



Maximizing Data Minimization

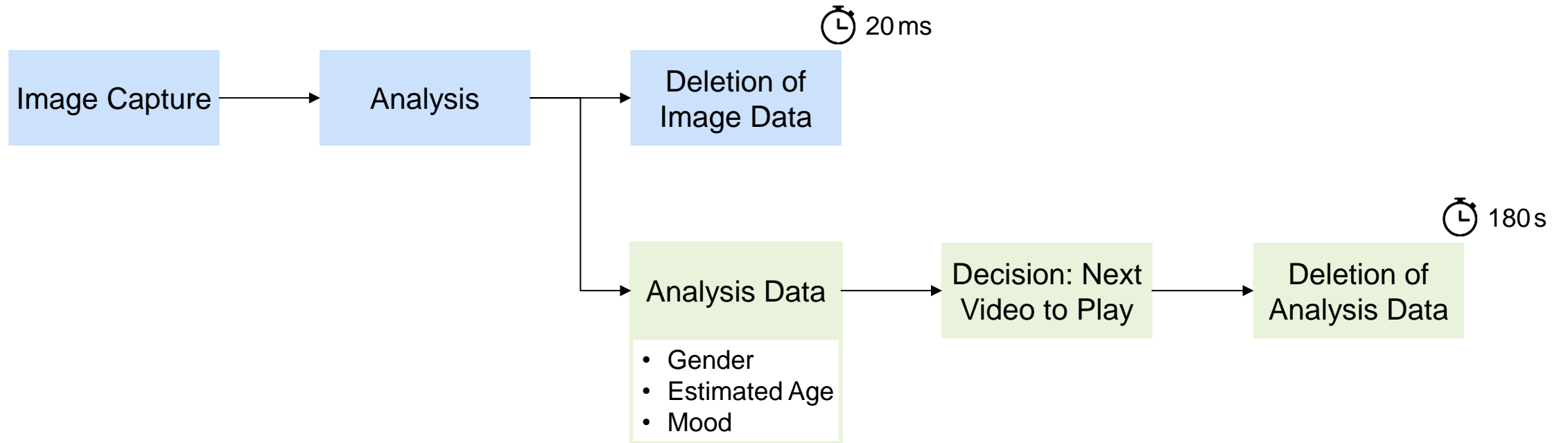
Identifying Problems with Non-Identifiable Data

Geneva Internet L@w Research Colloquium – June 22, 2018

Damian George, Kento Reutimann, Aurelia Tamò Larrieux



AdPack



Implications



Age 85 [+/-13]

Gender Male

Angry

Happy

Sad

Surprised



Age 62 [+/-8]

Gender Female

Angry

Happy

Sad

Surprised

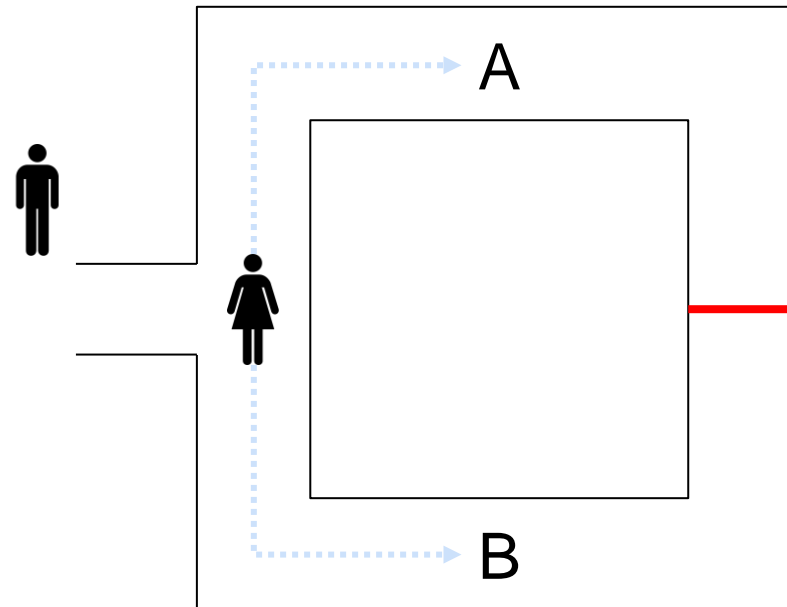


Autonomous Vehicles





Zero Knowledge Proof The Ali Baba Cave



1x → 1/2 (50%)

5x → 1/32 (3.125%)

20x → 1/1048576 (0.000001)



Zero Knowledge Proof Application in Casinos





Summaries

AdPack

- Objective: Anonymous characteristics to show ads
- Images as a technical necessity
- "Personalization" of ads

Autonomous Vehicles

- Objective: Obstacle recognition to avoid accidents
- Images as a technical necessity
- Identification of persons is neither necessary nor intended

ZK Proofs

- Objective: Proof of certain personal characteristics without revealing the actual information
- Third-party required to approve information



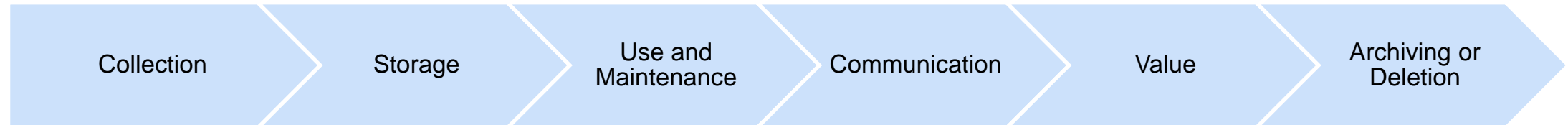
Article 2 of the GDPR: Material Scope

1. This Regulation applies to the **processing** of the **personal data** wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

[...]



Processing





Personal Data

Article 4 of the GDPR: Definitions

For the purposes of this Regulation:

- (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;

[...]



Personal Data Recital 26 of the GDPR

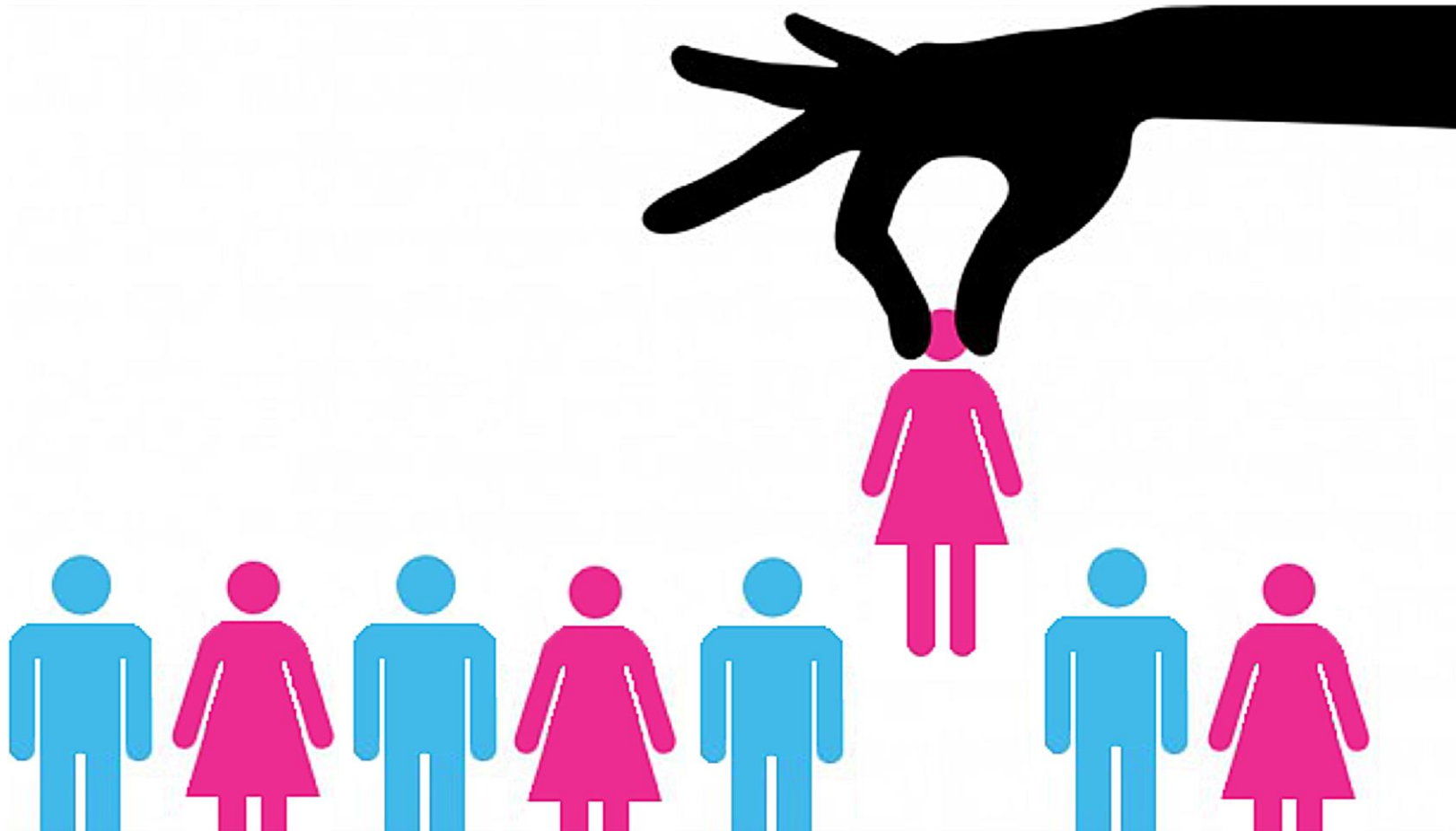
[...] **To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly.** To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information [...].

Personal Data – Identifiability





Personal Data – Singling out



Implications: AdPack



Age 85 [+/-13]


Gender Male

Angry

Happy

Sad

Surprised

 20ms



Age 62 [+/-8]


Gender Female

Angry

Happy

Sad

Surprised

 180s



Article 11 of the GDPR: Processing which does not require identification

1. If the purposes for which a controller processes personal data **do not or do no longer require the identification of a data subject** by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation.
2. Where, in cases referred to in paragraph 1 of this Article, the controller is able to **demonstrate that it is not in a position to identify the data subject**, the controller shall inform the data subject accordingly, if possible. In such cases, **Articles 15 to 20 shall not apply** except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification.



Article 11 of the GDPR: Processing which does not require identification

1. If the purposes for which a controller processes personal data **do not or do no longer require the identification of a data subject** by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation.
2. Where, in cases referred to in paragraph 1, **the controller is able to demonstrate that it is not in a position to identify the data subject**, the controller shall inform the data subject accordingly, if possible. In such cases, **Articles 15 to 20 shall not apply**, except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification.

Article 15: Right of access by the data subject
Article 16: Right to rectification
Article 17: Right to erasure ('right to be forgotten')
Article 18: Right to restriction of processing
Article 19: Notification obligation regarding rectification or erasure of personal data or restriction of processing
Article 20: Right to data portability



© marketoonist.com



Questions

- How far shall the scope of the GDPR reach and is there a need to re-think our "privacy approach" in Europe?
- What further technologies could be classified as "GDPR bypass technologies" and do they stir up controversies?
- When applying the single-out approach of the GDPR (see Recital 26), could the fact that based on his or her facial features a person is assigned to a category and subsequently targeted with specific ads be sufficient for the GDPR's applicability?
- While Data Protection Authorities – e.g. the Bavarian Data Protection Authority in the case of AdPack – see "sensing" technologies as falling outside the scope of the GDPR, civil society groups firmly advocate for the opposite understanding. How can we balance these viewpoints?