Privacy-Preserving Architecture: From W3C Standards to Smart Cities

Presenter: Pierre Tholoniat*

Other student participants: Alison Caulfield*, Giorgio Cavicchioli*, Mark Chen*, Navid Pargoo, Shuren Xia**, Xiaotian Zhou****

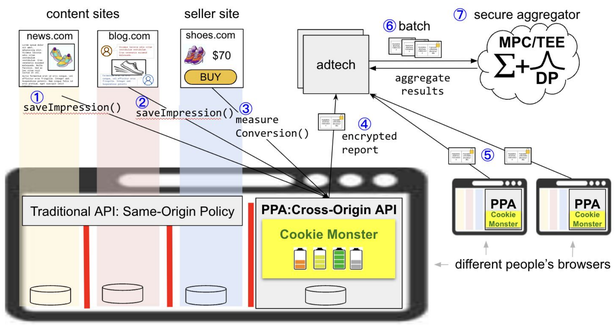
CS3 Faculty: Roxana Geambasu* and Jorge Ortiz**

***Columbia University & **Rutgers University**

The Web Privacy Challenge & Cookie Monster

- Historically, online advertising relied on cross-site tracking via cookies and fingerprinting, fueling web surveillance.
- Browsers are developing **privacy-preserving APIs** for ad measurement (PPA).

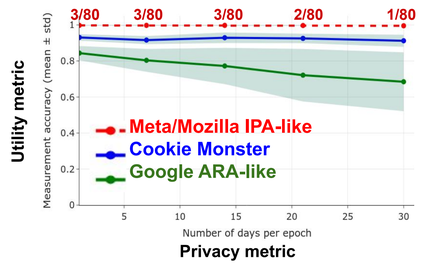
Privacy-Preserving Attribution: Level 1
Editor's Draft, 3 March 2025
▾ More details about this document
This version:
https://w3c.github.io/ppa/



Cookie Monster is the privacy architecture we developed for the W3C's PPA draft standard.

- Ensures per-browser privacy budgeting to control data exposure.
- When the privacy budget is depleted, only encrypted null reports are sent, stopping user-data flow.
- This puts the user's own browser in full control of their cross-site privacy.

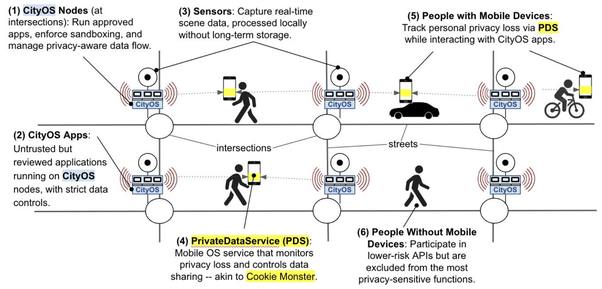
- Cookie Monster tracks **differential privacy (DP) loss** individually per browser, enforcing a budget for each adtech.
- It does so **more efficiently** than initial APIs from Meta/Mozilla and Google (see graph).
- This lets adtechs measure and optimize ad effectiveness without tracking users.



- The development of Cookie Monster, led by Geambasu's team, provided the first **well-defined privacy architecture** that was lacking in initial API proposals.
- **PPA API,** built on Cookie Monster architecture, is now advancing in standardization, with all major browsers involved. **Demo available here. Code available here.**
- If successful, could be rolled out to billions of devices and change privacy world-wide.

The Smart City Privacy Challenge & CityOS

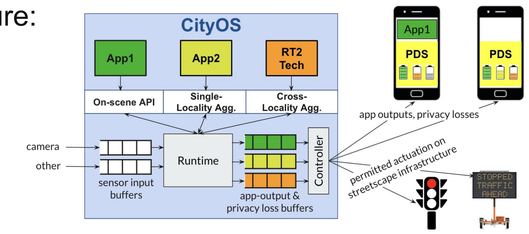
- Cities risk repeating the web's privacy mistakes with urban data collection.
- Surprising analogies exist between privacy risks and data access patterns on the web vs. in smart cities.



CityOS is a preliminary but **comprehensive privacy design** for smart cities, inspired by Cookie Monster and web APIs.

- Provides **built-in privacy** for urban data collection.
- Exposes a **structured API** for accessing streetscape data streams.
- Incorporates **privacy loss accounting** for aggregation-oriented endpoints, putting users' devices in control of privacy for most egregious aggregations.

- Features a three-tiered privacy architecture:
  1. **On-Scene API**: Real-time data with no tracking
  2. **Single-Locality Aggregation**: DP localized statistics
  3. **Cross-Locality Aggregation**: Privacy-aware citywide measurements, mediated by user devices
- Architecture roughly corresponds to web APIs, but aims to improve upon first-party web APIs and mirrors the PPA API with Cookie Monster privacy.



- Geambasu & Ortiz's team are now implementing and evaluating CityOS on several CS3 applications, with plans to expand to more apps and RT2 technologies in Year 4. **Demo available here. Code not yet public but will be.**
- If successful, this will be the world's first well-defined privacy architecture for smart cities—and progress on it may feed back to web/mobiles.

This work was supported by the National Science Foundation (NSF) and Center for Smart Streetscapes (CS3) under NSF Cooperative Agreement No. EEC-2133516.