



PRIVACY & UTILITY ANALYSIS OF THE TOPICS API FOR THE WEB

(PETS'24 - SecWeb'24)

Yohan Beugin, Patrick McDaniel
University of Wisconsin-Madison

MADS&P

MOTIVATION

Topics API for the Web



Third-party cookies



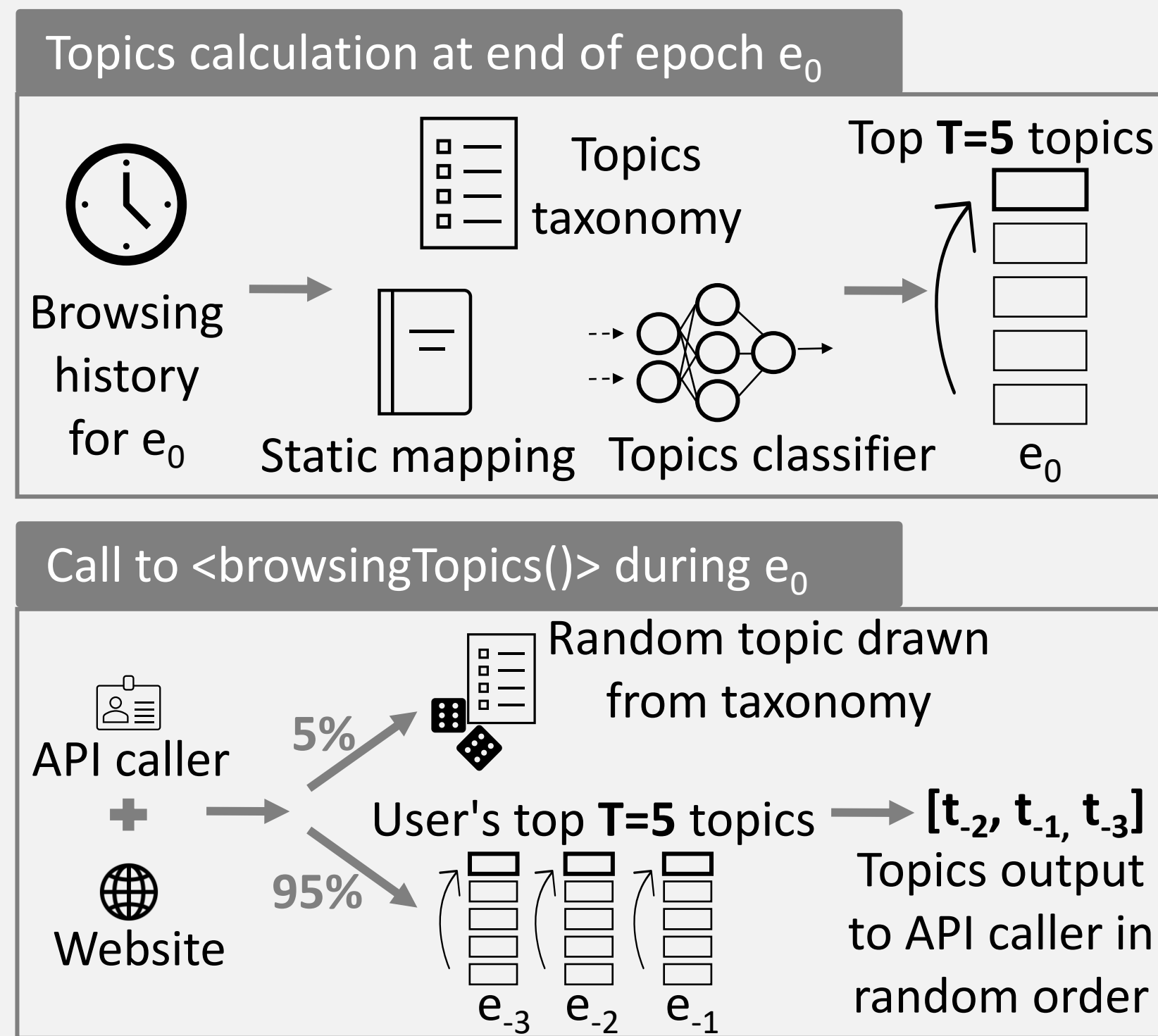
Fingerprinting



Interest-based advertising

Google's Goals

1. It must be difficult to reidentify significant numbers of users across sites using just the API.
2. The API should provide a subset of the capabilities of third-party cookies.
3. The topics revealed by the API should be less personally sensitive about a user than what could be derived using today's tracking methods.
4. Users should be able to understand the API, recognize what is being communicated about them, and have clear controls. This is largely a UX responsibility but it does require that the API be designed in a way such that the UX is feasible.

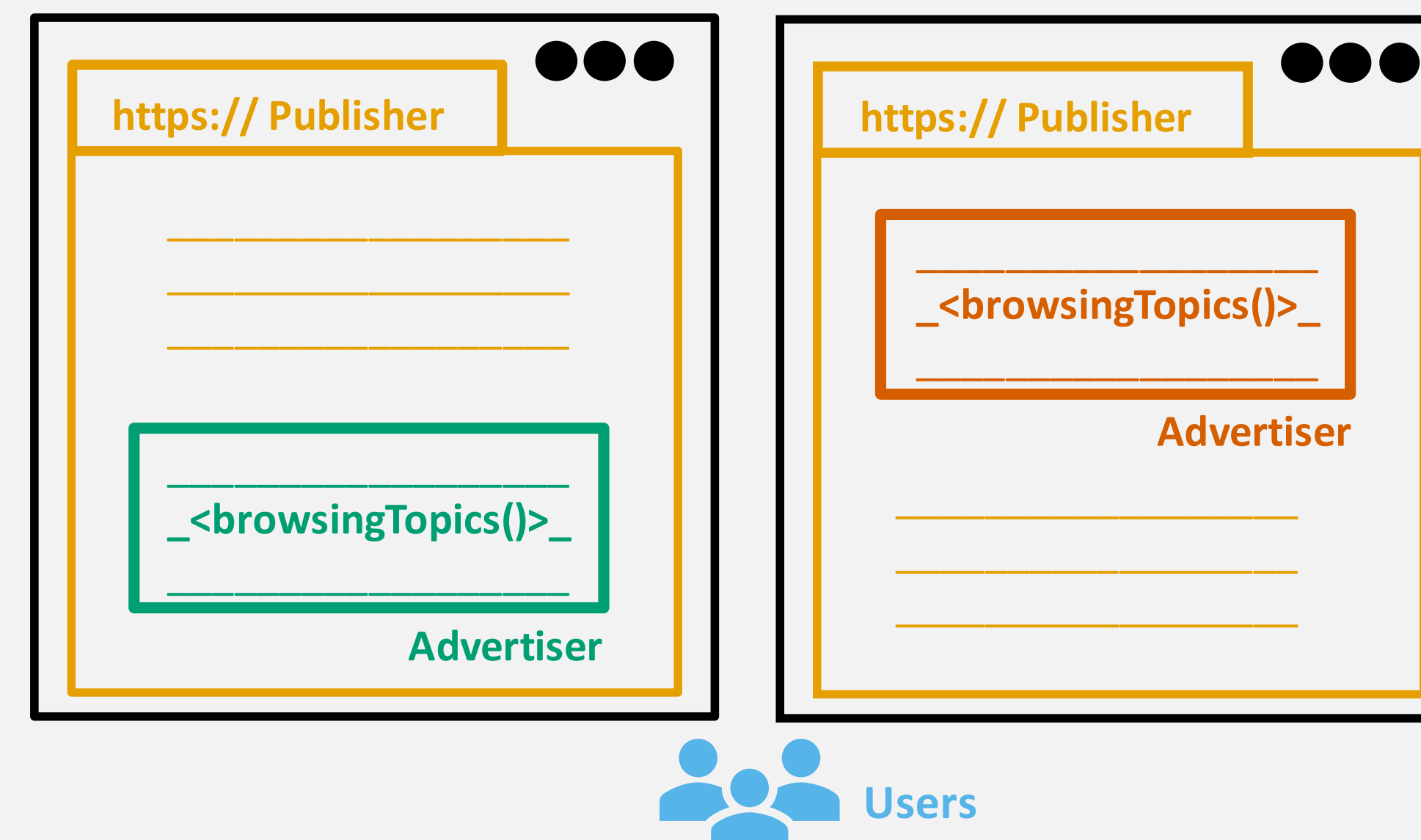


OVERVIEW

Systematic and Reproducible Analysis

- AB Goals redefined to be quantifiable
- Formal and worst-case studies
- Measurements
- Simulations on synthetic and real data

Threat Model



UTILITY EVALUATION

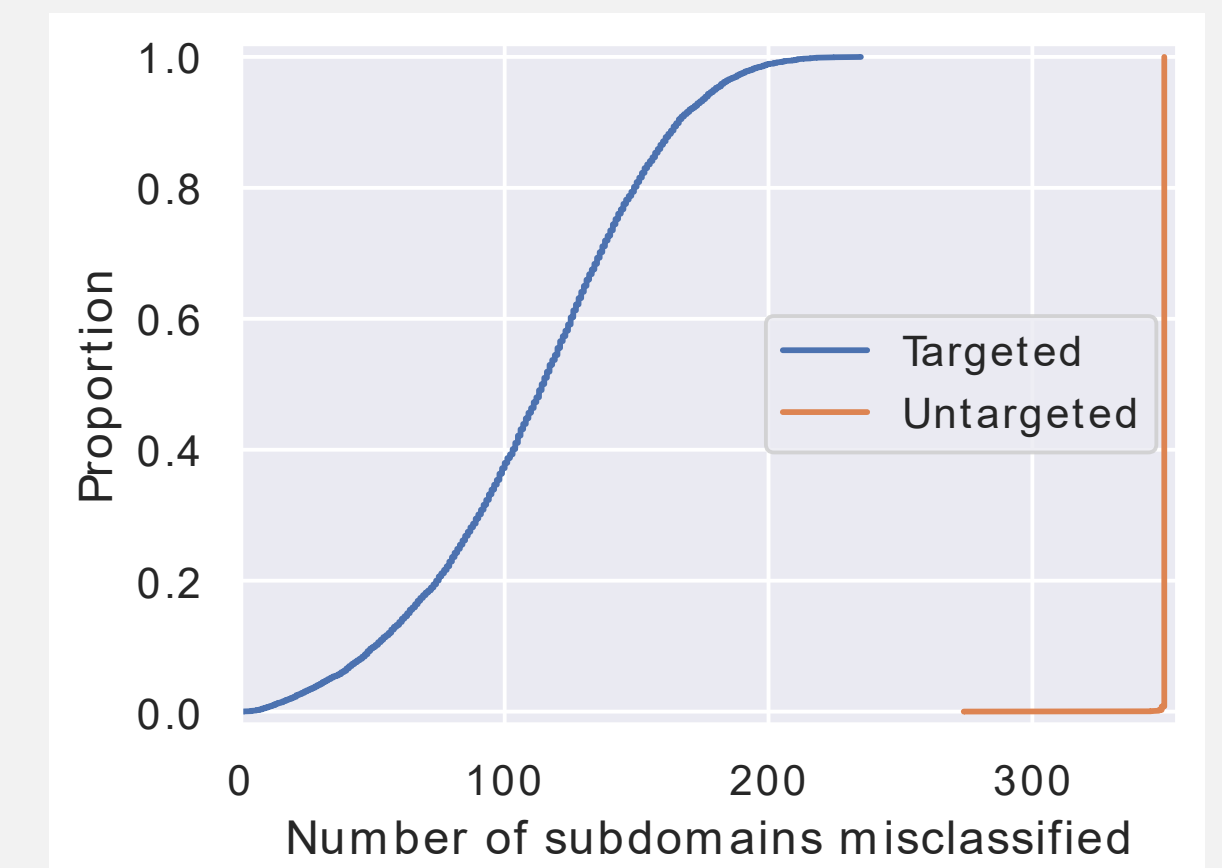
Classification Comparison

- Manual Verification (385 domains)
 - Static Mapping (10k domains)
 - Cloudflare Radar Categorization (348k domains)
- Result: **at least 1 true topic** aligned with ground truth in **about 60% of cases**

Abuse Potential

Topics (word): *Comics (batman), Dance (dance), ...*
 Domain: *example.com, ...*
 Crafted subdomains: *batman.example.com, dance.example.com, ...*

350 topics x top 10k domains = 3.5M subdomains



Result: classification can be **influenced**

PRIVACY EVALUATION

Identification of Noisy and Real Topics

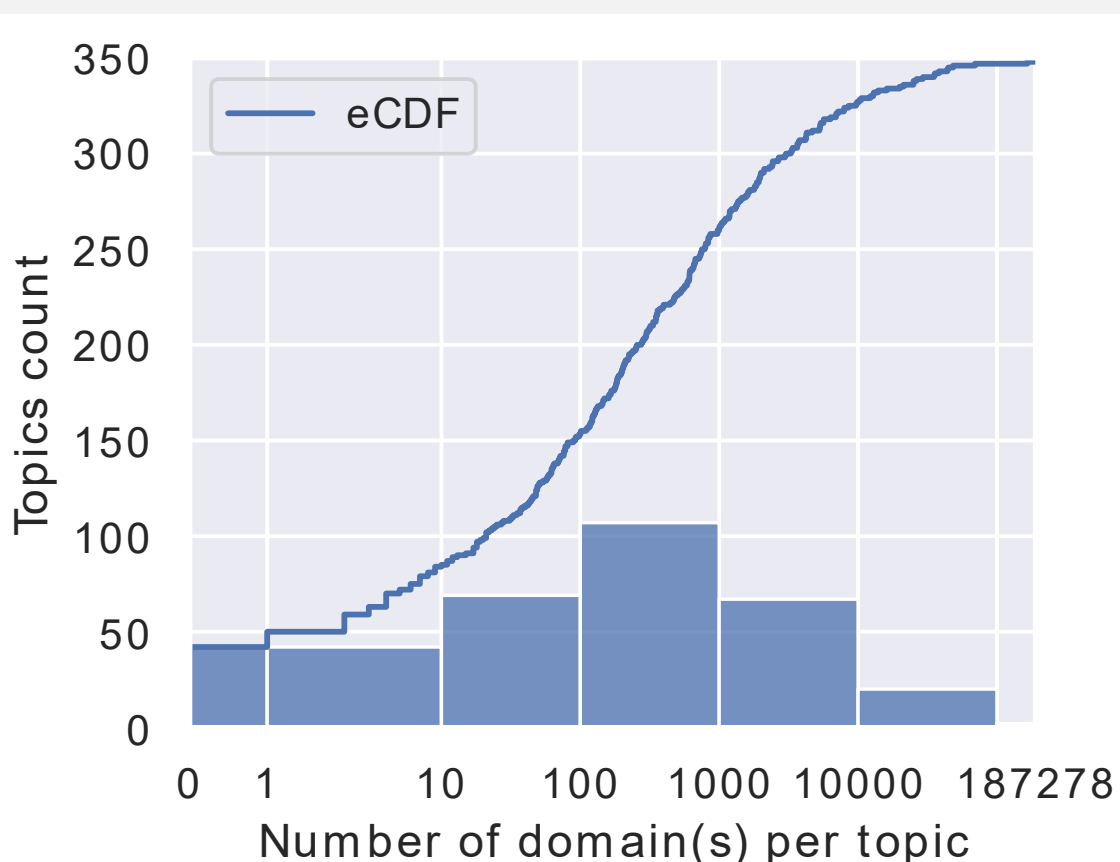
Asymmetric topics distribution on the web: our classifier considers every topic that does not appear at least on 10 websites among the top 1M as noisy.

Repetitions leak real topics: Coupon Collector's Problem.

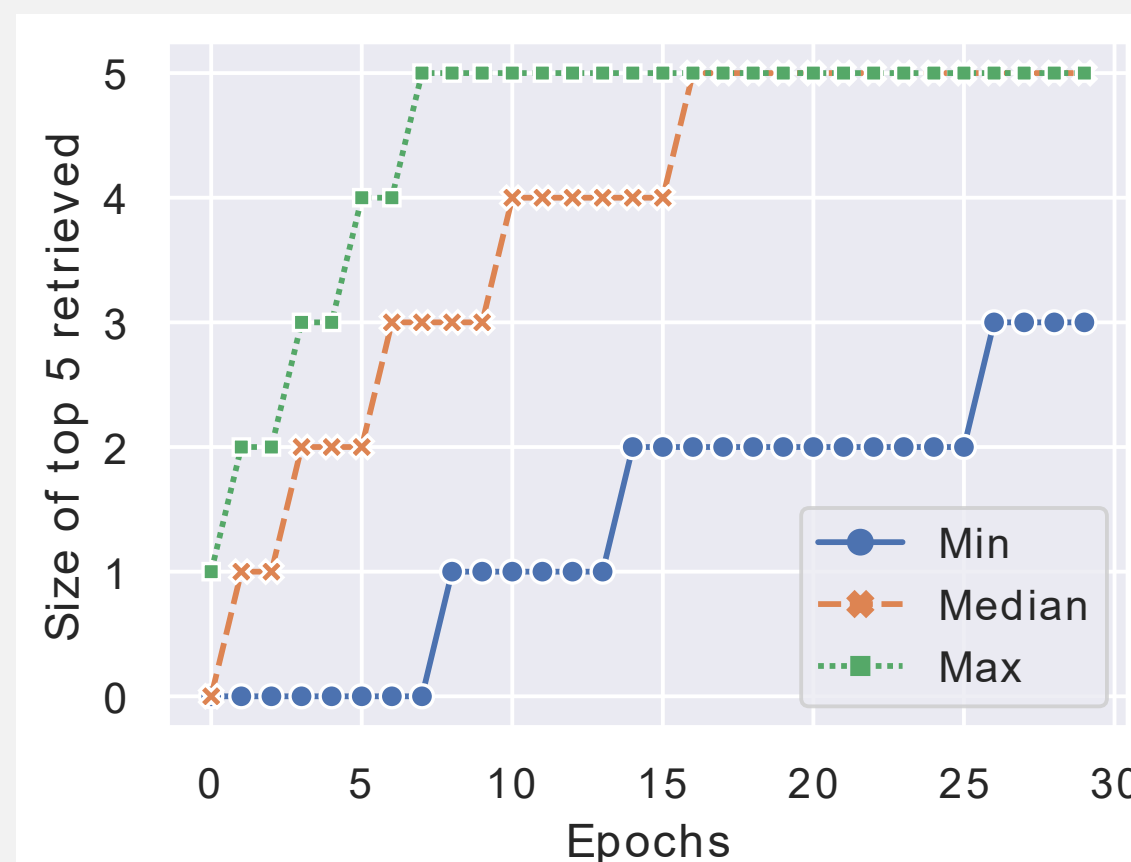
- **One-shot:** 25% of noisy topics removed.
- **Multi-shot:** 49-94% (15-30 epochs) removed.

Result: **plausible deniability can be refuted**

Epoch	Topics
0	Real: [Real Topics] Noisy: [Noisy Topics]
1	Real: [Real Topics] Noisy: [Noisy Topics]
2	Real: [Real Topics] Noisy: [Noisy Topics]
3	Real: [Real Topics] Noisy: [Noisy Topics]
4	Real: [Real Topics] Noisy: [Noisy Topics]
5	Real: [Real Topics] Noisy: [Noisy Topics]
6	Real: [Real Topics] Noisy: [Noisy Topics]



Topics distribution on top 1M most visited websites (CrUX)



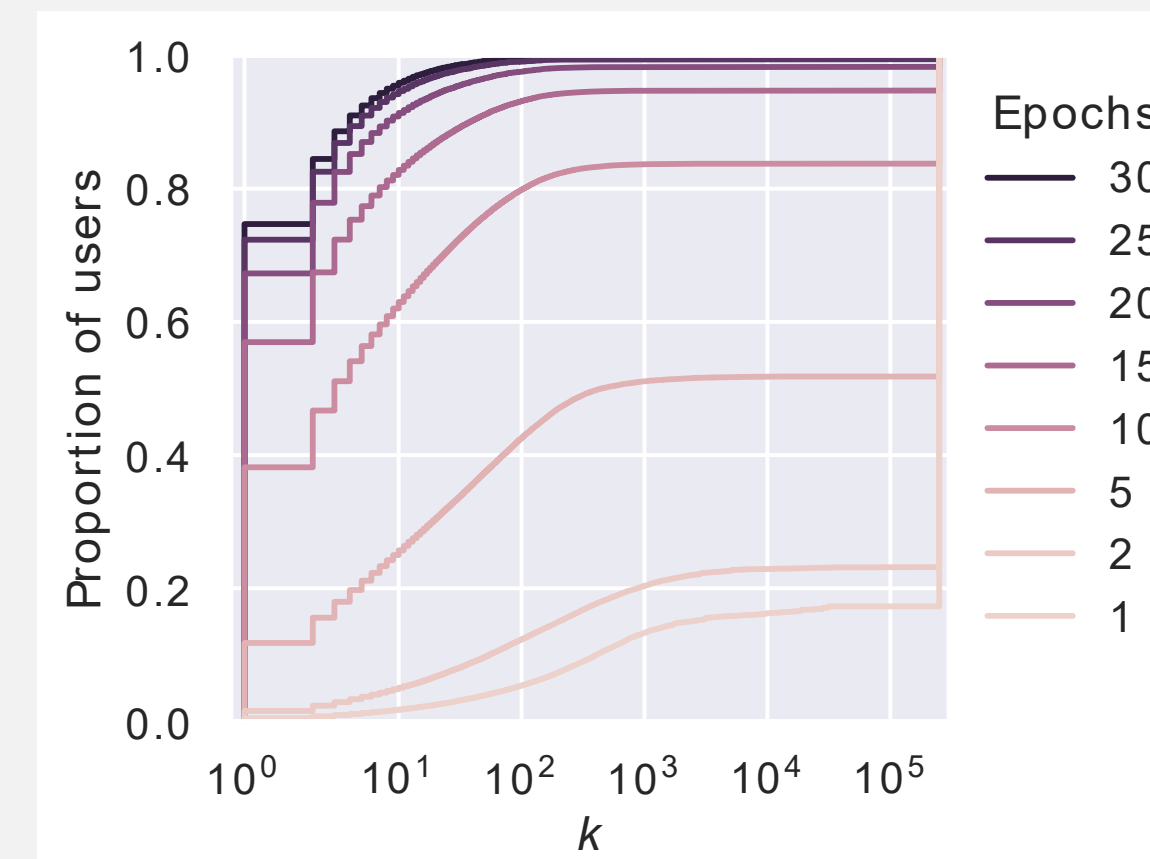
Simulation on 250k stable users

Re-identification Experiment

Simulation: quantification of the fingerprinting risk of Topics for an arbitrarily large population of users (250k) over time (30 epochs).

k-anonymity across time: How "difficult" is it to re-identify "significant numbers of users across sites"?

Result: users can be **fingerprinted by the Topics API**



Measurement on Real Browsing Histories

Real data: 1207 users from Germany over 5 weeks in October 2018.

- **Uniqueness:** 94% have unique topics profiles.
- **Stability:** at least 47% have 3 or more stable topics.

Topics observation(s)	Users re-identified
1	46%
2	55%
3	60%

Result: third parties can **track users across websites** by observing their topics

TAKEAWAYS

Topics API can be used to Fingerprint Users

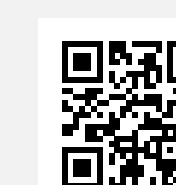
- Topics can not guarantee non re-identification across websites to all users.
- Users have stable and unique web behaviors that need to be considered.
- Google's non-reproducible analyses are disconnected from reality and lack systematization in their approach.

Some Utility Retained, but Classification can be Manipulated

- Topics returned are somewhat aligned with users' interests.
- Utility buckets introduced after advertisers' feedback is making topics profiles more unique (privacy-utility tradeoff).
- Unclear if Google's current mitigation (external attestation mechanism) will prevent further abuse.

Need for a (Research) Sandstorm through the Privacy Sandbox

- Call for reproducible analyses and release of tools and datasets.
- More evaluations are required to understand all potential impacts.
- Launch of a new research hub at <https://privacysandstorm.com>



<https://yohan.beugin.org>



yohan@beugin.org