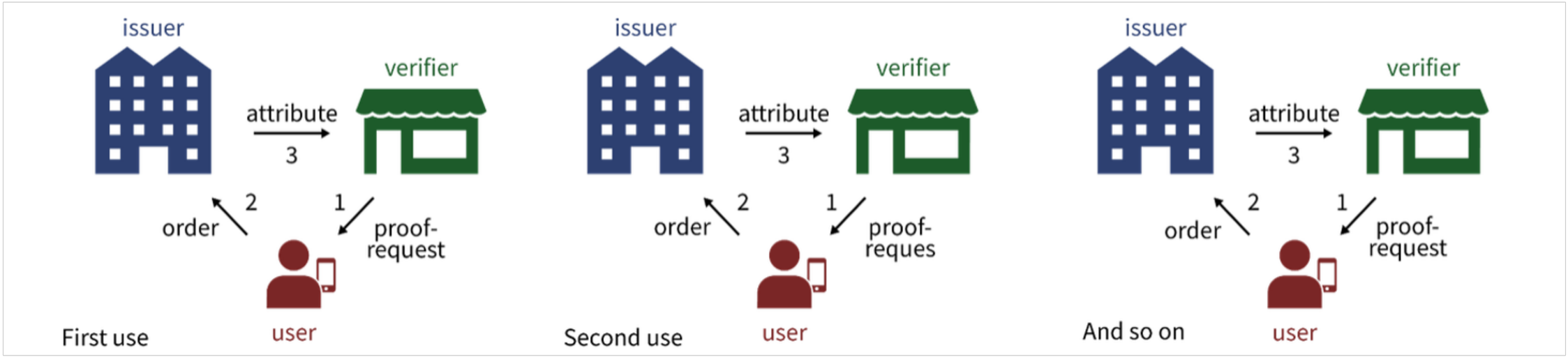
- Right to information
- Right to inspect
- Right to rectification and completion
- Right to be forgotten or to erasure
- Right to restriction of data processing
- Right to data portability
- Right to object
- Right not to be subjected to automated individual decision-making
- Right to revoke consent

Privacy by Design (PbD) strategies

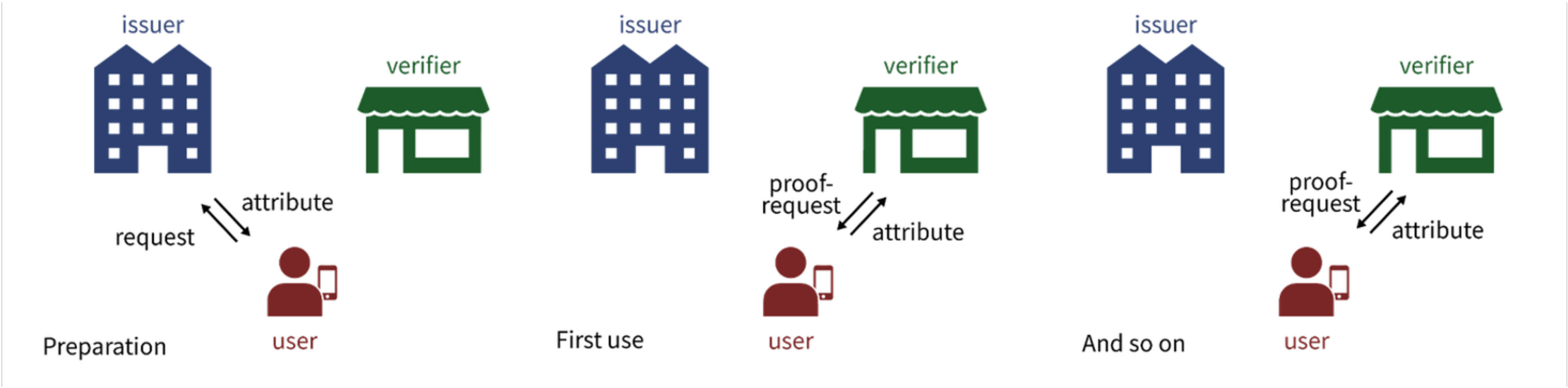


(Jaap-Henk Hoepman, "Privacy Design Strategies (The Little Blue Book)", https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf)

Example: PbD in Identity Management

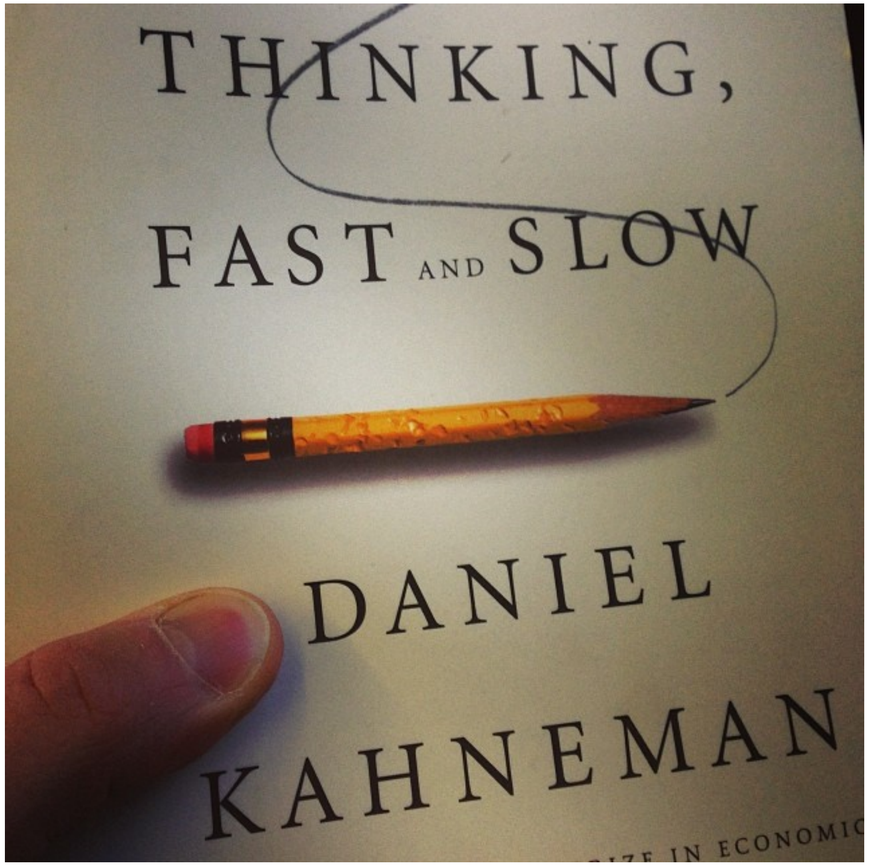


Example: PbD in Identity Management



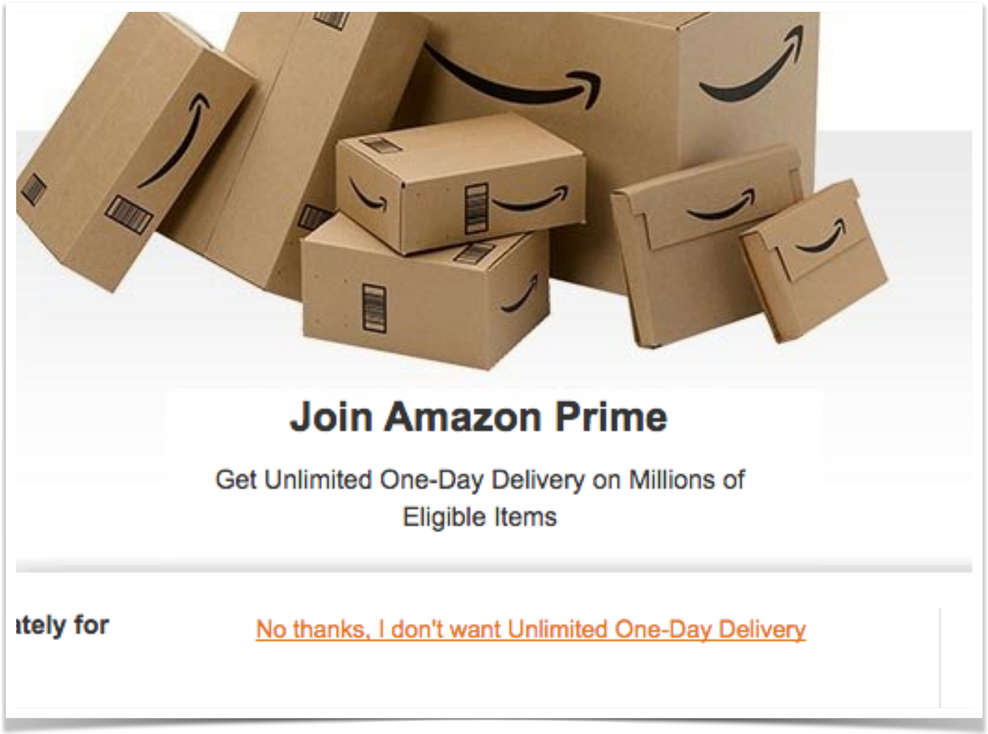
Thinking fast, thinking slow...

- **System 1** (intuitive)
  - Autonomous: fast, nonconscious, automatic, biased...
- **System 2** (reflective)
  - Requires working memory: slow, conscious, abstract, hypothetical thinking...

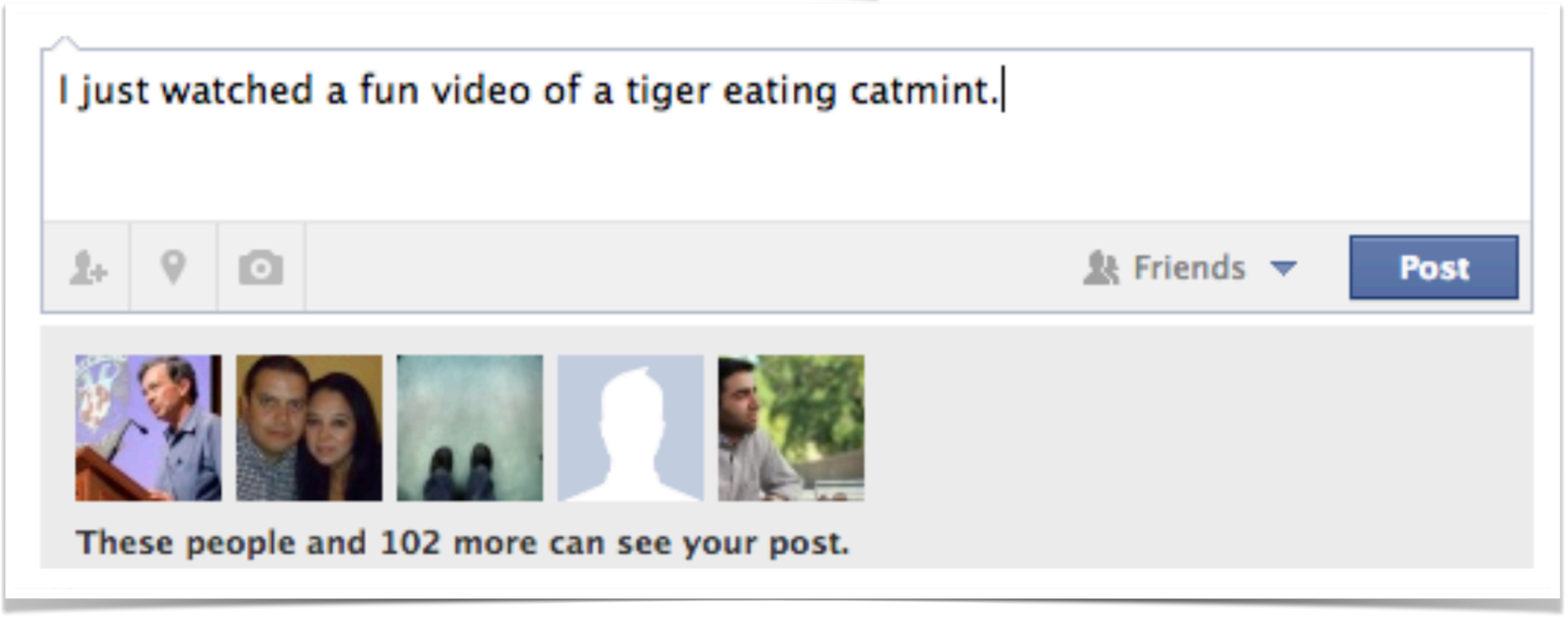


Dark Patterns

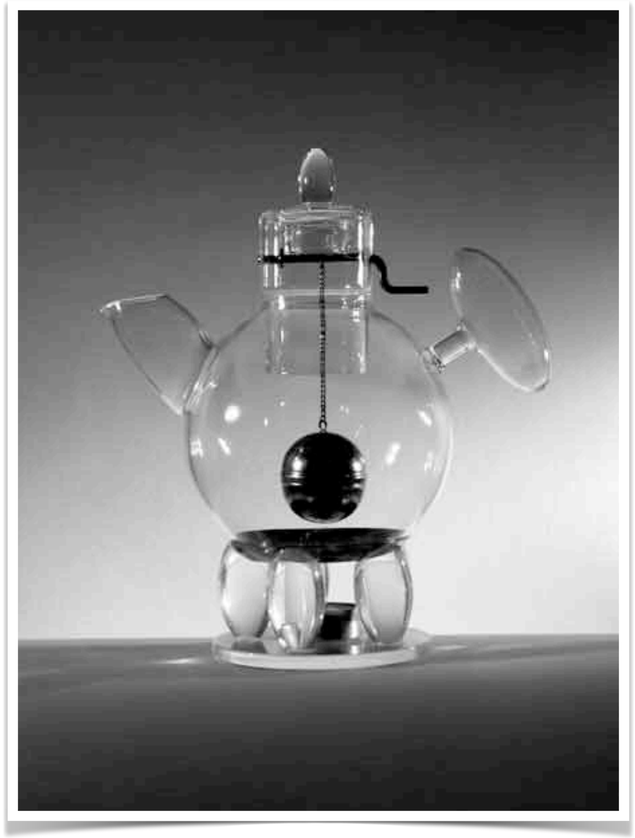
- A dark pattern is "a user interface that has been carefully crafted to trick users into doing things, such as buying overpriced insurance with their purchase or signing up for recurring bills"
- For example, **confirmshaming**
- For more, see darkpatterns.org


Join Amazon Prime
Get Unlimited One-Day Delivery on Millions of Eligible Items
itely for
No thanks, I don't want Unlimited One-Day Delivery

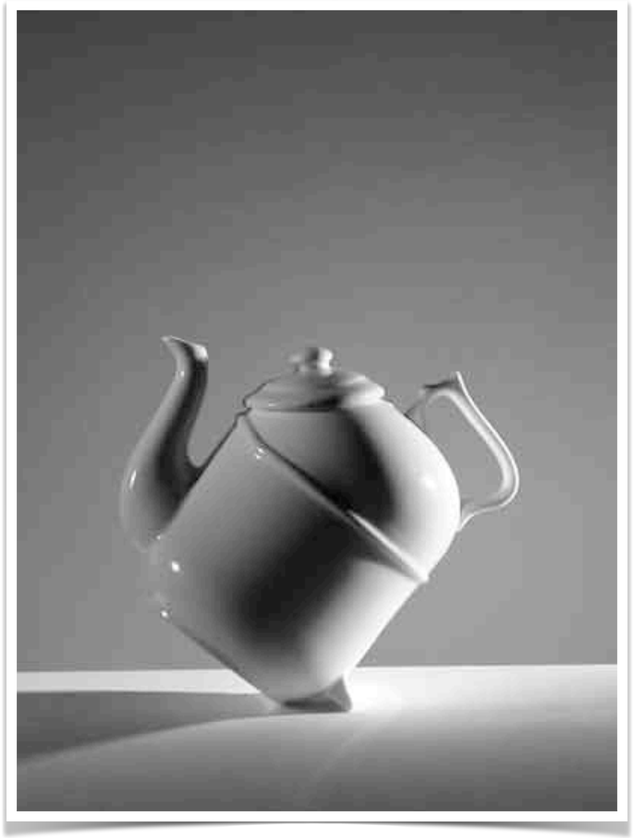

LIEVE
-0,90 CAL
-0,80 CAL
-0,70 CAL
-0,60 CAL
-0,50 CAL
-0,40 CAL
-0,30 CAL
-0,20 CAL
-0,10 CAL


I just watched a fun video of a tiger eating catmint.
Friends
Post
These people and 102 more can see your post.

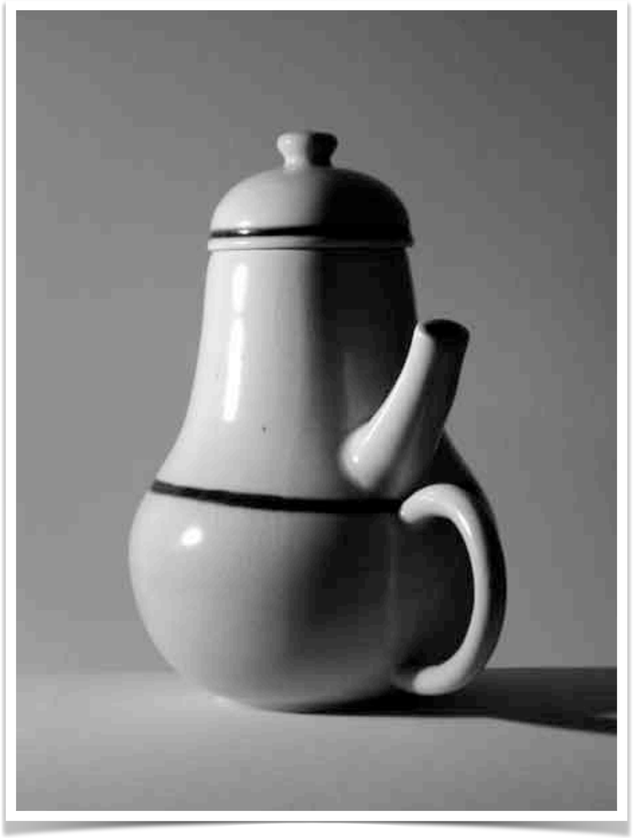
Three levels of design



Visceral



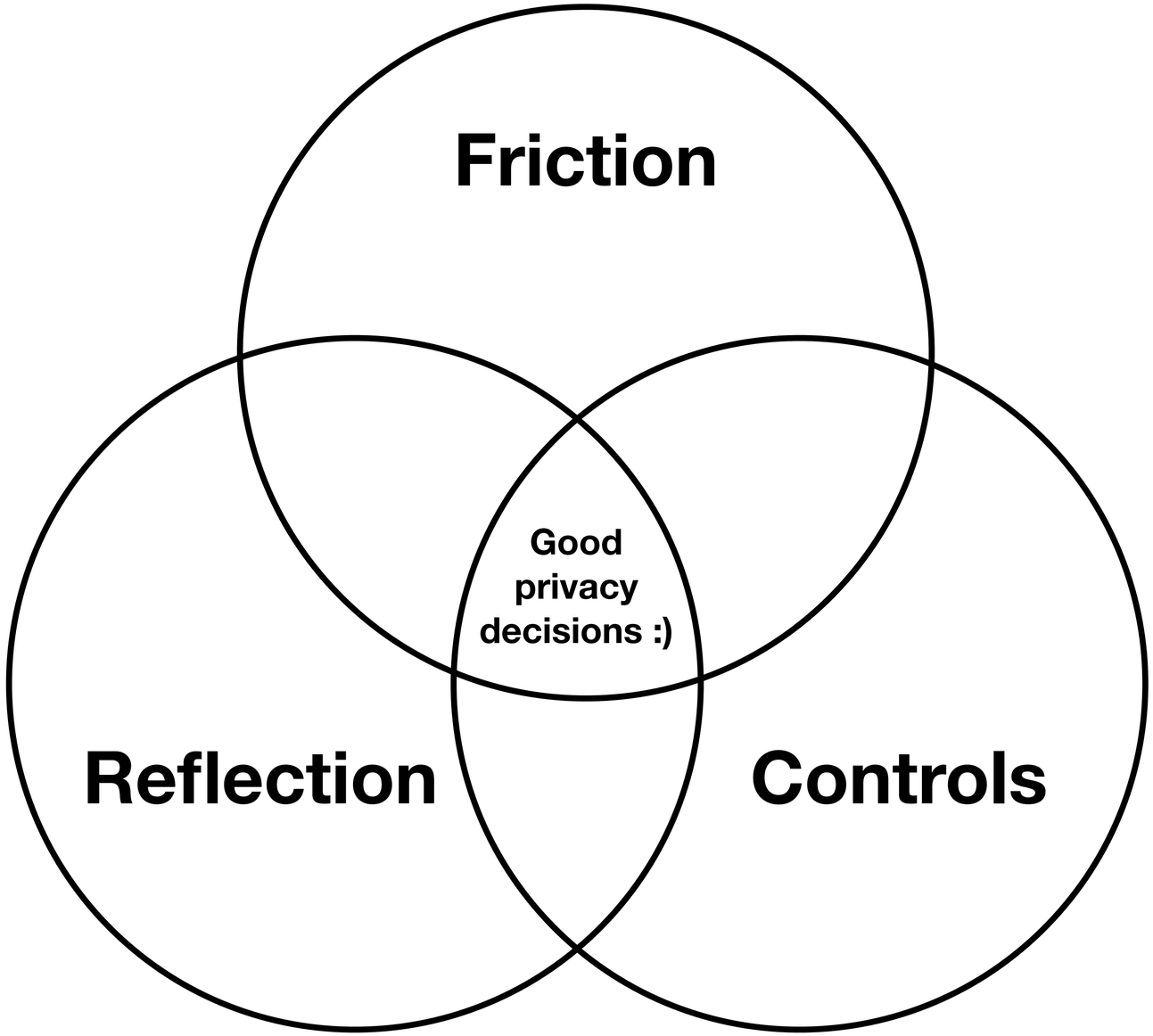
Behavioural



Reflective

(Norman, 2004)

Proposed model (Terpstra *et al.*, 2019)



Friction: only annoying?

- **Frictionless** is the mantra in tech
  - "Until then, apps connected to Facebook would regularly ask users if they wanted to publish their latest activity to their feed on the social network. Those pop-up messages — from apps like Spotify, Netflix and The Washington Post — were annoying, Mr. Zuckerberg said, so the company had created a new category of apps that could post directly to users' feeds, without asking for permission every time.

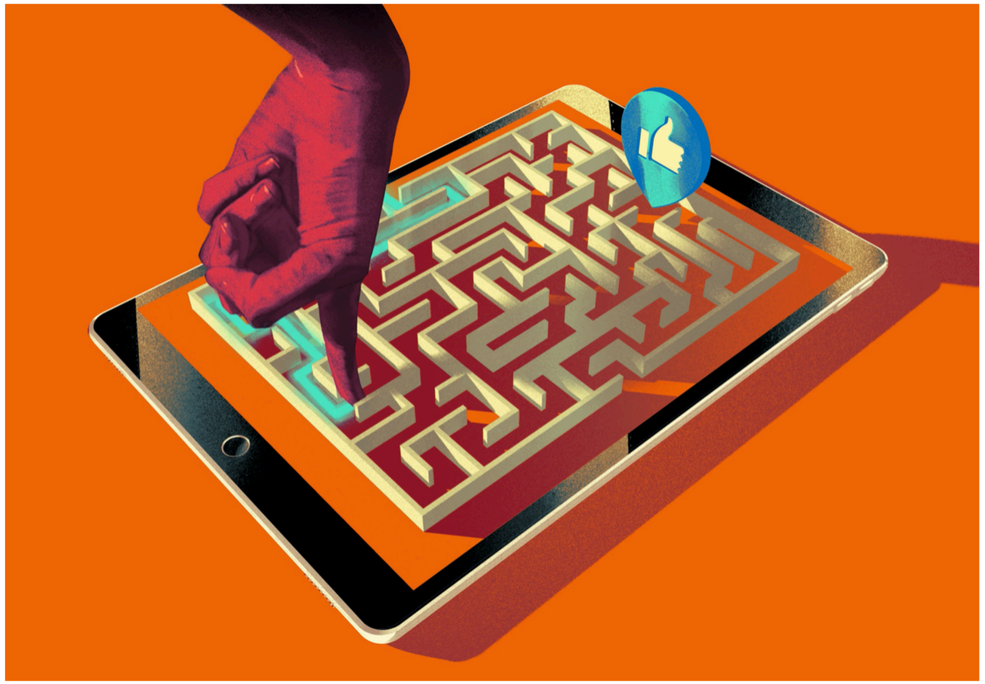
    "From here on out, it's a frictionless experience," Mr. Zuckerberg said."

- Friction **is part of society**
  - Oxford dictionary: "a lack of friendship or agreement among people who have different opinions about something"

The New York Times

THE SHIFT

Is Tech Too Easy to Use?



https://www.nytimes.com/2018/12/12/technology/tech-friction-frictionless.html

Project Alias
http://bjoernkarmann.dk/project_alias

Questions?

arnout.terpstra@surf.nl

@arnoutnl