

Replication: The Effect of Differential Privacy Communication on German Users' Comprehension and Data Sharing Behaviour

SOUPS - August 8th, 2022

Patrick Kühnreiter, Viktoriya Pak, Delphine Reinhardt

University of Göttingen, Institute of Computer Science
Computer Security and Privacy (CSP)

Goldschmidtstr. 7

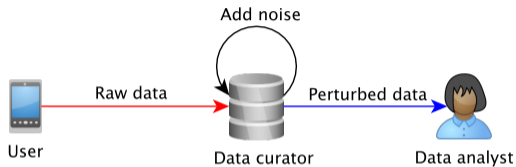
37077 Göttingen, Germany

Email: kuehtreiber@cs.uni-goettingen.de

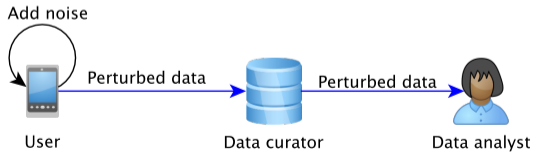
www.csp.informatik.uni-goettingen.de

Motivation

Differential Privacy



Global Differential Privacy (DP)



Local Differential Privacy (LDP)

- Can DP increase users' willingness to share data? (e.g., for machine learning)

- Can DP increase users' willingness to share data? (e.g., for machine learning)
- Replication of a 2020 study by Xiong et al.

- Can DP increase users' willingness to share data? (e.g., for machine learning)
- Replication of a 2020 study by Xiong et al.
- A country's culture, privacy regulations, etc. impact its citizens' privacy attitudes

Effect of DP Communication

Differences to original study

	Original study	Our study
Country	USA/India	Germany
Age	80% < 45y	repr.
Education	60% Bachelor	repr.
#Experiments	4	2
Avg. #Participants	~ 466	~ 728

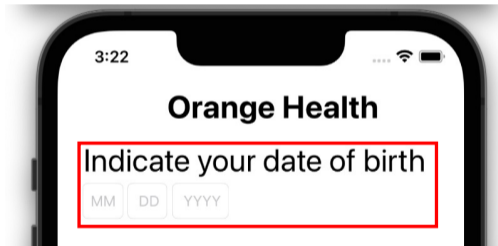
repr. = “representative of the German population”

- Online questionnaire
- You download a health app that requires (sensitive) information to ...
 1. ...improve the app locally for you
 2. ...improve the app via machine learning on the app's server for everyone
- Three groups: DP/LDP/Control

Effect of DP Communication

Experiment 1 - Example question

Participants were asked to decide how they want their answers to be *processed*:



- Only used by the app locally
- Used by the app locally and the server
- Used neither by the app nor the server
- I choose not to answer

Confirmed:

- Hardly any difference between DP and LDP

Confirmed:

- Hardly any difference between DP and LDP

Differences / New findings:

- (L)DP communication was effective, especially in high-sensitive questions
- Participants showed more trust in the app if they use a health app already

- Same scenario as in experiment 1

Experiment 2 - Scenario

- Same scenario as in experiment 1
- Eleven groups: different descriptions of (L)DP

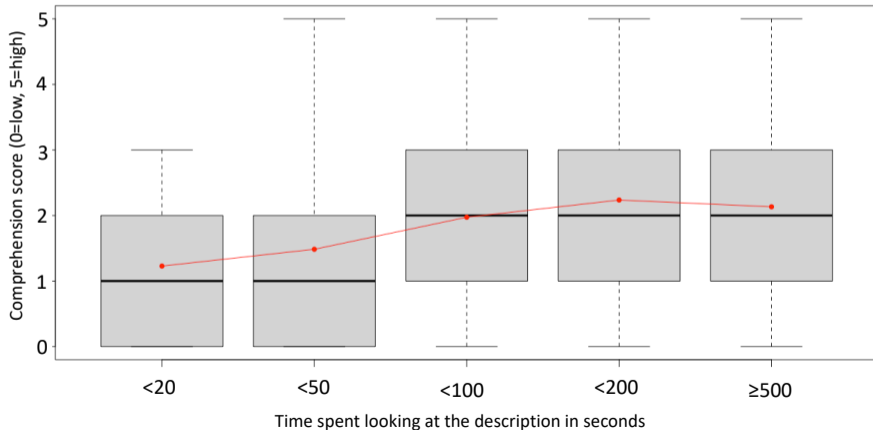
Experiment 2 - Scenario

- Same scenario as in experiment 1
- Eleven groups: different descriptions of (L)DP
- Willingness to share personal data and why

- Same scenario as in experiment 1
- Eleven groups: different descriptions of (L)DP
- Willingness to share personal data and why
- Focus lies on comprehension
- E.g., “Can an attacker see your real data if they get access to the data base?” (Yes for DP, No for LDP).

Effect of DP Communication

Experiment 2 - Attention and Comprehension



Confirmed:

- Similar overall sharing rate (52.83% vs. 47.8%)
- Similar overall difficulty-to-comprehend rating (13.4% vs. 13.3%)

Confirmed:

- Similar overall sharing rate (52.83% vs. 47.8%)
- Similar overall difficulty-to-comprehend rating (13.4% vs. 13.3%)

Differences:

- More similarity among groups
 - No sharing < 46%
 - No difficulty-to-comprehend < 10%
- IT-Background ↔ difficulty-to-comprehend ↔ actual understanding
- Usage of health apps ↔ willingness to share

- (Local) Differential Privacy was not well understood

- (Local) Differential Privacy was not well understood
- “All or nothing”

- (Local) Differential Privacy was not well understood
- “All or nothing”
- Text is not the ideal way to communicate privacy protection techniques
- Better (graphical) descriptions of (L)DP are needed

Replication: The Effect of Differential Privacy Communication on German Users' Comprehension and Data Sharing Behaviour

Patrick Kühtreiber, Viktoriya Pak, and Delphine Reinhardt