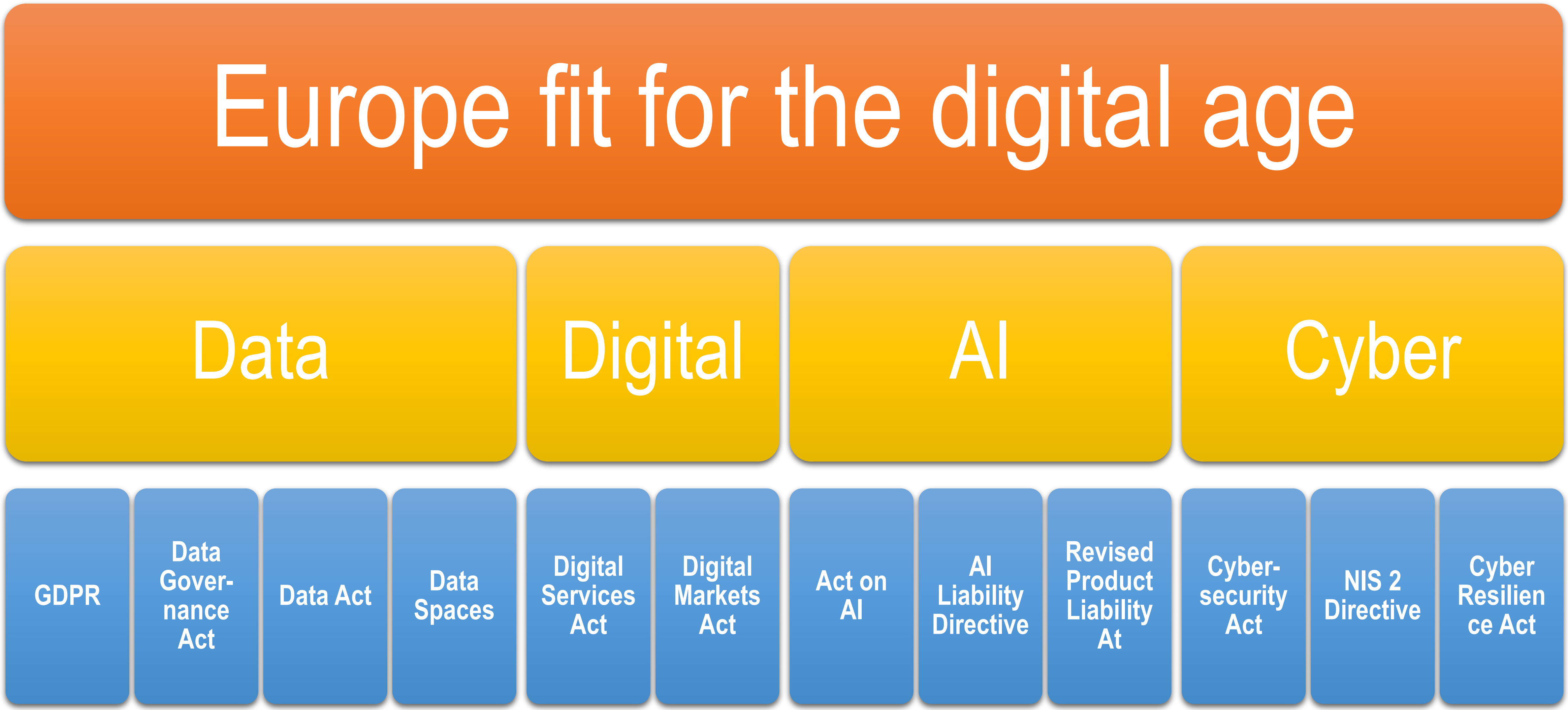
UZ LEUVEN

The triangular relationship between data subject, holder and user

SAMEN GRENZEN VERLEGGEN

Data driven Innovation in Personalised Medicine and Care
Prof. dr. Griet Verhenneman, 23 November 2023

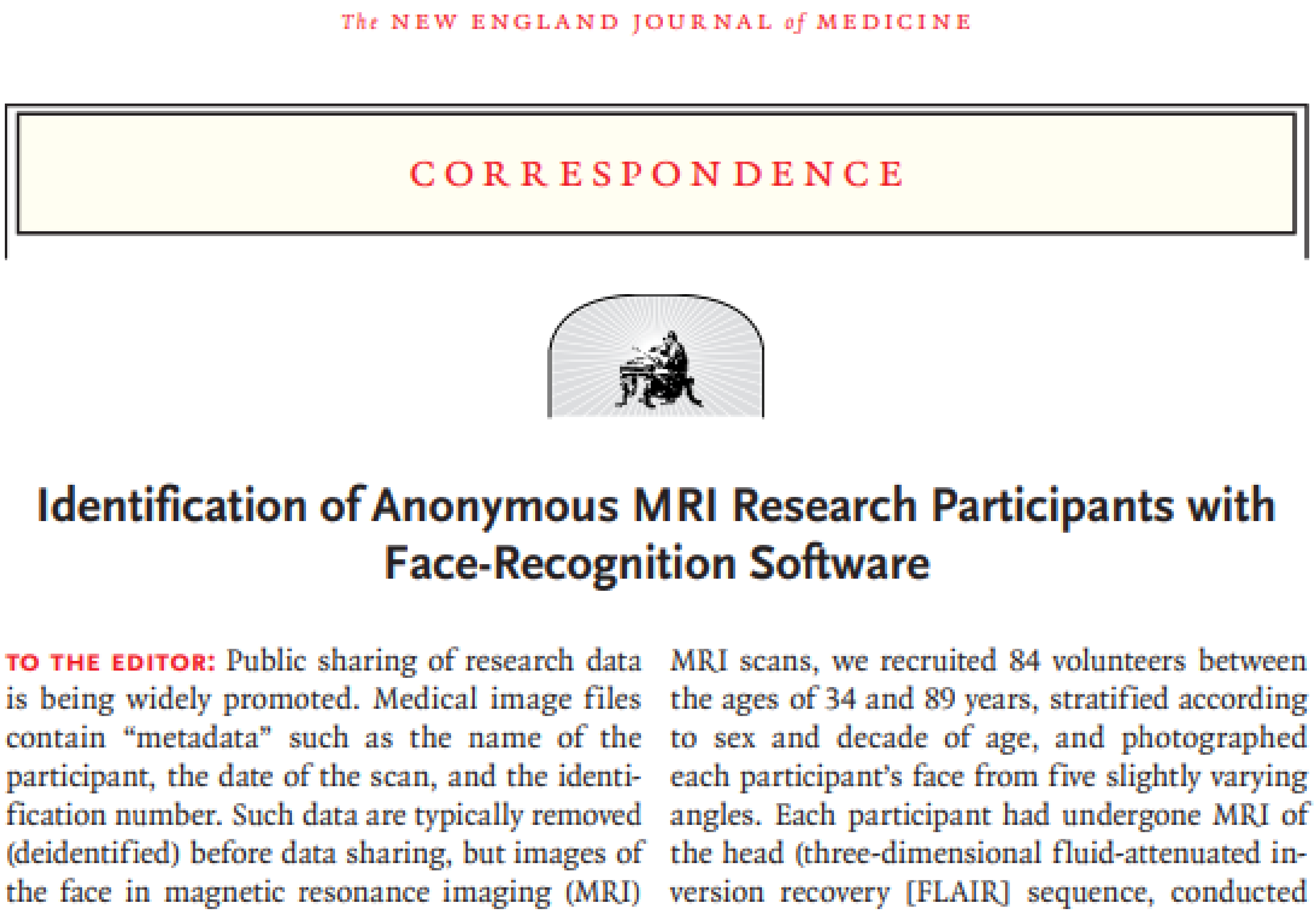


Europe fit for the digital age

- Data
  - GDPR
  - Data Governance Act
  - Data Act
  - Data Spaces
- Digital
  - Digital Services Act
  - Digital Markets Act
- AI
  - Act on AI
  - AI Liability Directive
  - Revised Product Liability At
- Cyber
  - Cybersecurity Act
  - NIS 2 Directive
  - Cyber Resilience Act

Progress in:

- Technical measures that enhance privacy, such as federated learning
- Data custodianship versus data ownership
- Lawfulness of secondary use

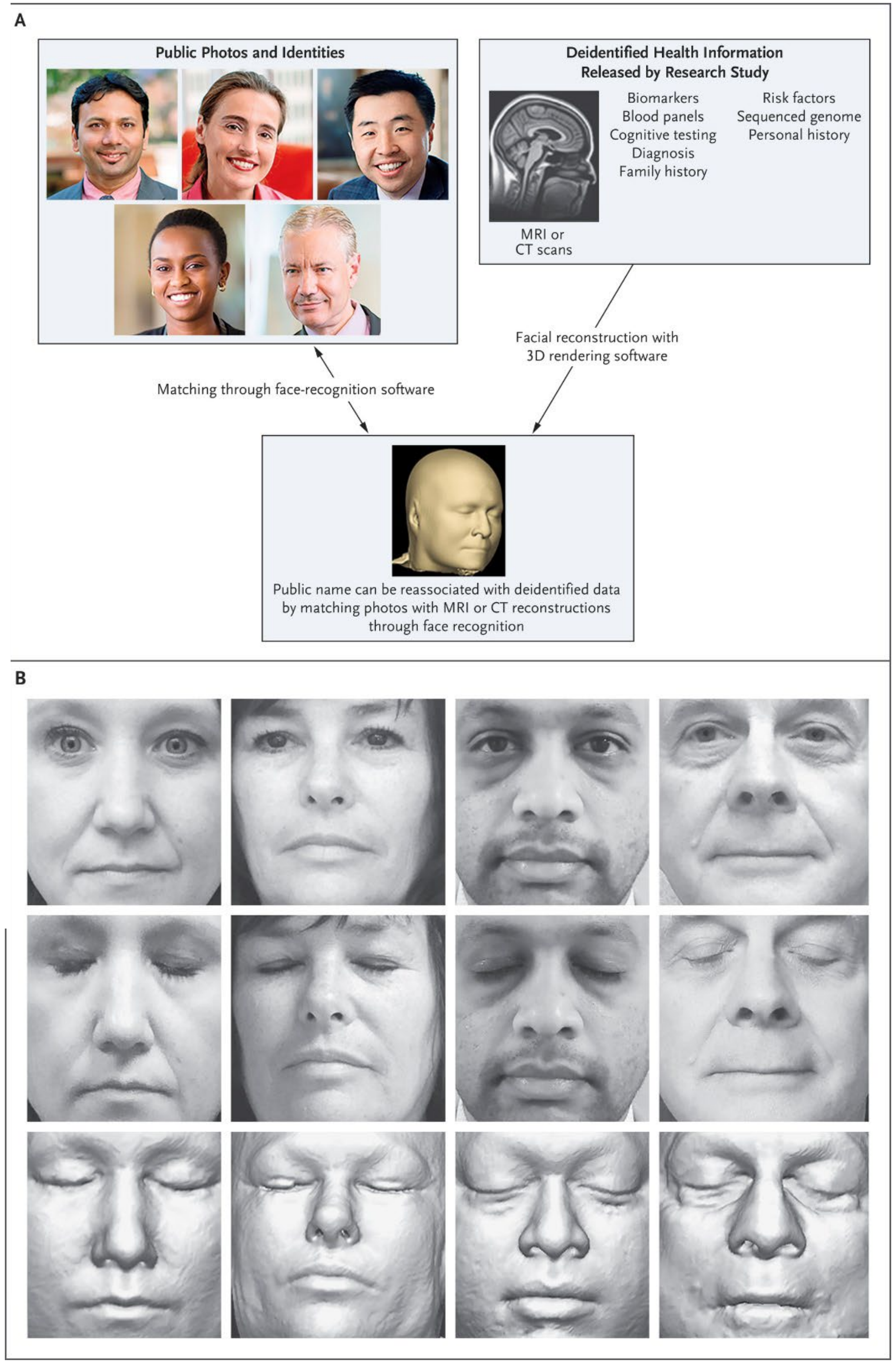


The NEW ENGLAND JOURNAL of MEDICINE

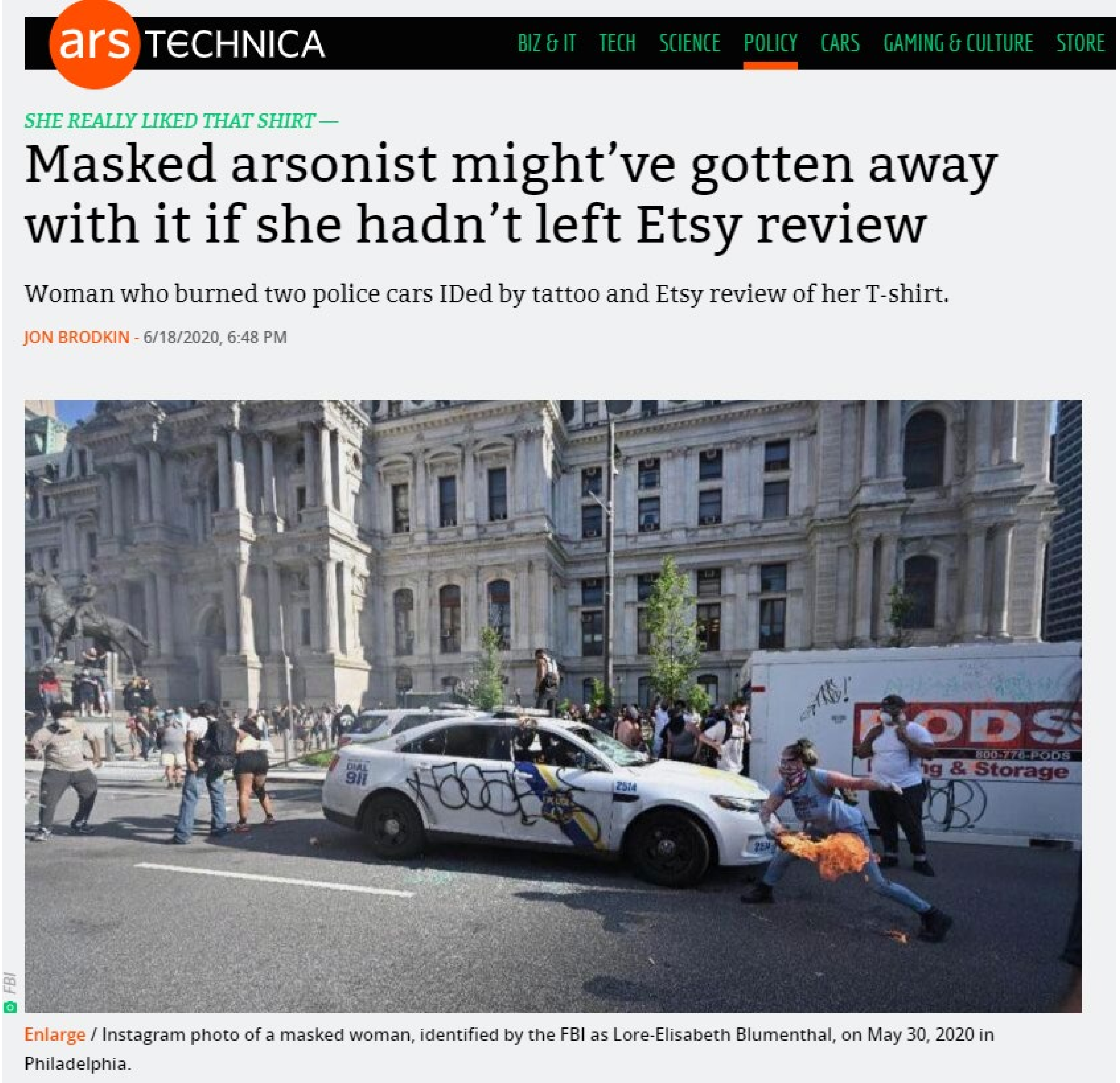
CORRESPONDENCE

Identification of Anonymous MRI Research Participants with Face-Recognition Software

TO THE EDITOR: Public sharing of research data is being widely promoted. Medical image files contain “metadata” such as the name of the participant, the date of the scan, and the identification number. Such data are typically removed (deidentified) before data sharing, but images of the face in magnetic resonance imaging (MRI) MRI scans, we recruited 84 volunteers between the ages of 34 and 89 years, stratified according to sex and decade of age, and photographed each participant’s face from five slightly varying angles. Each participant had undergone MRI of the head (three-dimensional fluid-attenuated inversion recovery [FLAIR] sequence, conducted


A
Public Photos and Identities
Deidentified Health Information
Released by Research Study
Biomarkers
Blood panels
Cognitive testing
Diagnosis
Family history
Risk factors
Sequenced genome
Personal history
MRI or
CT scans
Facial reconstruction with
3D rendering software
Matching through face-recognition software
Public name can be reassociated with deidentified data
by matching photos with MRI or CT reconstructions
through face recognition
B

See: C. Schwarz e.a., “Identification of Anonymous MRI Research Participants with Face-Recognition Software, NEJM, 2019, 1684-1689.



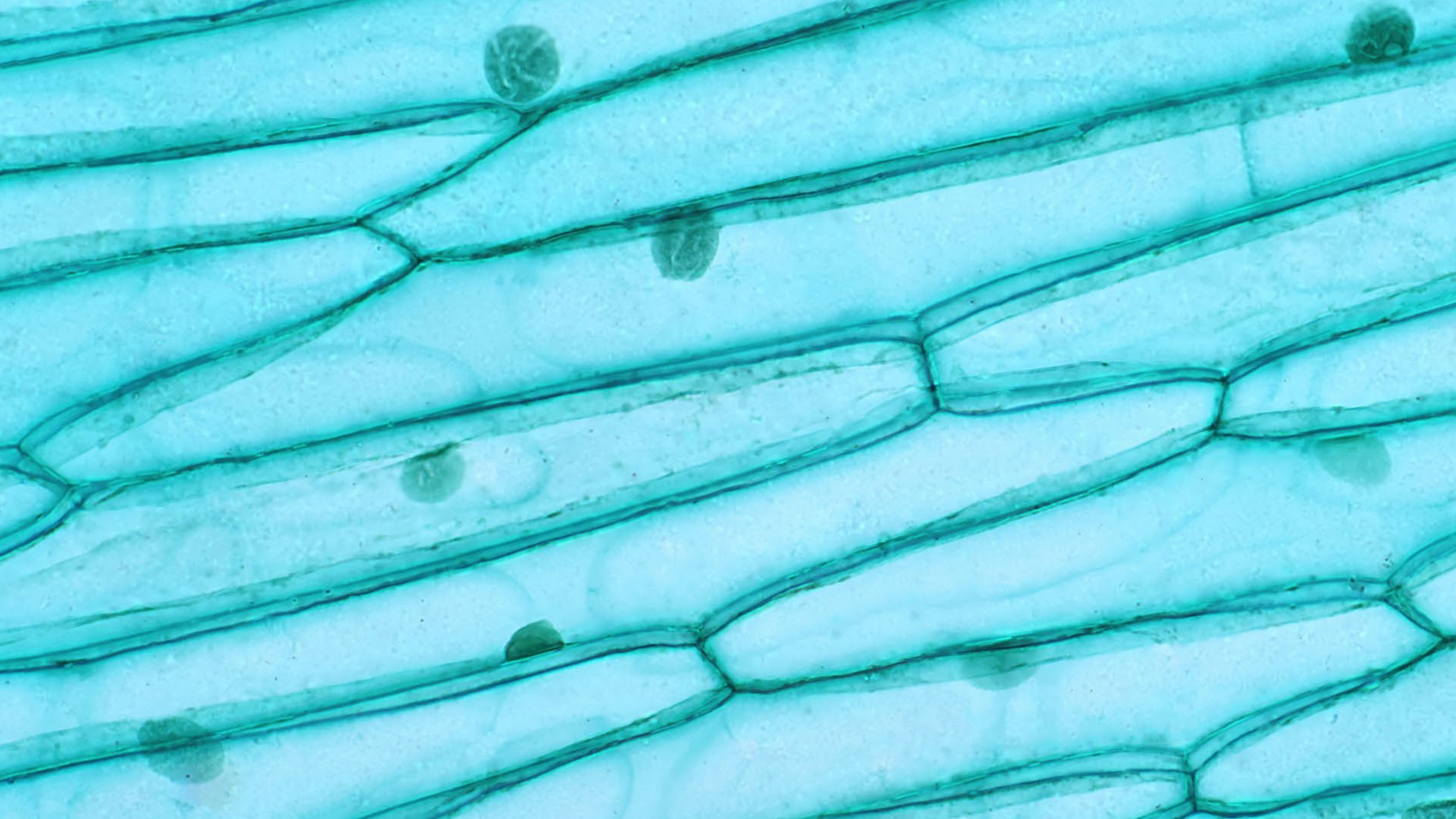
SHE REALLY LIKED THAT SHIRT —

Masked arsonist might've gotten away with it if she hadn't left Etsy review

Woman who burned two police cars IDed by tattoo and Etsy review of her T-shirt.

JON BRODKIN - 6/18/2020, 6:48 PM

Enlarge / Instagram photo of a masked woman, identified by the FBI as Lore-Elisabeth Blumenthal, on May 30, 2020 in Philadelphia.



Anonymisation

Two key questions:

- Keeping in mind the multitude of “very simple experiments”* that show the ease of identification in all sorts of datasets, how can I show in all probability that the data subjects are not re-identifiable?

- In that assessment, should I or should I not take into account information that is available only after performing illegal actions?

See: Latanya Sweeney, https://youtu.be/tivCK_fBBfo?si=MAXCnVXII-4iClvg

Preserving privacy through federated learning

Advantages

- Security and confidentiality of individual level data ↑
- Risk for misuse of individual level data ↓
- No need for complicated Data *Transfer* Agreements*

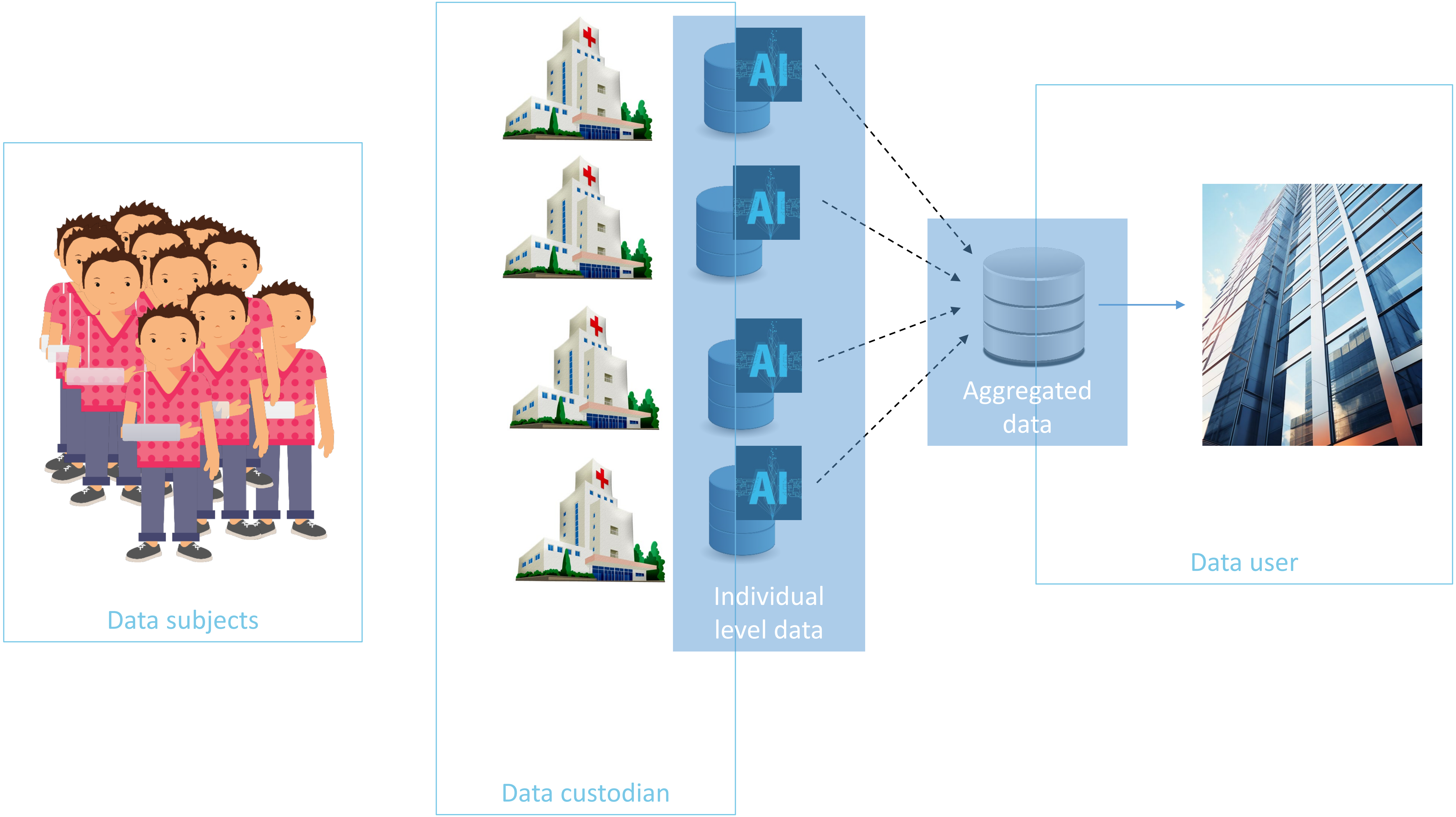
But data are processed for a secondary purpose.

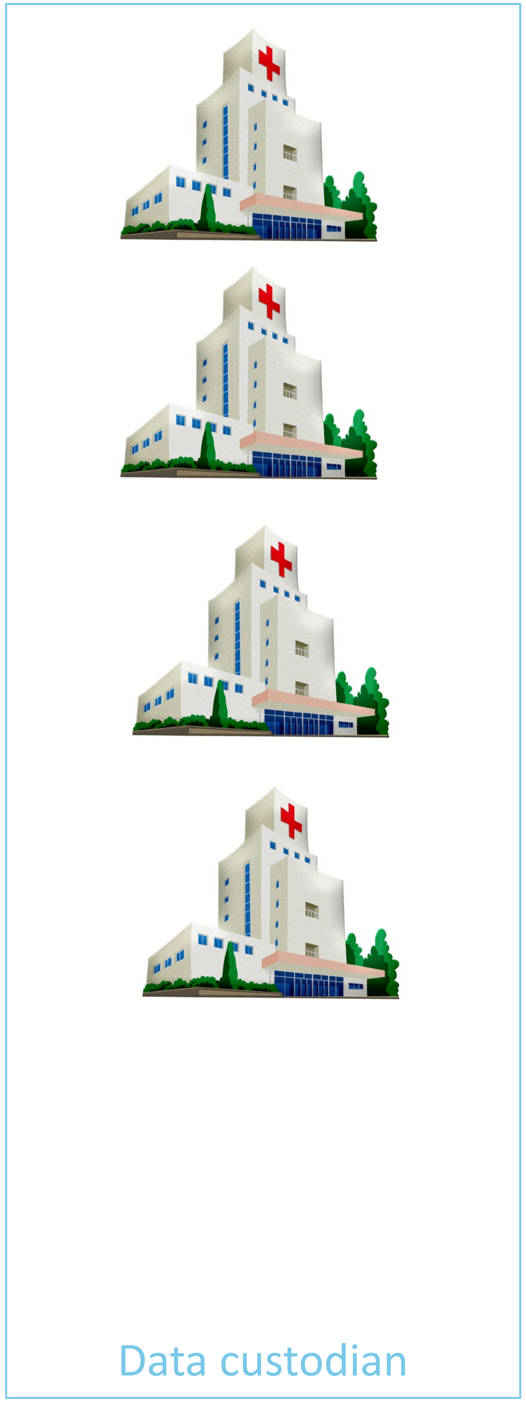
Data are collected, analysed, stored… = data processing operations

=> **Consequently**:

- All GDPR principles apply to the secondary processing
- Data subject's rights have to be respected
- Roles and responsibilities have to be determined

**Unless the data transferred to the central node should be considered personal data*


Data subjects
AI
AI
AI
AI
Individual level data
Data custodian
Aggregated data
Data user



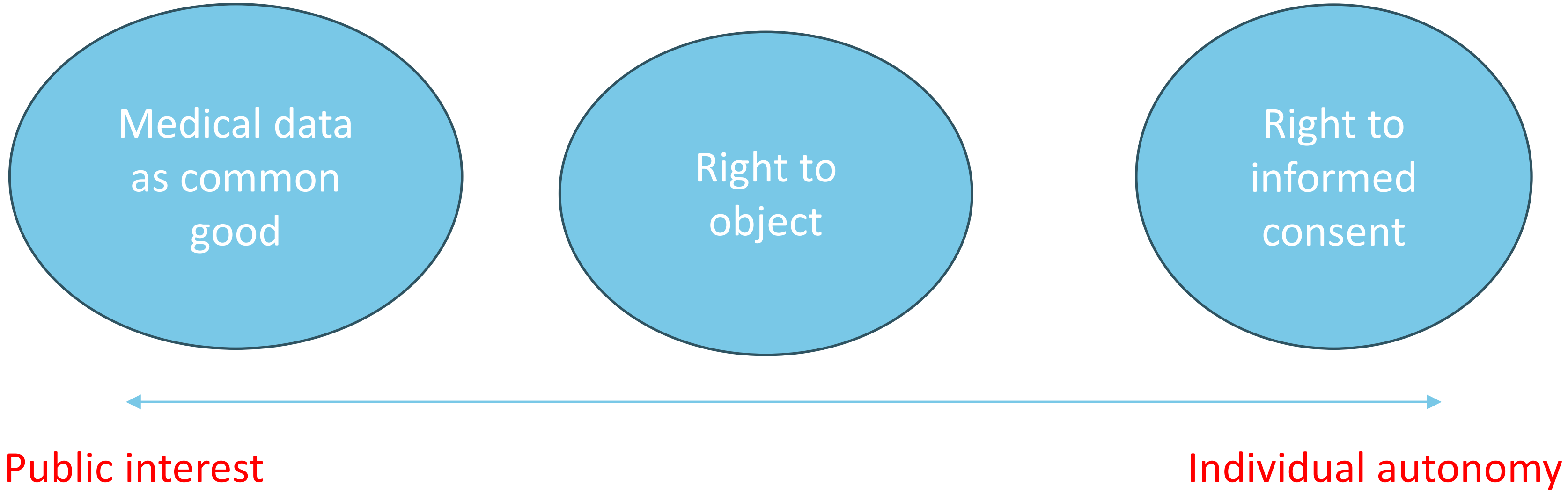
No patients… no data
No doctor, lab technician, nurse,… no added knowledge or inferred interpretations.

Legally data “ownership” would imply the right to solely decide about who can have, hold, destroy,… the data.

European / Belgian legal framework does not recognise data ownership. It confirms rights and obligations for several parties.

Medical data save lives, not only yours.

Data subjects



Medical data as common good

Right to object

Right to informed consent

Public interest

Individual autonomy

Legal footnote:
Article 5 and 6 GDPR: requirement for legal basis, not necessarily informed consent
Article 9 GDPR: requirement for exemption to general prohibition, not necessarily informed consent unless Union or MS law foresees in IC as an additional safeguard.

prof. dr. Griet Verhenneman

Data Protection Officer, UZ Leuven (resigning)

Assistant Professor Privacy Law, UGent

Lecturer European Privacy and Data Protection Law,
KU Leuven

✉ griet.verhenneman@ugent.be

or gdpr@uzleuven.be