ERHVERVSAKADEMI
AARHUS

Privacy, GDPR, (PIPEDA)

What is privacy?

ERHVERVSAKADEMI AARHUS

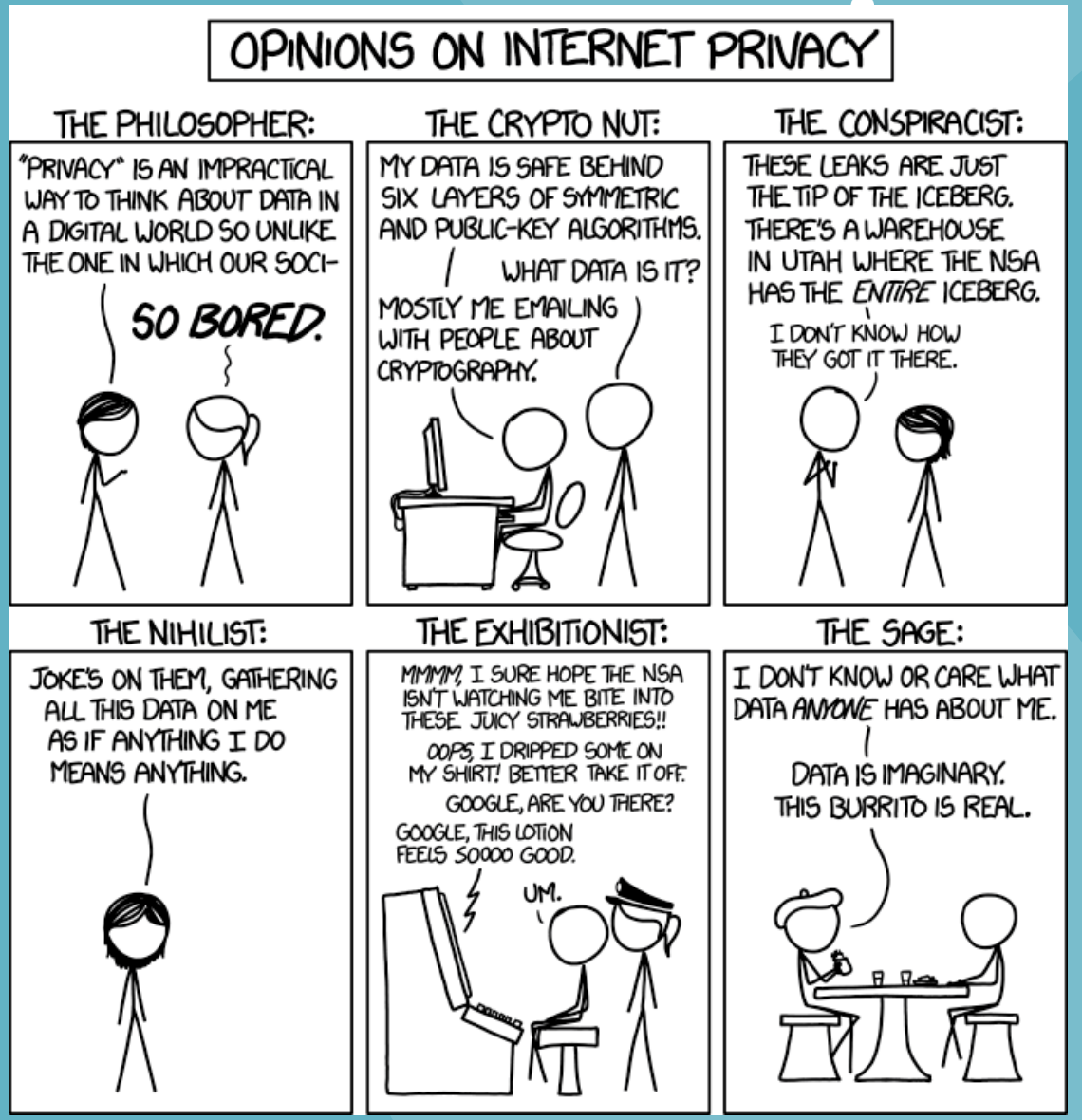
- One definition

Privacy is the right to control who knows certain aspects about you, your communications, and your activities.

- Types of data that many people consider private:
  - Identity
  - Finances
  - Health
  - Biometrics
  - Privileged communications
  - Location data

Round the table

- 1 minute: Individually
  - Write down some current concerns you have regarding privacy and online services?
    - At least three
    - Be specific
    - Why is a concern?
- 7 minutes: group
  - Each member explains **one** of her concerns to the group. Discuss and disagree if applicable.
    - Do you agree?
    - Why or why not?
  - Move to the next member
  - Keep going until time is up
- Start with the group member who has the next birthday



Cathay Pacific: We Are Collecting Your Data

ERHVERVSAKADEMI
ÅARHUS

An update to Cathay Pacific's customer privacy policy makes clear that passengers flying on Cathay Pacific should expect absolutely no privacy. The Hong Kong-based carrier has served notice that everything from favorite in-flight dining choices and seatback entertainment selections to photographs taken onboard and even habits on the ground are fair game for data collection.

WIRED PRIVACY

New indoor tracking tech could stalk your every move

By JAMES TEMPERTON
22 Nov 2014

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTUR

BIZ & IT —

Equifax website hack exposes data for ~143 million US consumers

Breach affecting 44 percent of US population is one of the biggest yet.

DAN GOODIN - 9/8/2017, 12:31 AM

GIZMODO

Cops Are Giving Amazon's Ring Your Real-Time 911 Caller Data

Dell Cameron
8/01/19 4:54pm • Filed to: SURVEILLANCE TECH

28.9K 32 2

World's Biggest Data Breaches & Hacks

Select losses greater than 30,000 records

Last updated: 1 April 2019

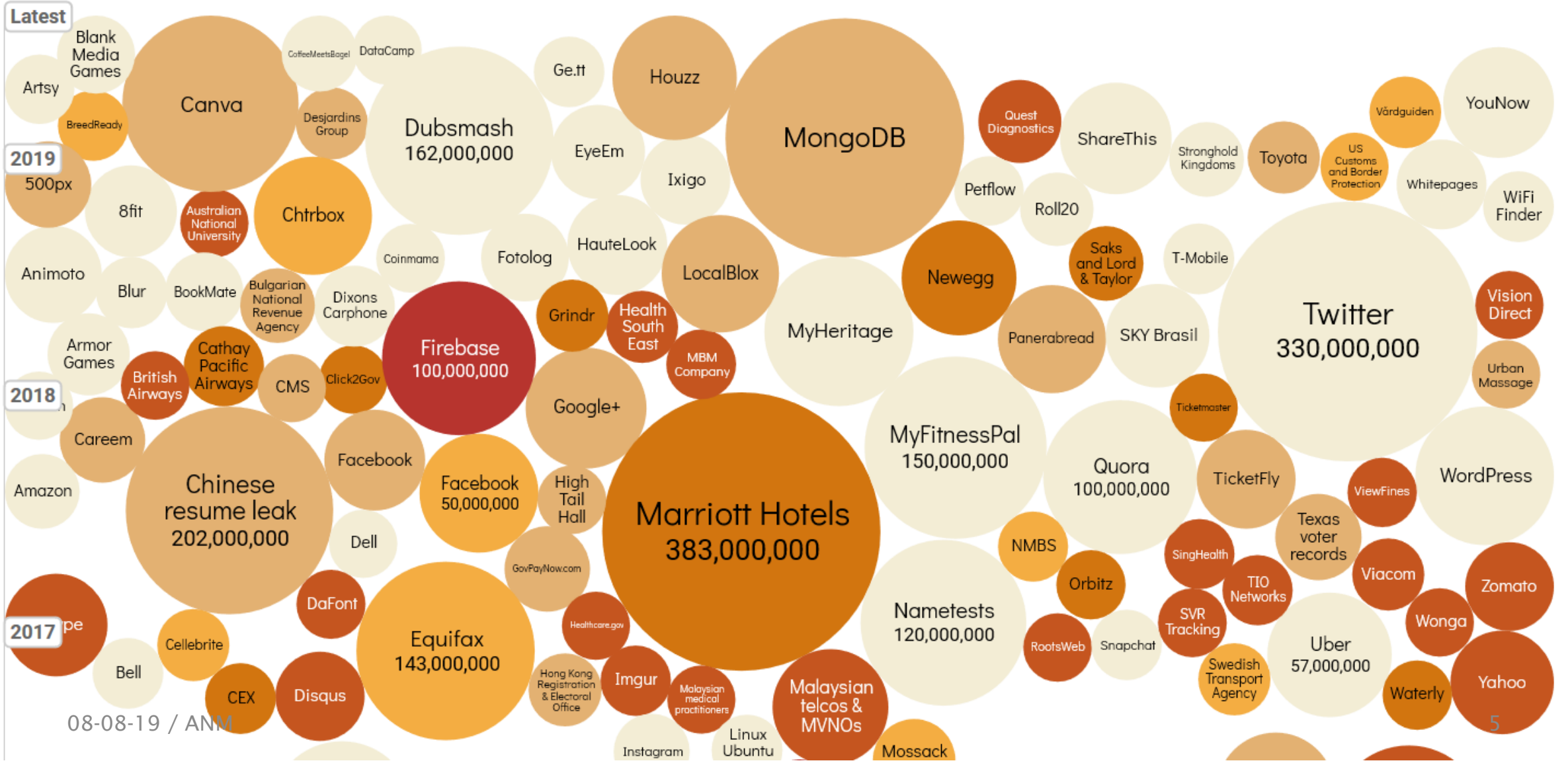
hxxps://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

interesting story

Filter Colour YEAR DATA SENSITIVITY

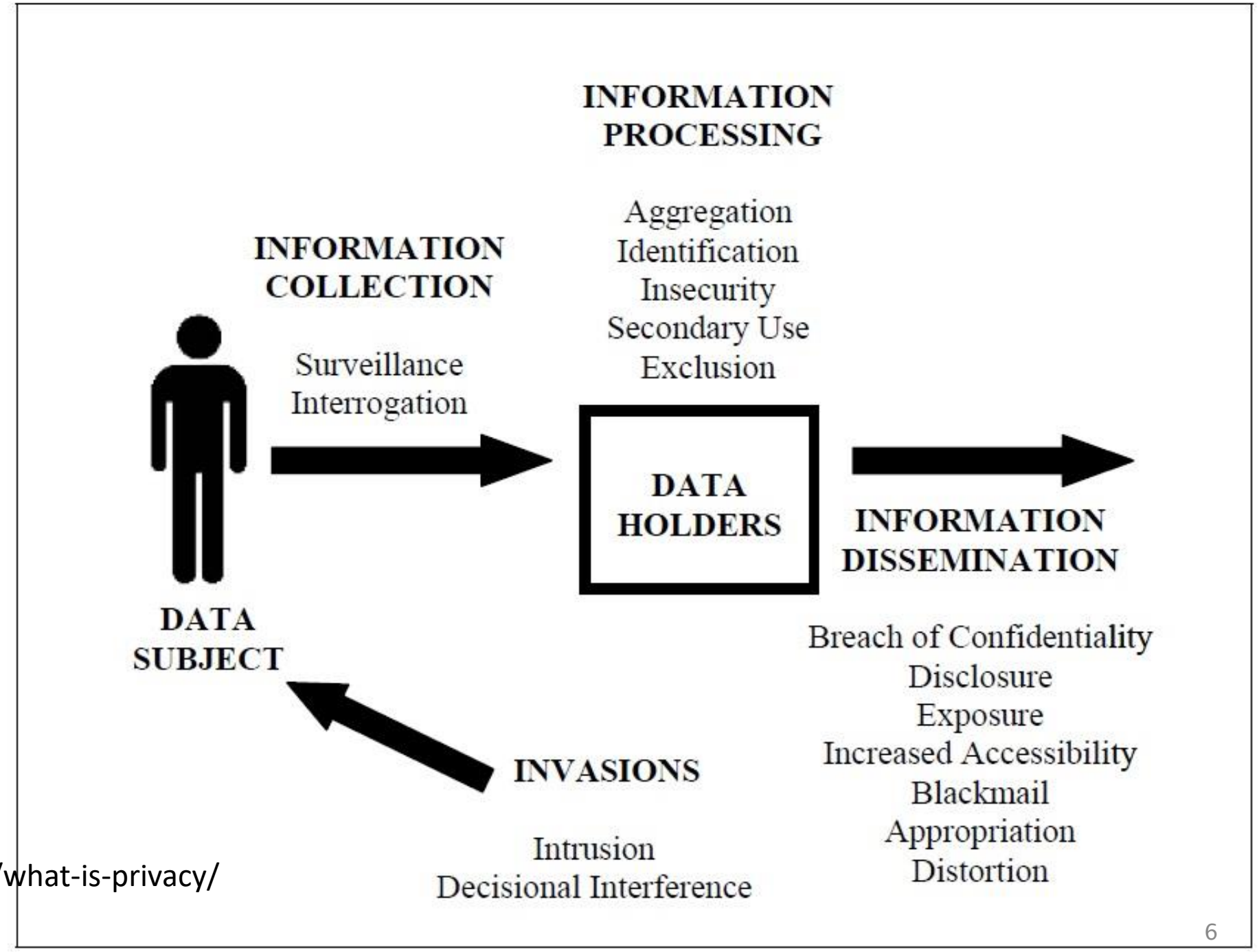
Low High

Search...



Taxonomy of privacy

Daniel J. Solove



https://teachprivacy.com/what-is-privacy/

GDPR - purpose

ERHVERVSAKADEMI AARHUS

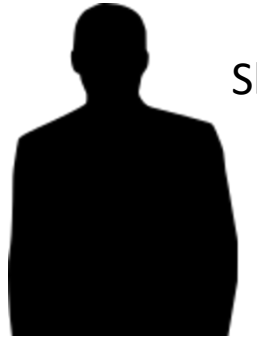
- EU Perspective
  - Protection of personal data is a fundamental right
    - Not an absolute right
  - Support the free exchange of personal data within the EU
  - Aimed at commercial and organizational use of personal data
  - Controller and processer must provide a high level of protection

What does the data subject expect?

ERHVERVSAKADEMI AARHUS

Doesn't understand what he is agreeing to

Shares as little as possible



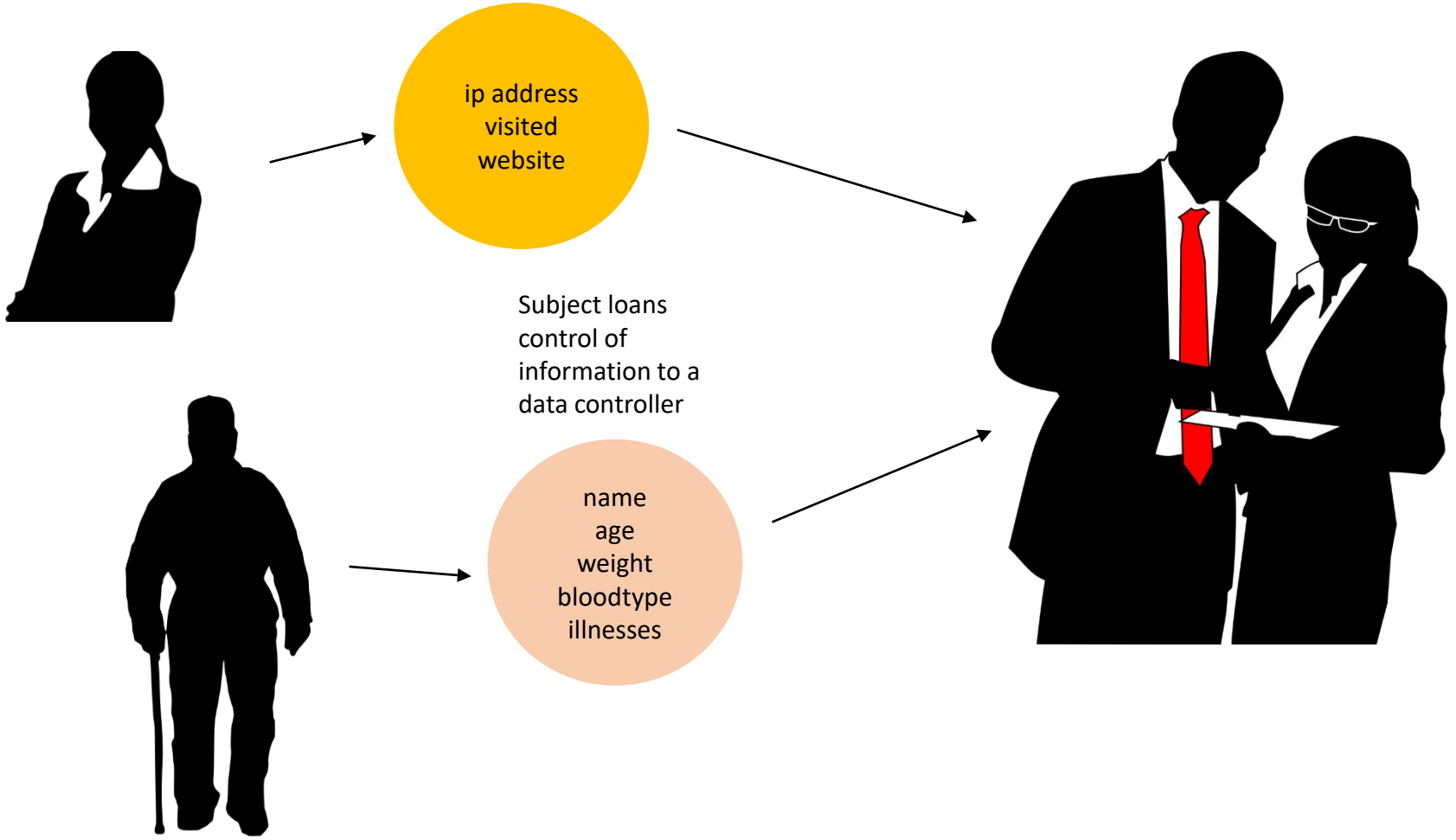
Shares everything – no problem

Shares some things, but wants to control it

Very suspicious, doesn't want to share anything

Subject loans control of her/his own personal information

ERHVERVSAKADEMI AARHUS



What is ”Personal data”

ERHVERVSAKADEMI AARHUS

‘**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;

Article 4(1) GDPR

Personal Data

ERHVERVSAKADEMI AARHUS

What personal data would your application be collecting?

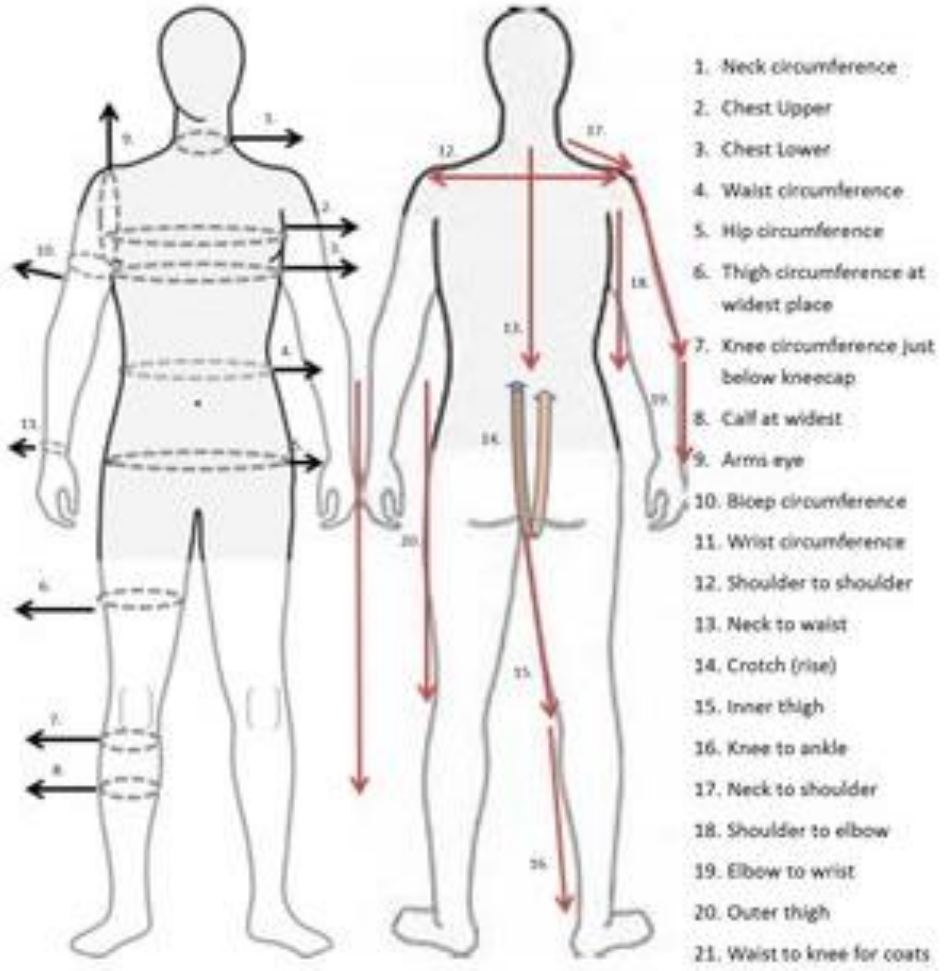
What would be the impact (to the data subject) if it was breached? *stolen, leaked, or deleted*

Personal Data

ERHVERVSAKADEMI AARHUS

Personal Data

- Name
- IP Address
- Grade (Education)
- Age
- Religion
- Union membership
- Digital fingerprint (cookie)
- Credit card number
- Sexual orientation
- Race
- Photo
- Address
- Login credentials
- MAC Address



Personal Data

ERHVERVSAKADEMI AARHUS

Personal Data

- Name
- IP Address
- Grade (Education)
- Age
- Religion
- Union membership
- Digital fingerprint (cookie)
- Credit card number
- Sexual orientation
- Race
- Photo
- Address
- Login credentials
- MAC Address

Sensitive Data (special categories)

- Racial or ethnic origin
- Political opinion
- Religion or beliefs
- Trade union membership
- Genetic or health status
- Sexual orientation

GDPR Principles

ERHVERVSAKADEMI AARHUS

1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner ('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; (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; ('accuracy');

(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; ('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')

Some rights of the data subjects

ERHVERVSAKADEMI AARHUS

- Right of access (Art. 15)
- Right to data portability (Art 20)
- Right to rectification – *the data is accurate* (Art 16)
- Right to erasure (*right to be forgotten*) (Art 17)
- Right to object (Art 21)
- Right not to be subject to a decision based solely on automated processing… (Art 22)

Lawful Basis for Processing

ERHVERVSAKADEMI AARHUS

- Lawful basis for Processing
  - Consent
    - Freely given, Specific, Informed, Unambiguous(clear),
    - **Can be withdrawn**
  - Contractual necessity
  - Compliance with legal obligations
  - Protect the Data Subject's (or another's) vital interests
  - Public interests
  - Legitimate interests
    - Assessment based on weighing the interests of the data controller with respect to the rights of the data subject
    - Does not apply to special personal data

Article 6(1) GDPR

Information to the data subject

ERHVERVSAKADEMI AARHUS

- Not enough to just say ”we collect data about you”
  - what data?
  - for what purpose?
  - for how long?
  - who is it shared with?
  - who can be contacted to see the data, or get it changed or deleted?
  - how can consent be withdrawn?

Lawful Basis for Processing

ERHVERVSAKADEMI AARHUS

Given the data you identified earlier,

What would you use as the lawful basis for processing, why?

What problems could there be with using consent as a lawful basis?

How long should you keep the individual pieces of data?

What other limits could you enact on the data to make it more secure/compliant?

What other challenges do you see?

Security of personal data

ERHVERVSAKADEMI AARHUS

- Security of processing (Art 32)
  - ”the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk” (Article 32,1)
- Notification of a personal data breach to the supervisory authority (Art 33)
  - Within 72 hours of a breach
- Communication of a personal data breach to the data subject (Art 34)
  - In high risk situations, and if other mitigations haven’t been taken

Penalties

ERHVERVSAKADEMI AARHUS

4. Infringements of the following provisions shall… be subject to administrative fines up to **10 000 000 EUR**, or in the case of an undertaking, up to **2 %** of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;
(b) the obligations of the certification body pursuant to Articles 42 and 43;
(c) the obligations of the monitoring body pursuant to Article 41(4).

5. Infringements of the following provisions shall … be subject to administrative fines up to **20 000 000 EUR**, or in the case of an undertaking, up to **4 %** of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;
(b) the data subjects' rights pursuant to Articles 12 to 22;
(c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;
(d) any obligations pursuant to Member State law adopted under Chapter IX;
(e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).

Privacy by design

ERHVERVSAKADEMI AARHUS

- “Privacy by Design refers to the philosophy and approach of embedding privacy into the design, operation and management of information technologies and systems, across the entire information life cycle.
  - Ann Cavoukian, former Information and Privacy Commissioner of Ontario, Canada and now Executive Director of the Privacy and Big Data Institute at Ryerson University.

Privacy by design: 7 Foundational Principles

ERHVERVSAKADEMI AARHUS

1. **Proactive** not Reactive; **Preventative** not Remedial
2. Privacy as the **Default Setting**
3. Privacy **Embedded** into Design
4. Full Functionality — **Positive-Sum**, not Zero-Sum
5. End-to-End Security — **Full Lifecycle Protection**
6. **Visibility** and **Transparency** — Keep it **Open**
7. **Respect** for User Privacy — Keep it **User-Centric**

https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

Discussion

ERHVERVSAKADEMI AARHUS

A person wants to get into a club

what information should they be expected to give to the doorman?

You are stopped by the police while driving,

What information do you think the policeman should get from you?

Compare what information is available on the Danish and the Canadian drivers license – what is the difference?

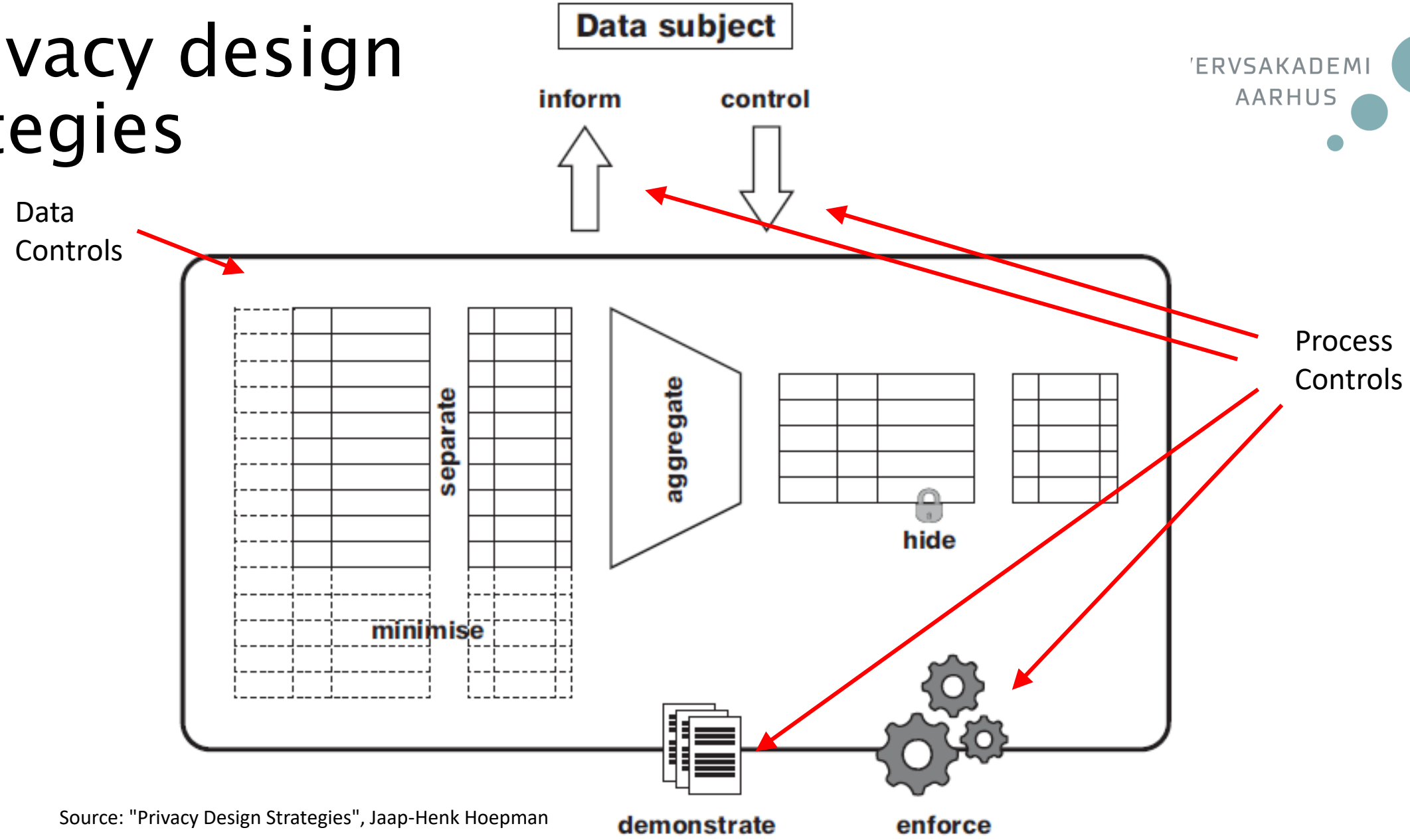
Privacy Enhancing Technologies (PET) Not that PET

ERHVERVSAKADEMI
AARHUS

"**Privacy-Enhancing Technologies** is a system of ICT measures protecting informational privacy by eliminating or minimising personal data thereby preventing unnecessary or unwanted processing of personal data, without the loss of the functionality of the information system."

Kilde: "Privacy Design Strategies", Jaap-Henk Hoepman

8 Privacy design strategies



Source: "Privacy Design Strategies", Jaap-Henk Hoepman

	Purpose limitation	Data minimisation	Data quality	Transparency	Data subject rights	The right to be forgotten	Adequate protection	Data portability	Data breach notification	(Provable) Compliance
MINIMISE	o	+								
HIDE		+					o			
SEPARATE	o						o			
AGGREGATE	o	+								
INFORM				+	+				+	
CONTROL			o		+			+		
ENFORCE	+		+			+	+			o
DEMONSTRATE										+

Legend: +: covers principle to a large extent. o: covers principle to some extent.

Table 1. Mapping of strategies onto legal principles.

Source: "Privacy Design Strategies", Jaap-Henk Hoepman

GDPR, Data Privacy, Anonymization, Minimization. . .Oh My!

Steve Touw, Immuta

I know stuff about Judd and Leslie!

Photo credit: Gawker

New York Taxi & Limousine Commission

Data was released containing taxi pickups, dropoffs, location, time, amount, and tip amount, among others. Seems pretty harmless?

taxi_medallion	pickup_datetime	dropoff_datetime	pickup_longitude	pickup_latitude	dropoff_longitude	dropoff_latitude	total_amount	tip_amount
8G12	2013-06-21 11:28:00	2013-06-21 11:35:00	-74.010826	40.719646	-74.005341	40.737122	9.6	2.1

Well, Judd and Leslie May Not Think It's Harmless

This photos was geotagged (with time), so by simply querying by medallion and time, we know how much Judd and Leslie tip!

taxi_medallion	pickup_datetime	dropoff_datetime	pickup_longitude	pickup_latitude	dropoff_longitude	dropoff_latitude	total_amount	tip_amount
8G12	2013-06-21 11:28:00	2013-06-21 11:35:00	-74.010826	40.719646	-74.005341	40.737122	9.6	2.1

This Is An Example Of a Link Attack

Medallion & Pickup Time

Medallion & Photo Time

I Swear This Is Relevant...

Back To GDPR

Yes...This Means

The New York Taxi Commission has personal data by GDPR definition (we identified individuals indirectly).

GDPR would apply to the New York Taxi Commission (but probably only if the data was generated in an EU city)!

Are you having an oh no moment?

GDPR Purpose Restrictions

No room for interpretation

Consent: personal data may be processed on the basis that the data subject has consented to such processing

Contractual necessity: processing is necessary in order to enter into or perform a contract with the data subject

Compliance with legal obligations

Vital interests: this essentially applies in "life-or-death" scenarios

Public interest: necessary for the performance of tasks carried out by a public authority or private organisation acting in the public interest

Legitimate Interests: must be specified at time of collection and reasonable (accountability on the data controller)

Room for interpretation by an auditor - riskier

Processing Principles

Fair, lawful and transparent processing: ability to tell the data subject what their data is being used for

The purpose limitation principle: what we just discussed

Data minimisation: only process the personal data that it actually needs to process in order to achieve its goals

Accuracy: responsibility for taking all reasonable steps to ensure that personal data are accurate

Data retention periods: data should not be retained for longer than necessary in relation to the purposes for which they were collected

Data security: data are kept secure, both against internal and external threats

Accountability: enforcement of the Data Protection Principles

Those Principles and Purposes are Scary...Maybe…

"Once a dataset is **truly anonymised** and individuals are no longer identifiable, **European data protection law no longer applies**."

-Article 29 Working Party

Bibliography and Resources

ERHVERVSAKADEMI AARHUS

- Privacy
  - https://teachprivacy.com/what-is-privacy/
  - https://teachprivacy.com/privacy-by-design-resources/
  - https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf
- GDPR
  - https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679#d1e40-1-1
- GDPR vs PIPEDA
  - https://iapp.org/news/a/matchup-canadas-pipeda-and-the-gdpr/
- Privacy Design Strategies
  - https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf
  - https://www.researchgate.net/publication/232642524_Privacy_Design_Strategies
- DPIA
  - https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

References

ERHVERVSAKADEMI AARHUS

- Title slide: https://www.rferl.org/a/afghan-women-proud-to-cast-vote-/25325688.html
- Slide 3: https://xkcd.com/1269/
- Slide 4:
  - WIRED: https://www.wired.co.uk/article/new-technology-can-track-you-indoors
  - Cathay Pacific: https://www.flyertalk.com/articles/cathay-pacific-passengers-not-to-expect-any-privacy.html
  - Cathay Pacific image: https://boingboing.net/2019/08/02/what-cld-go-rong.html
  - Equifax: https://arstechnica.com/information-technology/2017/09/equifax-website-hack-exposes-data-for-143-million-us-consumers/
  - Ring: https://gizmodo.com/cops-are-giving-amazons-ring-your-real-time-911-data-1836883867
- Slide 5: https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
- Slide 28-37: https://conferences.oreilly.com/strata/strata-eu-2017/public/schedule/detail/57693