Private Measurement of Single Events

Charlie Harrison
May 2023

What is “single-event measurement”?

- Queries which observe the outcome associated with single events.
- e.g. “Did *source impression* lead to a conversion, or not?”

Attribution Reporting API - event-level reports	Supported
Attribution Reporting API - summary reports	Supported
Interoperable Private Attribution	Supported
Private Click Measurement	Limited support

Goal for this discussion: either

1. **Agree** single-event measurement with differential privacy satisfies our privacy goals, OR
2. **Disagree** and investigate mitigations

This presentation

1. Differential privacy on single events can protect users
2. Noisy, per-event data can be useful
3. “Aggregation” as a boundary is hard to rigorously defend

Context:

- https://github.com/patcg/docs-and-reports/issues/41
- https://github.com/patcg-individual-drafts/ipa/issues/60

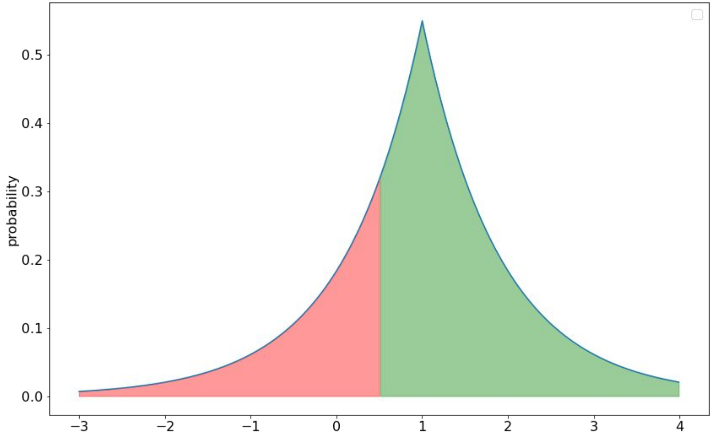
Differential privacy on single events can protect users

Per-event differential privacy

Did *source impression* lead to a conversion, or not? Imagine it did:

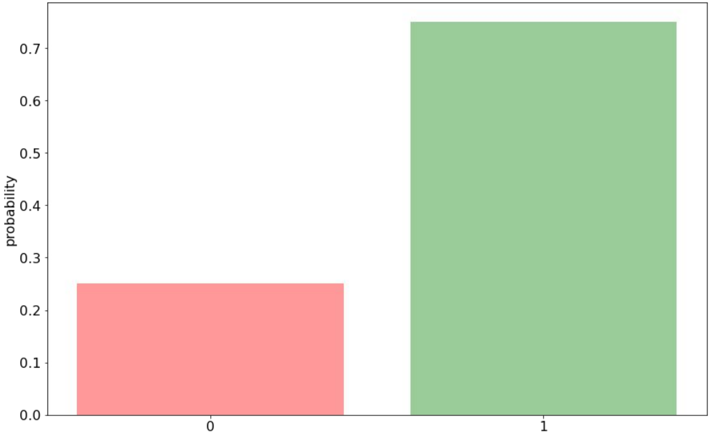
Laplace mechanism

```
return val + laplace(1 / epsilon)
```



Randomized response

```
if random() < 2 / (1 + exp(epsilon)):
  return choice([0, 1])
return val
```



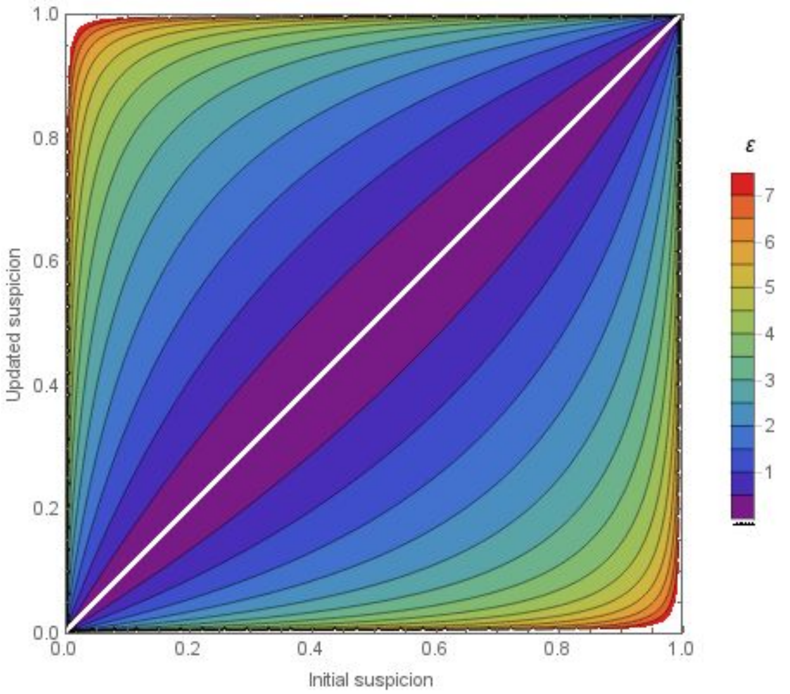
Semantic interpretation of differential privacy

- Attacker has a prior on the user's data
- Privacy mechanism bounds the posterior after looking at the data
- Applies to *any* mechanism satisfying DP
    - Includes mechanisms permitting single event measurement

ε = ~1.1 bounds a prior of 50% to [25%, 75%]

ε = ~2.2 bounds a prior of 50% to [10%, 90%]

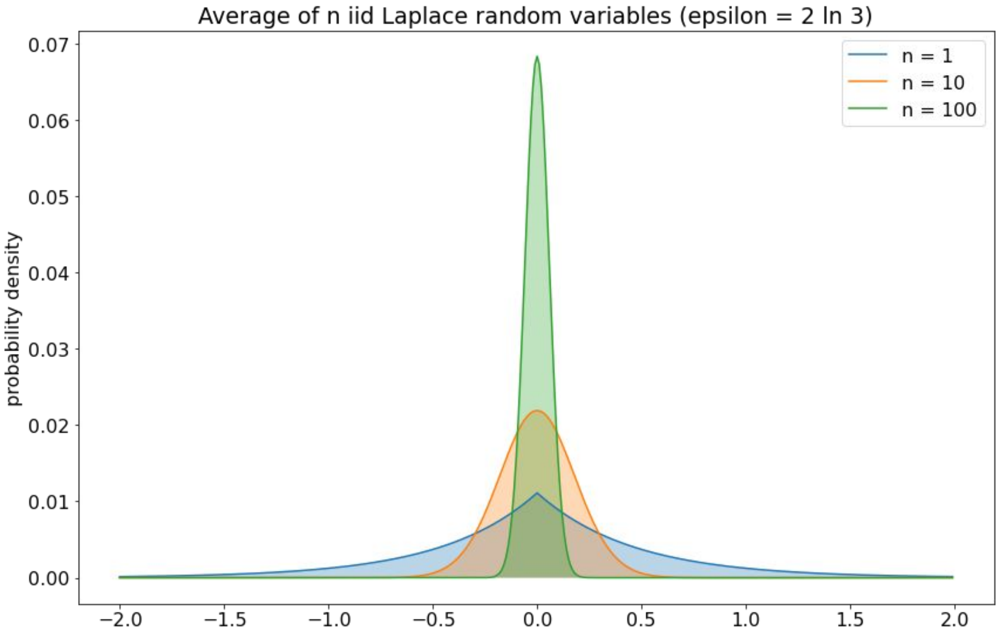
ε = ~2.9 bounds a prior of 50% to [5%, 95%]



Source: https://desfontain.es/privacy/differential-privacy-in-more-detail.html

Aggregation is a critical *post-processing* step here

- Take ε = ~2.2
- Laplace(1/ε) → $\boldsymbol{\sigma}$ = ~.64
- You can guess a single user's value, but in general this won't lead to accurate results
- What if you average N users?
  - Yields $\boldsymbol{\sigma}'$ = $\boldsymbol{\sigma}$ / sqrt(N)
  - N >=~150 yields $\boldsymbol{\sigma}'$ = ~.05

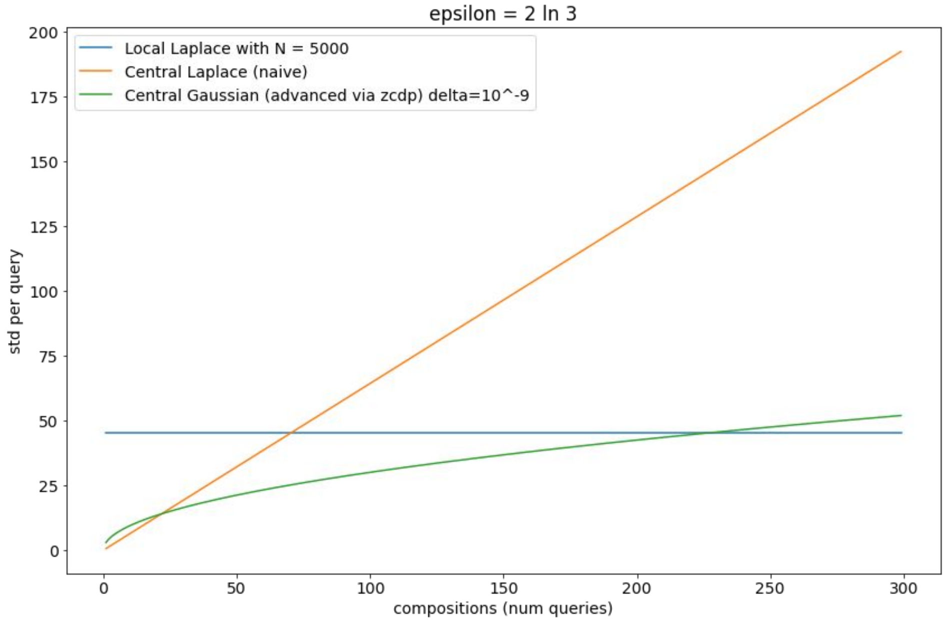


*Under high privacy regimes, single-event privacy ~**requires aggregation** for meaningful utility*

Noisy, per-event data can be useful

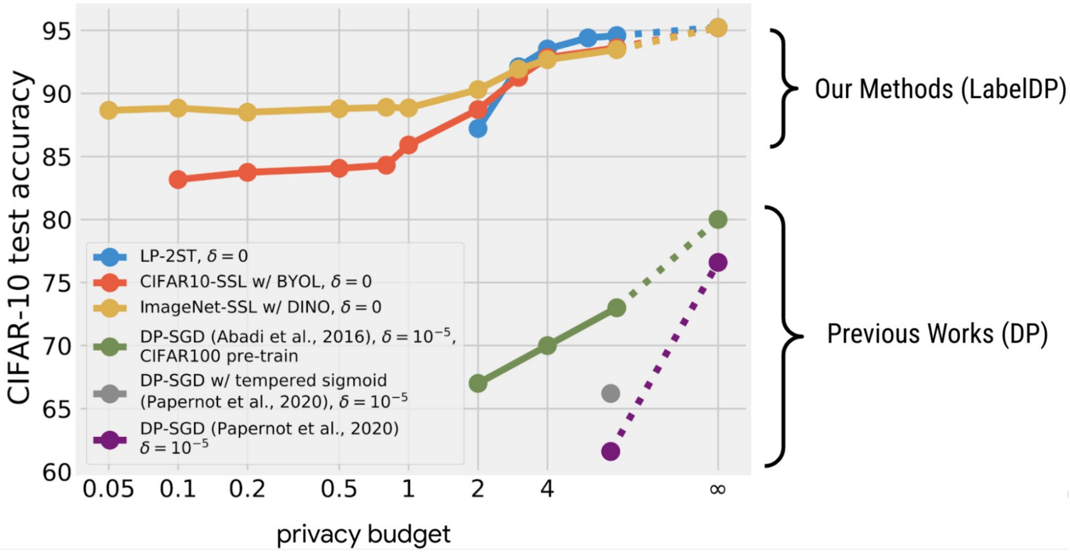
Flexible aggregation via post-processing

- Privacy is already “built-in”
  - Arbitrary aggregate slices
  - Avoids “regretful” queries
- Build complex mechanisms outside of the privacy mechanism
  - Allows us to satisfy use-cases before building custom algorithms for them
- May allow “data sharing” use-cases without industry standardization on breakdown keys
  - Think: multiple ad-tech measurers



Private optimization via Label DP

- Label DP
  - Differentially private optimization where *only the label* is private
  - Label = #conversions, $$, etc associated with an impression
- Ghazi et al (NeurIPS 2021, ICLR 2023)
  - “restricted k-ary randomized response”
  - State of the art performance in private learning
  - Continuing to explore future innovations in this setting
- Meta research
  - Malek et al (NeurIPS 2021)
  - Yuan et al (preprint)



Test accuracy with LabelDP vs. traditional DP learning on an image dataset

Source: https://ai.googleblog.com/2022/05/deep-learning-with-label-differential.html

“Aggregation” as a boundary is hard to rigorously defend

k-anonymity style mitigations

Remove outputs:

- whose inputs to a particular bucket < k_1
- whose output buckets < k_2

Problems:

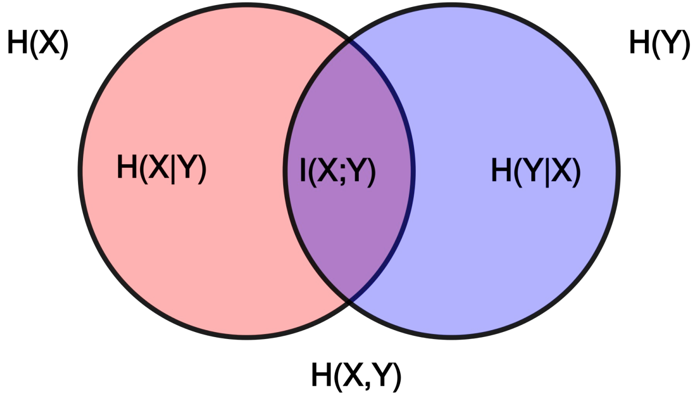
- Adversaries that injects fake events
- Breaks with composition, auxiliary data
  - Overlapping queries
  - Difference attacks
- Protection may rely on distributional assumptions unless backstopped by DP

Campaign	*Num impressions (k_1 < 150 removed)*	*Num conversions (k_2 < 30 removed)*
Campaign1	1004	40
Campaign2	120	31
Campaign3	304	12
Campaign4	13000	1000

*k-anon enforcement **only weakly protects** against measuring single events*

Maximum information gain / channel capacity

- X = encoded message sent through the API
- Y = API output
- Goal of the adversary: maximize mutual information I(X; Y)
    - Over all possible encodings → *channel capacity*
    - Measured in B "bits"
    - Can observe 2^B distinct events
    - Encompases both noise and data granularity
- Robust against composition
- No assumptions on adversary in general
- Amplified with DP



Info gain enforcement ***only weakly protects*** *against measuring single events (but it is a robust privacy definition to prevent scaled attacks across many users).*

This presentation: in conclusion

1. Differential privacy on single events can protect users
2. Noisy, per-event data can be useful
3. “Aggregation” as a boundary is hard to rigorously defend