

Introducing Data Trustees: A Vignette-Based Study Approach to Get Users in the Loop

Leona Lassak
Ruhr University Bochum

Hanna Püschel
TU Dortmund University

Tobias Gostomzyk
TU Dortmund University

Markus Dürmuth
Leibniz University Hannover

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.

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)

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

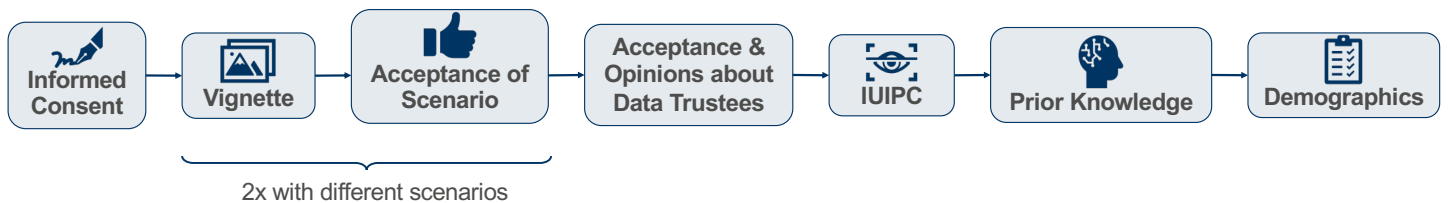
Online sector and IoT

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)

Vignette Study



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 **analyzes** 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.
- 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 sets
	Only non-personal data
Data Processing	Only Storing
	Aggregation from various sources
	Analysis → third parties can only access reports
Storage Location	Germany
	EU
	Worldwide
Receiver	Research institutions
	Private enterprises
	Law enforcement agencies
Access Type	Privat people
	Data sets transmitted to receiver
	Data sets remain with data trustees → requests
Benefits for Users	Monetary compensation
	Individualized services
Certification	Yes / No
Monitoring	Governmental institution
	Public auditors

Tab 1: Factors and factor levels for vignette study

Study Implementation



1000 Participants



Representative Study in Germany



Following:
China, USA, Australia and UK

Funded by:

Ministerium für
Kultur und Wissenschaft
des Landes Nordrhein-Westfalen



Project partners:

Fachhochschule
Dortmund
University of Applied Sciences and Arts

tu technische universität
dortmund



Further partners:

STIFTUNG
DATENSCHUTZ