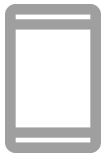
Threat Model for First Party Data

Mariana Raykova

What are we protecting in our designs ?

www.nytimes.com

Information that links user behavior across different contexts



www.shoes.com

What are we trying to measure in our designs ?

www.nytimes.com

impression

Information that links user behavior across different contexts

www.shoes.com

conversion

What are our design approaches ?

Privacy preserving computation on cross-site joined data that protects cross-site information about users/event (privacy units)

- ARA - on-device attribution
- IPA - off-device attribution

First Party Data

Data that a single party has about its users - **does not need to satisfy our privacy guarantees** since it is generated in first party interactions

First Party Data Uses

The use of first party data can improve utility of the privacy preserving computation and revealing it in the clear can improve efficiency.

- Information about the impressions and conversions being processed
- Other first party information

Report Counts

Revealed to aggregation infrastructure

ARA: Aggregatable reports

- Number of attributed conversions reports

Interoperable Private Attribution

- Number of impressions, number of conversions

Conversion Priors

Insights derived from prior conversion information

ARA: Event-level reports

- Reporting window configuration
- Flexible extension: full randomized response output states

IPA Issue #60 - consider RR-like mechanism

- Randomized response output states:
  - Break output space
    {[0, 10], [11, 100], [101+]}
  - Do k-ry RR on output space

On-Device processing

Any on device configuration that depends on data outside the impressions and conversions being processed

- Event level reports - configurations for local DP processing
- Aggregate reports - selection of reporting buckets based on additional information

First Party Data Uses

Are we OK with creating designs that require sharing of first party data with other parties in order to obtain utility?

- On device - accessible to multiple parties
  - the first party data depends on many other users
- With workers
  - are we OK with sharing all the impression or all the conversions

First Party Data Uses

Or should design mechanism that protect such first party data?

- On device - interaction with the measurement system to privately compute contribution (a mini two party computation between the client and the reporting server)
- Computation workers
    - Treat such data as private just like impression and conversions

Beyond the direct implications

Training models with **label differential privacy provides privacy with respect to the party that knows the labels, not with respect to other parties**

Will models be used only by the party with the features? Will predictions be used later in different context including other parties?

Questions

1. Should our threat model include first party data?
    a. Is the user device secure to handle such data?
    b. Are aggregation infrastructure workers OK to handle such data?
2. Should we leave this up to participant to handle the risks of their first party data when choosing to use the APIs?
3. Should we be defining privacy with respect to any party or with respect to the immediate consumer of the measurement? If the later should we worry with downstream uses of the measurements that involve other parties?