Comprehension from Chaos: Towards Informed Consent for Private Computation

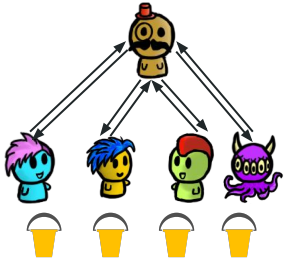
Bailey Kacsmar, Vasisht Duddu, Kyle Tilbury,
Blase Ur, Florian Kerschbaum

amii
UNIVERSITY OF ALBERTA
UNIVERSITY OF WATERLOO
THE UNIVERSITY OF CHICAGO

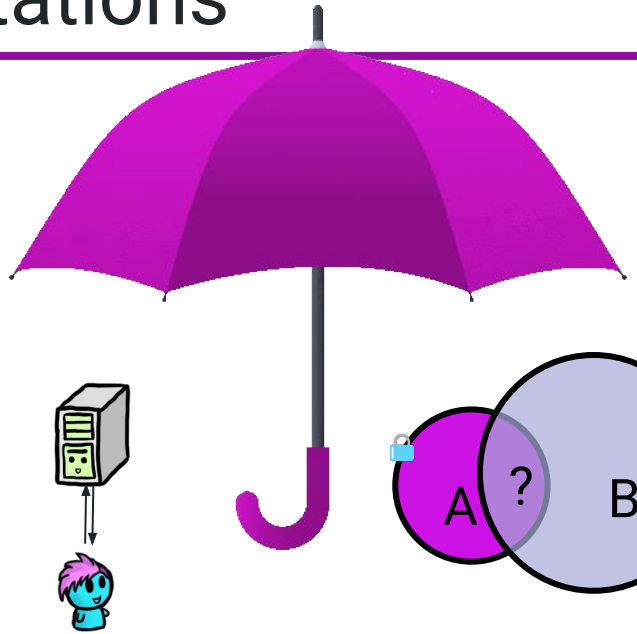
Private Computation?

Private Computation

Private Computations

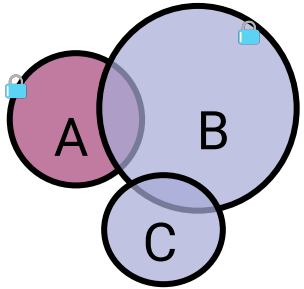


Private Machine Learning



Private Query Processing

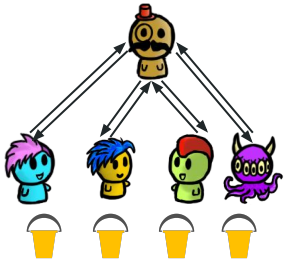
Private Set Intersection



Multiparty Computations

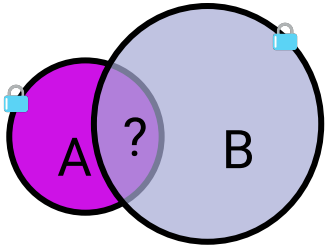
Private Computations Class

Define, **what** is being protected, from **whom**,
and under what **conditions** this protection will hold.

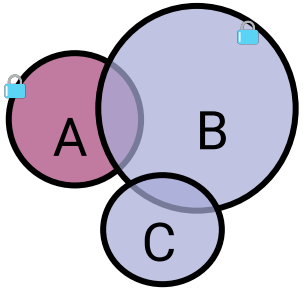


Private Machine Learning

Private Query Processing

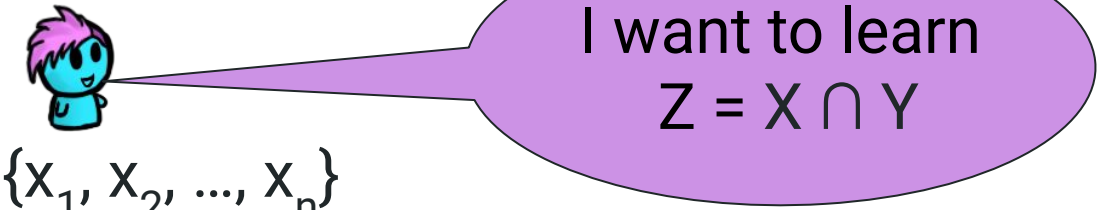


Private Set Intersection



Multiparty Computations

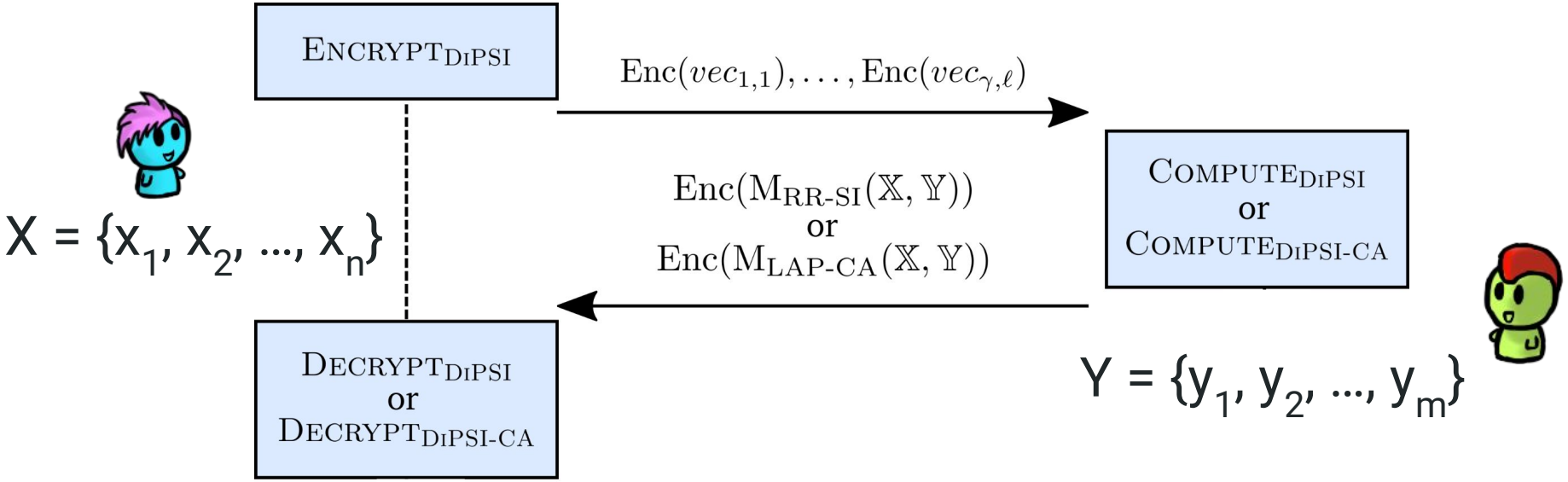
A Private Computation? Cryptography!



$X = \{x_1, x_2, \ldots, x_n\}$

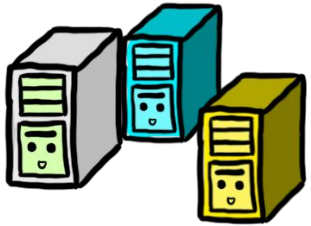
$Y = \{y_1, y_2, \ldots, y_m\}$

Private Set Intersection



B. Kacsmar, B. Khurram, N. Lukas, A. Norton, et al. "Differentially private two-party set operations." In 2020 IEEE European Symposium on Security and Privacy (EuroS&P), pp. 390-404. IEEE, 2020.

Why Private Computation?

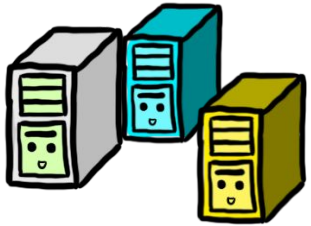


A company wants to analyze data

But the data has privacy implications for the data subjects

Researchers develop technical solutions

Why Private Computation?



A company wants to analyze data

But the data has privacy implications for the data subjects

Researchers develop technical solutions

In what ways does private computation matter to people?

Perceptions and Expectations

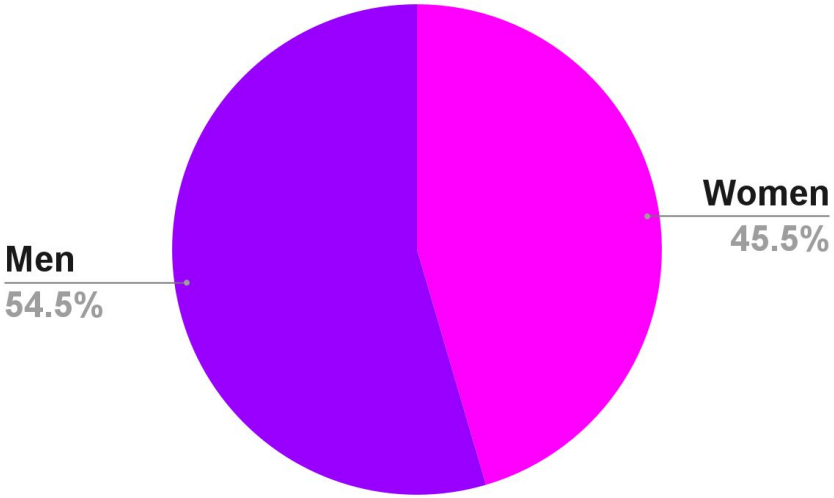
- **RQ1**: What do data subjects understand?
- **RQ2**: How is a data subject's willingness to share impacted?
- **RQ3**: How do data subjects perceive the risks?

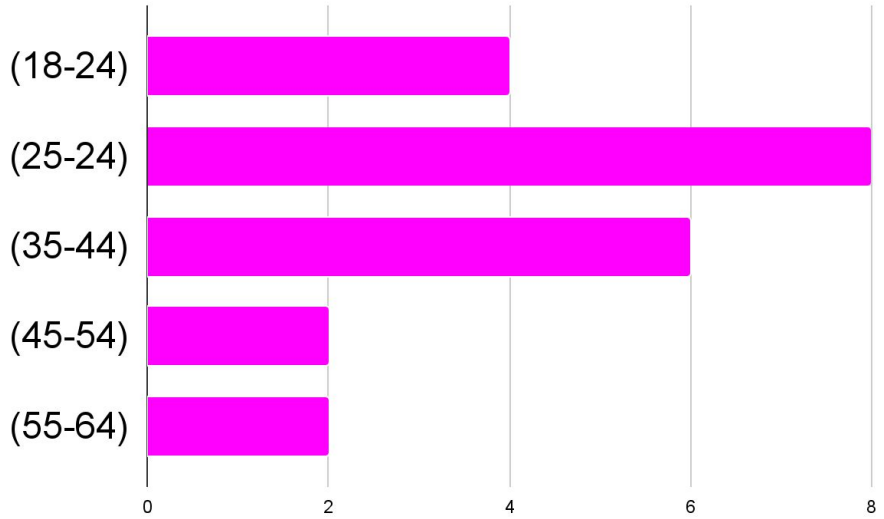
What they "want"

What they "need"

Build towards those attributes

The Participants





Recruited 22 through Prolific, across the United States

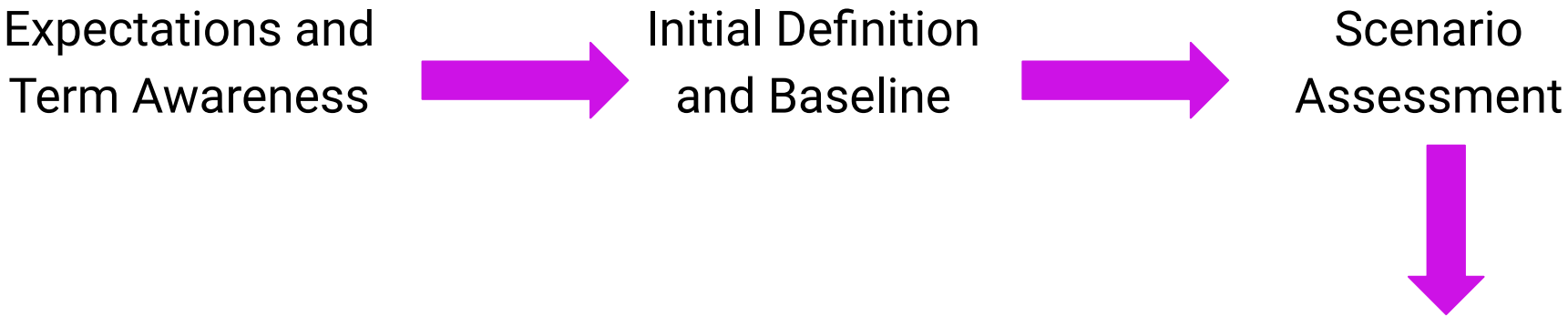
The Interview

Expectations and
Term Awareness

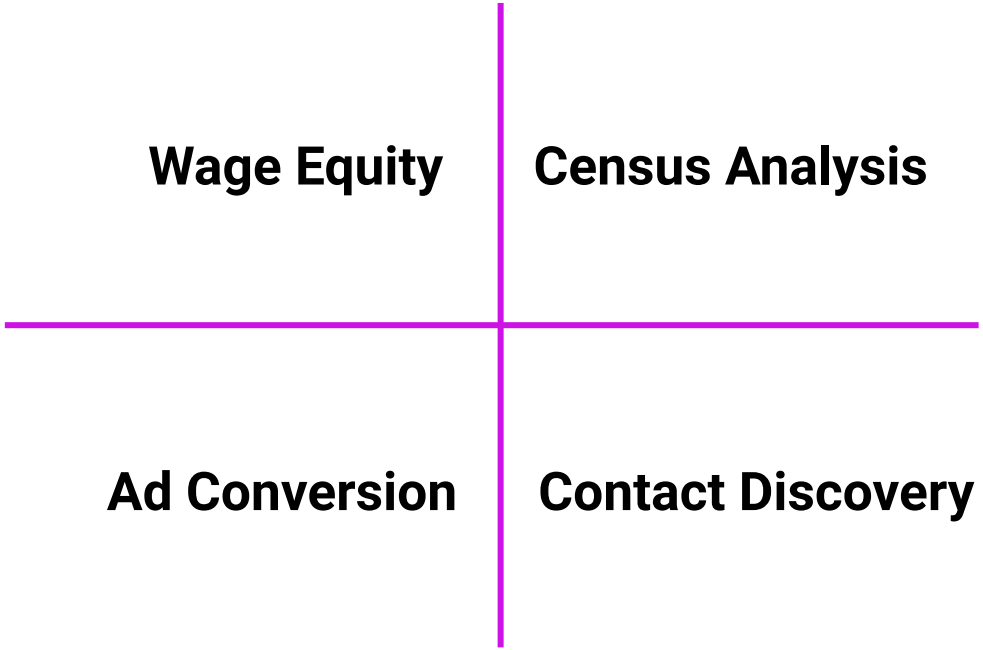
The Interview

Expectations and Term Awareness  Initial Definition and Baseline 

The Interview



The Scenarios

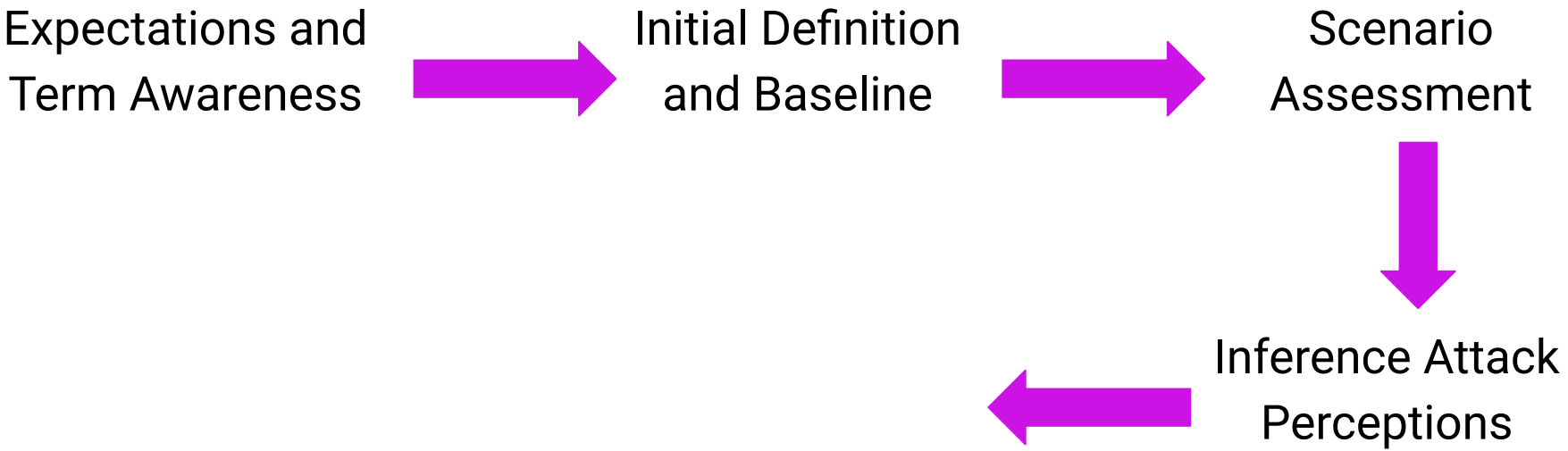


Contact Discovery Conceptual Example

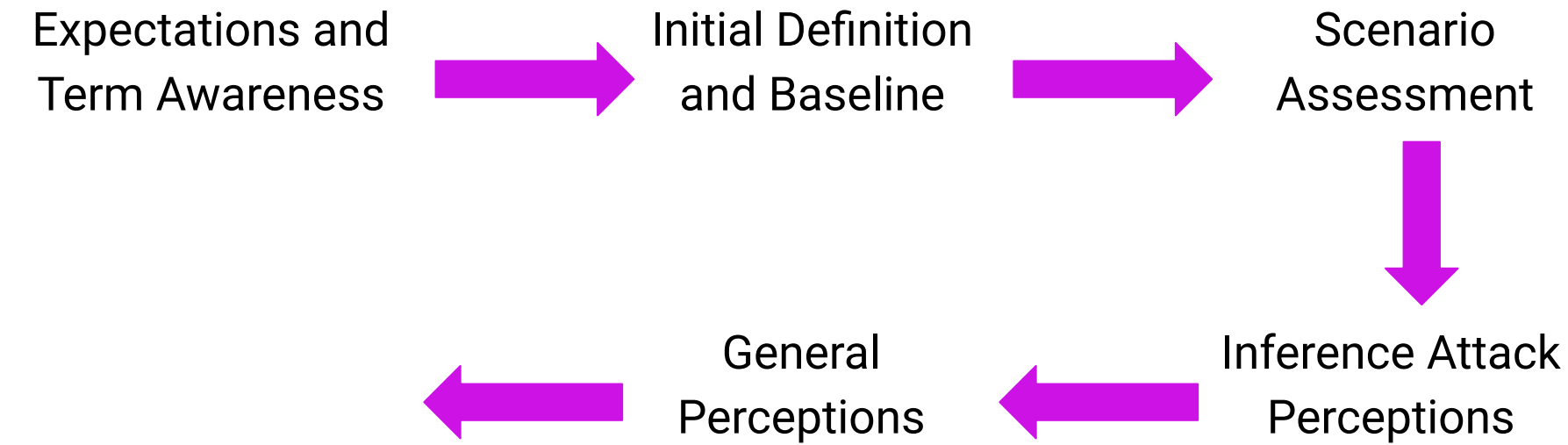
The app wants to **determine the common contacts** between the new user and the existing users via…

1. …the new user shares all their contact information with the social media app.
2. … the new user shares **a modified version** of their contact information…**such that** the social media app does not learn non-users…thus, **this means**…

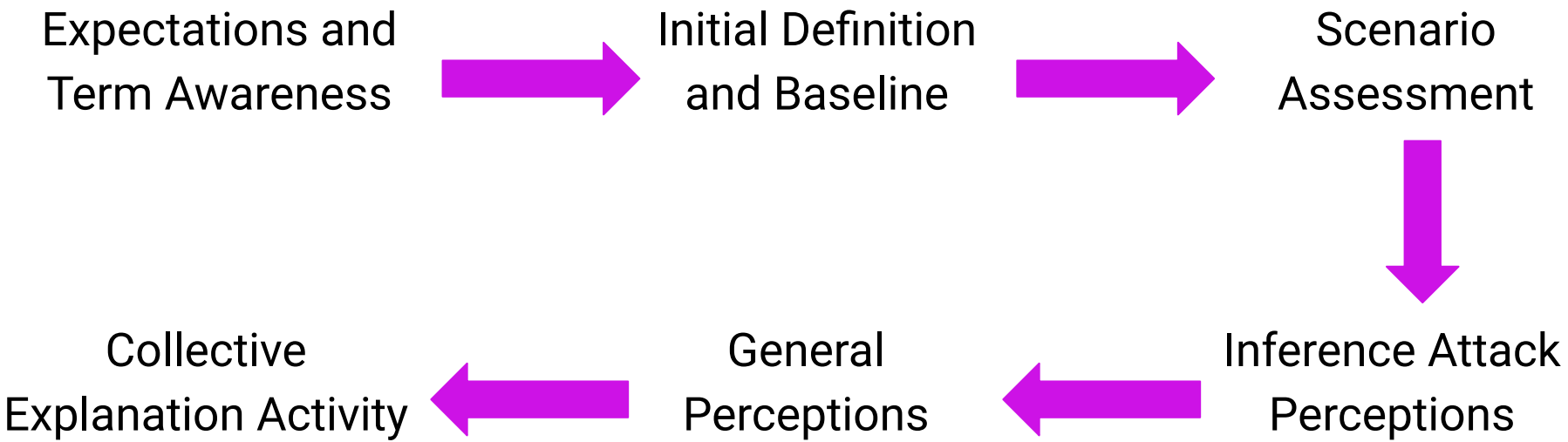
The Interview



The Interview



The Interview

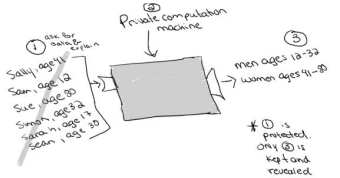


Participant Comprehension and Expectations

First Attempt

Second Attempt

Secure computation is a way that a company analyzes your data. The final analysis will be made public [at access location]. However, your specific data is protected and cannot be traced back to you nor can your specific data points be traced back to you. The analysis will be specifically [example], and this is being done because [purpose].



This is the information we're getting from you, but, rest assured, only Part Three will be shown. You can trust us to keep your information private. <If true>This information will only be used for this project and nothing else in the future.

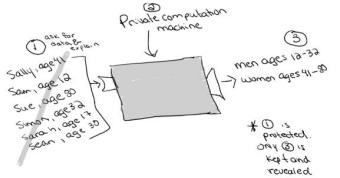
Final Consensus

Participant Comprehension and Expectations

First Attempt

Second Attempt

Secure computation is a way that a company analyzes your data. The final analysis will be made public [at access location]. However, your specific data is protected and cannot be traced back to you nor can your specific data points be traced back to you. The analysis will be specifically [example], and this is being done because [purpose].



This is the information we're getting from you, but, rest assured, only Part Three will be shown. You can trust us to keep your information private. <If true>This information will only be used for this project and nothing else in the future.

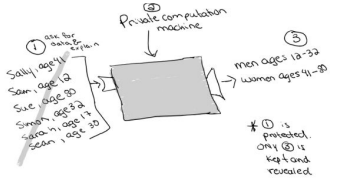
Final Consensus

Participant Comprehension and Expectations

First Attempt

Second Attempt

Secure computation is a way that a company analyzes your data. The final analysis will be made public [at access location]. However, your specific data is protected and cannot be traced back to you nor can your specific data points be traced back to you. The analysis will be specifically [example], and this is being done because [purpose].



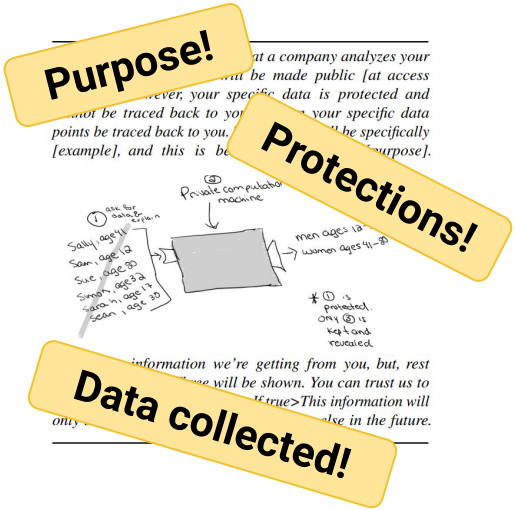
This is the information we're getting from you, but, rest assured, only Part Three will be shown. You can trust us to keep your information private. <If true>This information will only be used for this project and nothing else in the future.

Final Consensus

Participant Comprehension and Expectations

First Attempt

Second Attempt

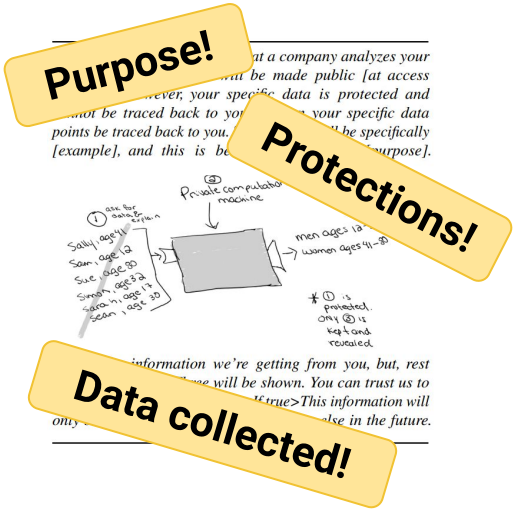


Final Explanation

Participant Comprehension and Expectations

First Attempt

Second Attempt



Final Explanation

Unconcerned with details of the mechanism, **impact** matters

Impact of Private Computation

"...they're trying to make it sound a little bit better" (P19).

"...it feels a little bit more protected that way" (P12)

Bounded Impact of Private Computation

Intentions Matter

Divulge the Details

Regulate the Restrictions

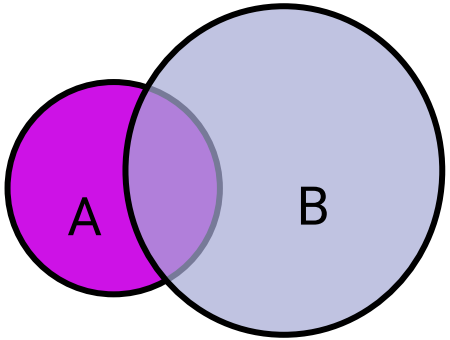
Consent Above All

“At the end of the day,
they’re still like learning specific things about me” (P7)

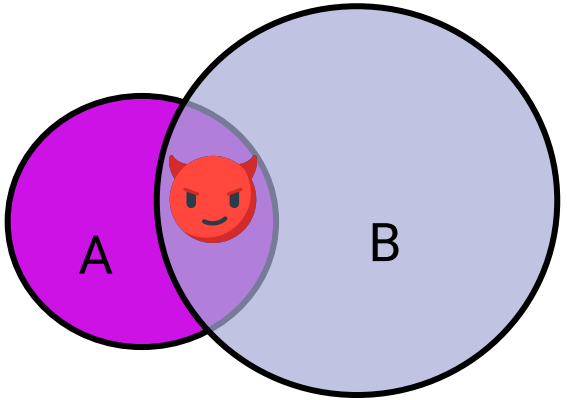
Awareness of Unique Threat Models

Alice

Joins Social App



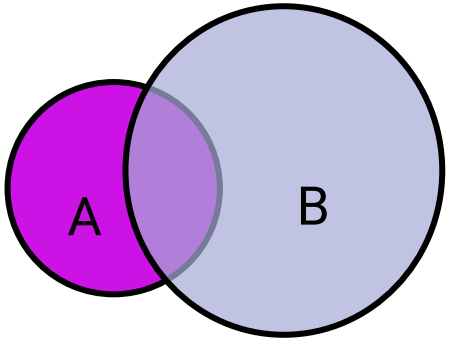
Contact Discovery

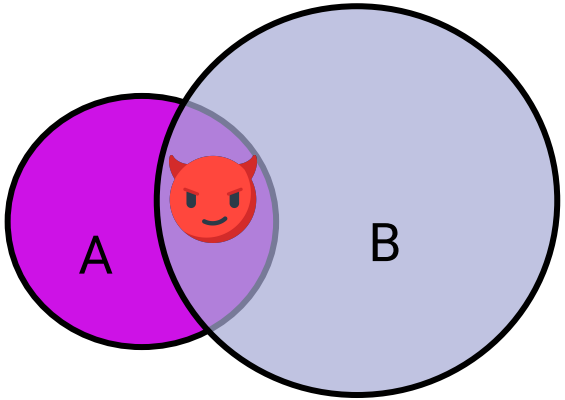


Real Identity Connected

Awareness of Unique Threat Models

Alice





Joins Social App

Contact Discovery

Real Identity Connected

There exist, and will continue to exist risks that cannot be regulated by technology

Takeaways

- **Protections provided by protocols** and constructions **do not encompass the full range of risks** experienced **by individuals** in society
- Private computation is a treatment and not a cure for data privacy concerns
- People find private computation plausible, but they **care about the context, not the math**

Takeaways

- **Protections provided by protocols** and constructions **do not encompass the full range of risks** experienced **by individuals** in society
- Private computation is a treatment and not a cure for data privacy concerns
- People find private computation plausible, but they **care about the context, not the math**

People can reason about private computation; let them.

Thanks!