# PPM for ads measurement on the web

IETF 112

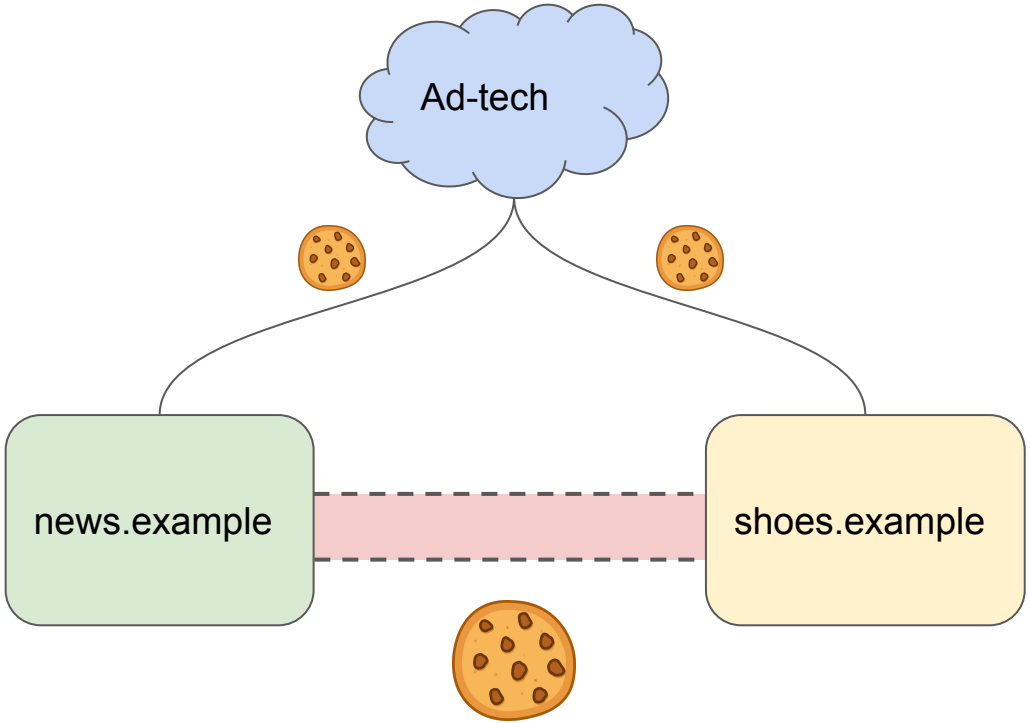
csharrison@google.com

# Problem: web privacy

- Third party cookies are bad for users' cross site privacy
- But, critical infrastructure that powers online ads depends on them
- Could we build a third party cookie alternative that gives good user privacy while still supporting ads use-cases?
    - In principle, many ads use-cases are totally fine with aggregate data!

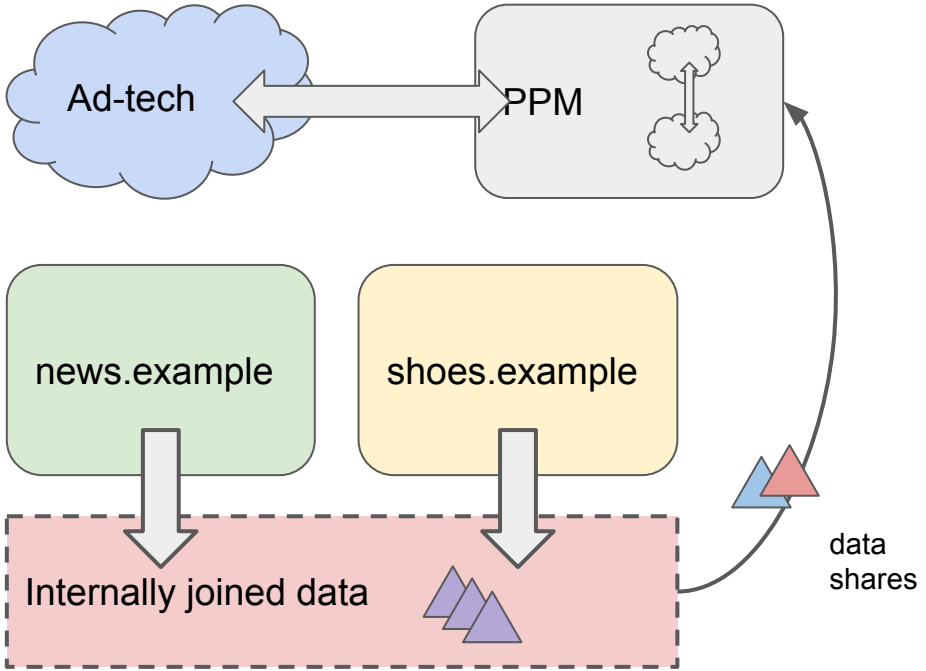
# Attribution Measurement: with cookies

- A third party cookie allows joining events from two sites
  - An impression (on a publisher site)
  - A conversion (on an advertiser site)
- This allows building a graph of user browsing activity.
- The cookie becomes a sort of mega-identity that allows your activity to be seen wherever the cookie is read



# Attribution Measurement: with PPM

- Browser internally joins two events, and generates contributions to some aggregate measure (e.g. a histogram)
  - x-axis: ad campaign
  - y-axis: number of conversions
- Browser splits contributions into shares, and submits them to the PPM system
- PPM securely aggregates and shares with ad-tech



# More use-cases to consider

- Guaranteeing differential privacy on PPM output
- Reporting under very large, sparse, domains
- Training machine learning models
  - e.g. compute pConversion given an impression
- Supporting infrastructure for ads targeting use-cases
  - e.g. github.com/WICG/turtledove
  - k-anonymity checks, ad serving measurement, etc.
- Reach measurement (how many users saw my ads?)
- Generic cross site measurement on the web

# Appendix

# Formal privacy guarantees: Differential privacy

Take two neighboring databases d and d' that differ on a single user's contributions. Run the two databases through a randomized algorithm M.

M is *epsilon* differentially private if: **$P(M(d) = O) <= e^{epsilon} P(M(d') = O)$** For all possible outputs O.

In other words, the output of M looks "basically the same" whether that single user is in the database or not, via noise introduced by M.

**PPM can guarantee that output is differentially private, even if one party is dishonest.**

- Each aggregator can add independent noise
- Clients can add noise