Solutions for Autonomous Data Decisions

Data Trustees

SecHUMAN FORSCHUNGSKOLLEG
SECURITY FOR HUMANS IN CYBERSPACE

Leona Lassak

Prof. Dr. Markus Dürmuth
Mobile Security Group,
Ruhr University Bochum

Hanna Püschel

Prof. Dr. Tobias Gostomzyk
Institute for Journalism
TU Dortmund University

Motivation

In the age of Big Data, digitization, the use of social networks, and search engines, increasing amounts of personal (PD) and non-personal data are being processed. However, while there is an overuse of personal data in some areas (i.e. online sector) - partly in violation of data protection and consumer protection law - in other areas - such as medical research - data is still underused.

Why do we need Data Trustees?

Medical sector

- Too little usable data
- Large data sets and linking of data can advance patient care, therapy options, and treatment approaches enormously

Online sector and IoT

Processing of personal data is often based on the data protection law „fiction of consent"
→ consent is often not informed

Automotive sector

Lots of personal data that is not easily identifiable for end users (i.e. location, behavioral)

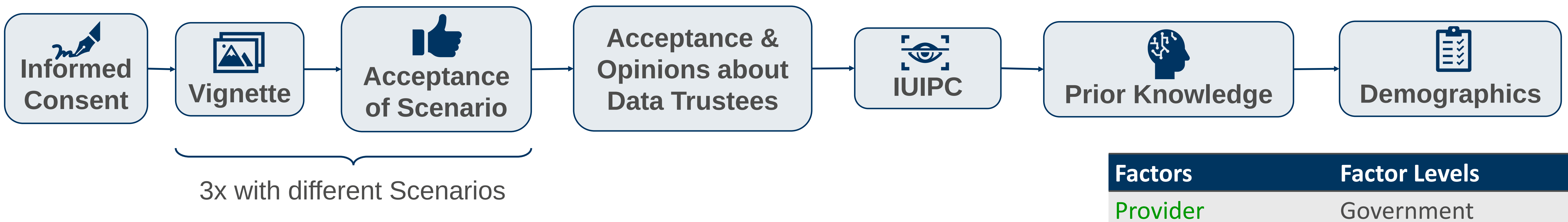
What are Data Trustees?

Goal: Make data use and data protection compatible

Potential Applications:

- grant data privacy consents according to individual's privacy preferences
- act as a trust center, independently conduct data analyses, pseudonymize and anonymize data
- mediate data access to various stakeholders (encouraging data subjects to get value of personal data)

Vignette Study



Informed Consent → Vignette → Acceptance of Scenario → Acceptance & Opinions about Data Trustees → IUIPC → Prior Knowledge → Demographics

3x with different Scenarios

Imagine you are at the doctor's office and the doctor stores the following data about you:

- Name, address, date of birth, sex
- Medical check-ups, regularity of check-ups, illnesses
- Emergency information (allergies, illnesses, blood type…)

Your doctor asks you if you are interested to allow a non-profit service provider access to this data. The service provider grants third parties access to the data under the following conditions. This option is voluntary.

- The service provider receives anonymized data and analyses it.
- The data is only stored on servers in the EU.
- Access to the data is granted to research institutions and private companies.
- You receive monetary compensation for your data. Additionally, your data generally helps research and development.
- The certified service provider gets monitored for compliance with the regulation by public auditors.

Are you interested to give the service provider access to your data?

Fig 1: Example vignette with example factor levels

Factors	Factor Levels
Provider	Government
	Corporation
	NGO
Data Type	Non-anonymized raw data
	Anonymized data
	Only non-personal data
Data Processing	Only Storing
	Aggregation from various sources
	Analysis → third parties can only access reports
Storage Location	Germany
	EU
	Worldwide
Data Access	Research institutes
	Industry
	Governmental organizations
	Law enforcement agencies
	Privat people
Access Type	Data records transmitted to third party
	Data records remain with data trustees → requests
Benefits for Users	Monetary incentives
	Individualizes services
Certification	Yes / No
Monitoring	Governmental institution
	Public auditors

Tab 1: Factors & factor levels for vignette study

Voices from real world Data Trustees

We conducted interviews with BMBF-funded pilot projects for data trustees (i.e. for medicine, agriculture, logistics, automotive).

Main Results:

- Research is still very rudimentary
- The issue of user acceptance is barely covered → main focus: technical
- Legal insecurities exist in all projects (i.e. unclarities about GDPR applicability)

Funded by:

Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen

Project partners:

Fachhochschule Dortmund
University of Applied Sciences and Arts

technische universität dortmund

RUB

Further partners:

STIFTUNG DATENSCHUTZ