DVAE25 Local Differential Privacy

Anders Kristoffer Norman

Requirements of explanations

- Short explanations
- Should understand more noise increases privacy
- Should understand more noise increases needed samples

Semi-structured interviews

- Questions generated from a test interview with one person

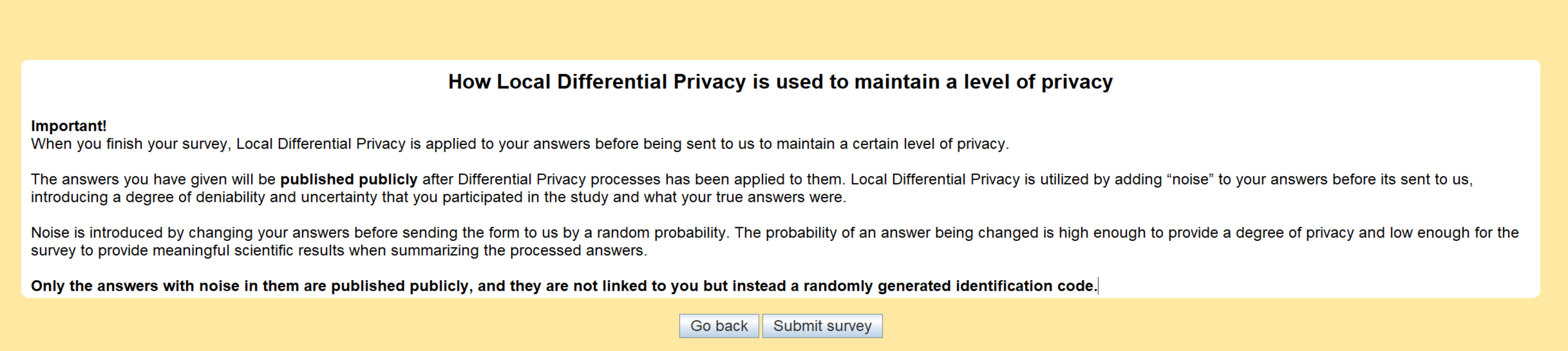
- Example questions
  - What was the name of technique?
  - Was the information sensitive?
  - What parameters are important for Local Differential Privacy?
  - What is "noise" in this context?
  - How does it protect your privacy?
  - Do you trust the method to protect your privacy?

Fake survey - scenario

- Participants requested to participate in fake survey about finding a correlation between online purchases and advertisement exposure

- Participants were told that the survey answers would be published after Local DP.

Explanation



How Local Differential Privacy is used to maintain a level of privacy

Important!
When you finish your survey, Local Differential Privacy is applied to your answers before being sent to us to maintain a certain level of privacy.

The answers you have given will be **published publicly** after Differential Privacy processes has been applied to them. Local Differential Privacy is utilized by adding “noise” to your answers before its sent to us, introducing a degree of deniability and uncertainty that you participated in the study and what your true answers were.

Noise is introduced by changing your answers before sending the form to us by a random probability. The probability of an answer being changed is high enough to provide a degree of privacy and low enough for the survey to provide meaningful scientific results when summarizing the processed answers.

Only the answers with noise in them are published publicly, and they are not linked to you but instead a randomly generated identification code.

Fake survey – results 1

- Most people ignored the explanation of Differential Privacy
- Didn't find the questions sensitive
- Most people understood what noise refered to
- Most people didn't trust the method (with sensitive information)
- Most people couldn't explain how this would protect their privacy

Fake survey – results 2

- Most people understood that more noise meant more samples were needed

- Few people understood that you could look at the answered surveys to possibly decide who is who.

- One person found it inappropriate to change answers

Signup chat service - scenario

- Participants were told they were about to signup for a chat service

- Participants were told information would be collected by them to publish statistics

Signup chat service - results 1

- Most people skipped Differential Privacy explanation again
- Some people had a hard time understanding what noise were
- None of the participants found the information collected was sensitive
- Some people didn't understand what the purpose of Local Differential Privacy was
- Most people didn't trust the method (with sensitive information)

Signup chat service - results 2

- Most people couldn't explain how this would protect their privacy

- People had a hard time understanding more noise meant more privacy