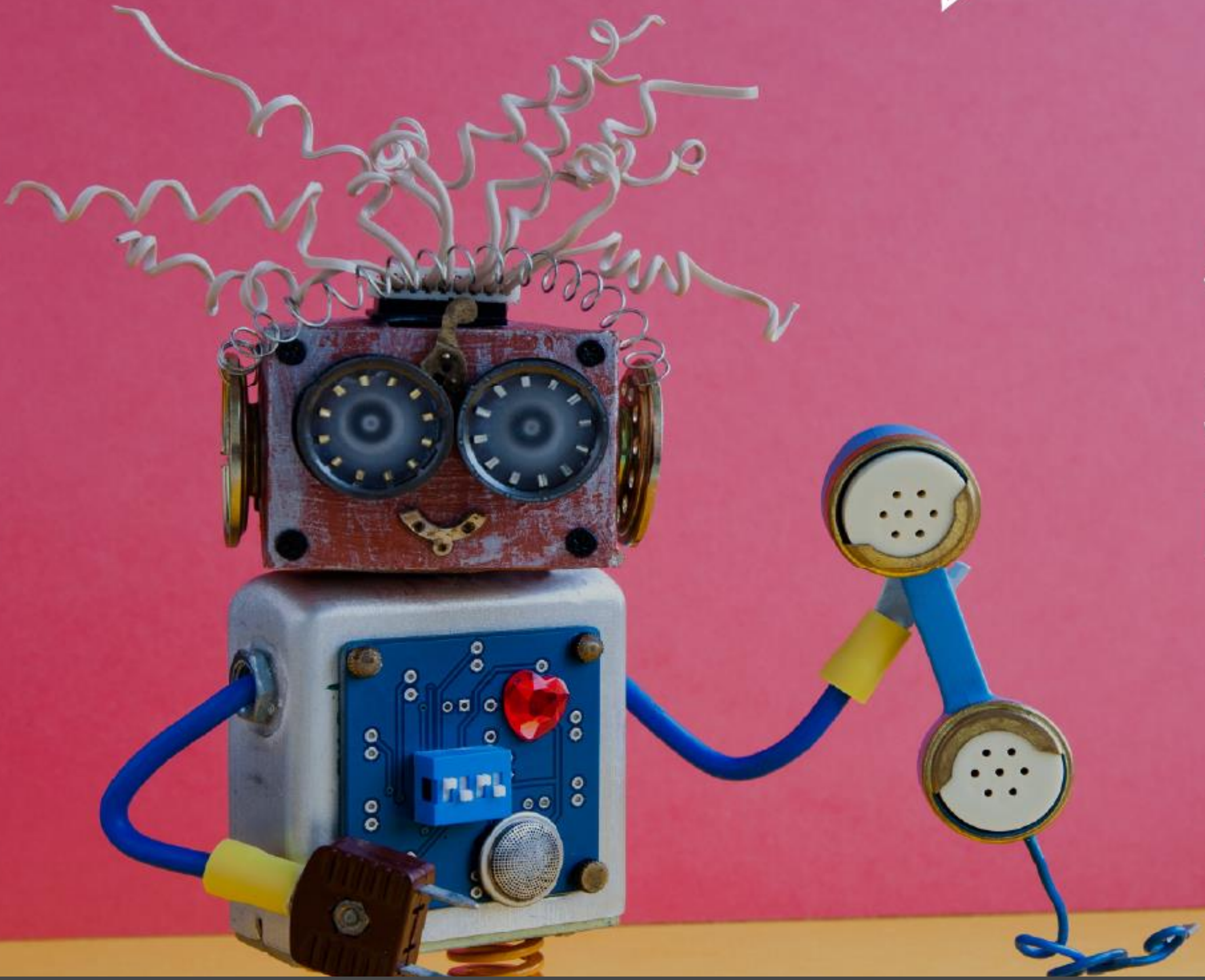
iab. australia

WEBINAR SERIES

THURSDAY 10 DECEMBER
2 PM - 2:45 PM



STATE OF PLAY:

3RD PARTY COOKIES, IDENTITY AND PROJECT REARC

THIS WEBINAR WILL START SHORTLY

Jonas Jaanimagi

Technology Lead

IAB Australia

Project Rearc Update & Identity State-of-Play

Jordan Mitchell

SVP, Head of Consumer Privacy, Identity & Data, IAB Tech Lab

iab. TECH LAB

Ongoing Identifier Challenges and Re-Architecting our Industry

Jordan Mitchell
SVP – Identity, Data and Privacy
IAB Tech Lab

iab. TECH LAB

Agenda Today

- Refresher on Project Rearc
- Updates from Accountability and Addressability Working Groups
- Other relevant states of play:
  - The latest on the UID2 proposal from The Trade Desk
  - An update on the Partnership for Responsible Addressable Media
  - W3C update

Key Takeaways

Digital advertising systems depend on 3P identifiers to support key use cases. Cookies, device IDs and the signals for fingerprinting are all being removed.

Short-term “work-arounds” only fuel their narrative and exacerbate the problem.

We must re-architect systems & processes for privacy-preserving addressability:

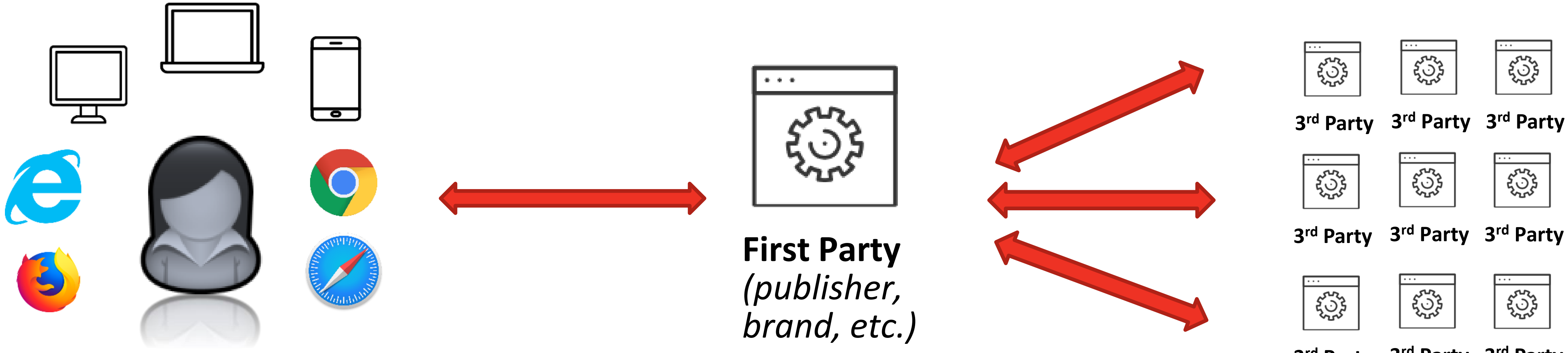
- Technical standards, guidelines and best practices
- Accountability/compliance program

Tech Lab is heads-down focused on collaboration towards standards to achieve:

- Predictable privacy for consumers through the 1st parties they trust
- Increased accountability and trust for our industry
- Improved market innovation and competition

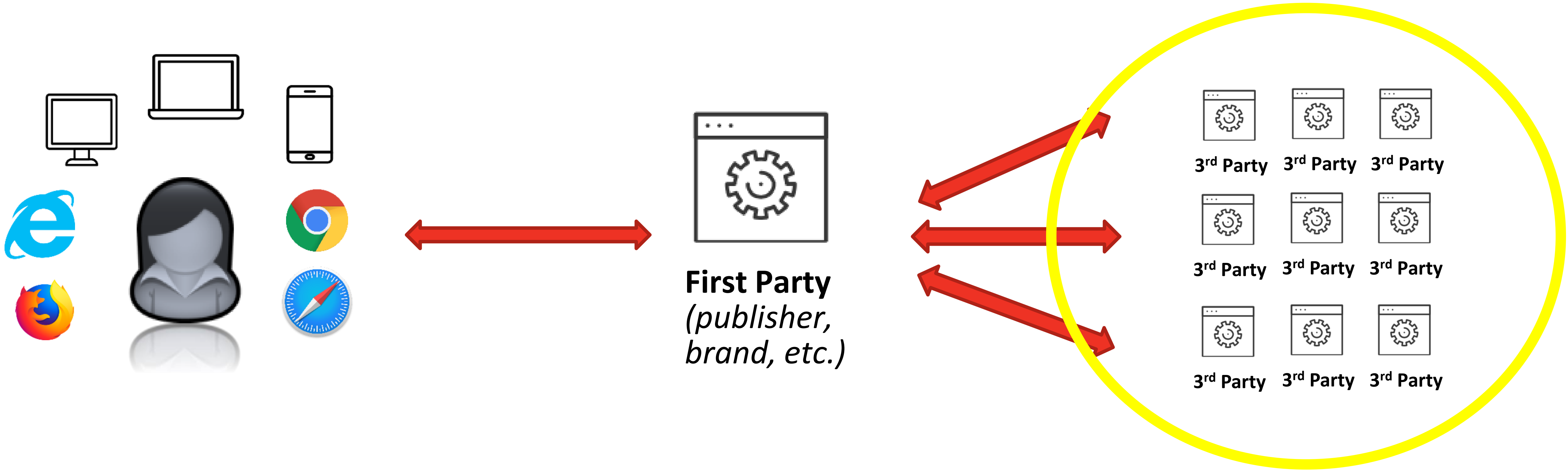
If you want to go fast, go alone. If you want to go far, go together.

The Benefits of an Open Ecosystem



Fantastic innovation in consumer content, services and conveniences.
Rich set of third-party vendors to support first party business models and use cases.
Consumers get to choose the first parties they utilize, rely on and trust.

The Challenges of an Open Ecosystem



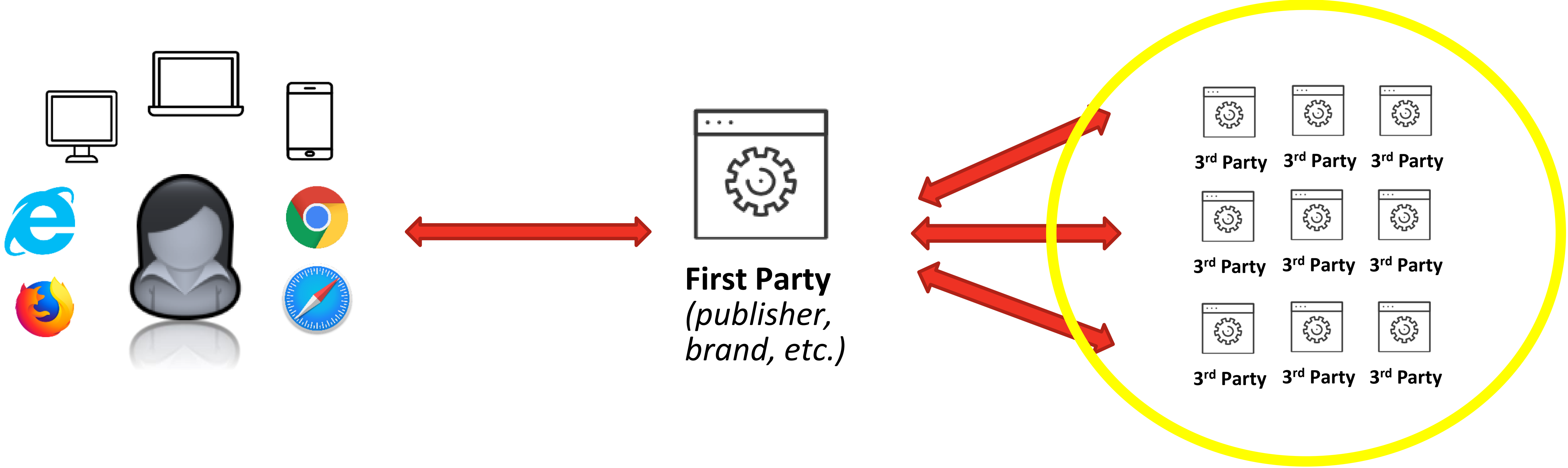
Many parties involved in the delivery of consumer experiences.

Opaque consumer data collection, sharing and use.

First party data leakage.

Fragmented consumer transparency and control.

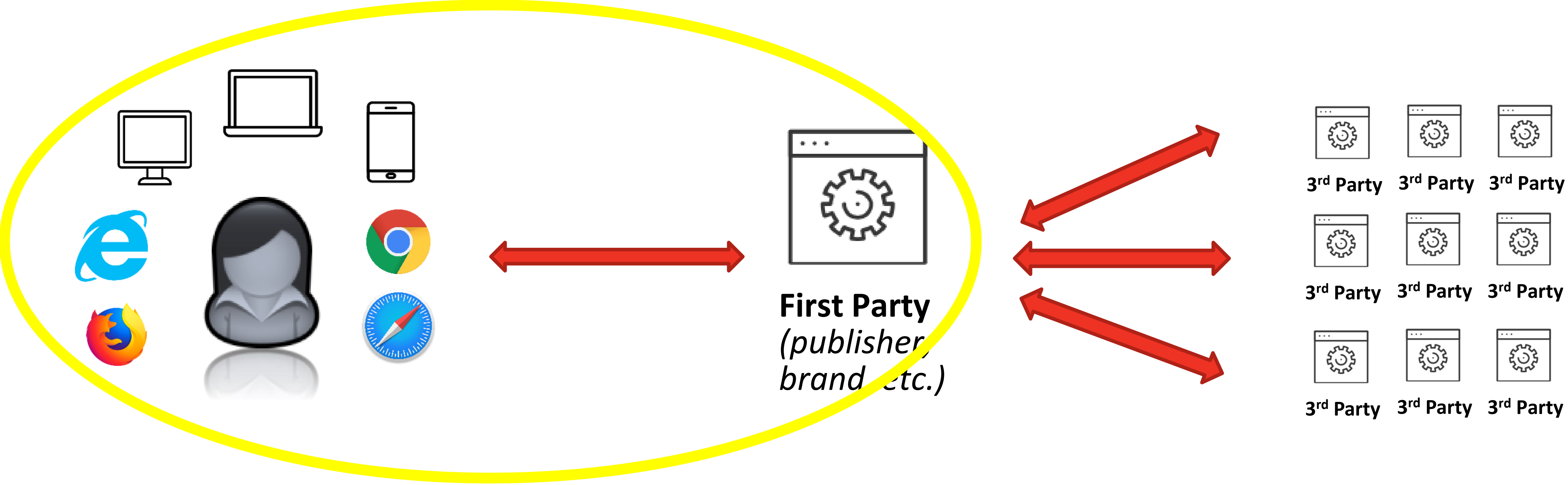
The Approach of Leading Browser/OS Platforms



Privacy by default (or privacy by decree)?

Cut off third-party access to device IDs, hindering core business activities.
Establish "custody" over the consumer (paternalistic decision-making).
Fracture open standards and UX convention.
Further confuse consumers across devices and channels.

Our Approach – Predictable Consumer Privacy thru Standards



It's up to Consumers and the First Parties they choose to engage with!

Standardized signals for consumer privacy preferences.

Standardized signals for first party data usage rights.

Secure IDs and personal data from unauthorized use.

Establish supply chain trust with auditability and accountability.

Participation within Tech Lab Working Groups

Participation from **37** countries!

20 industry trade orgs globally, including **12** national/regional IABs and the **Partnership for Responsible Addressable Media**

Project Rearc Task Force – **599** people from **379** companies

Addressability Working Group – **228** people from **134** companies

Accountability Working Group – **225** people from **121** companies

The Process

Phase 1 – Understanding the Problem *

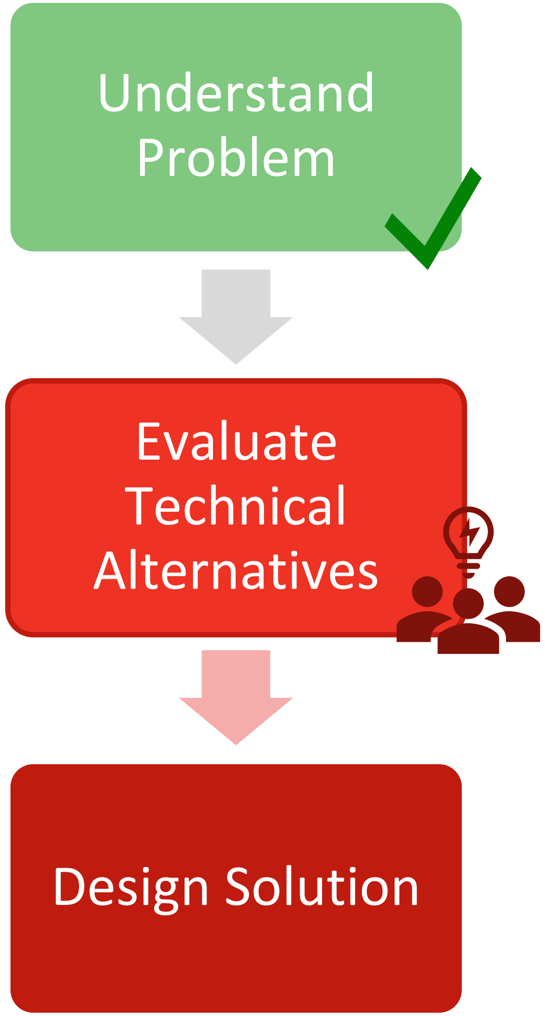
- ✓ Business activities and identifier dependencies
- ✓ Business impact from loss of identifiers
- ✓ Privacy issues and principles

Phase 2 – Understanding Technical Alternatives *

- Discussion of technical alternatives
- Business, technical, and policy considerations around each
- Definition and application of evaluation criteria
- Browser/OS proposal analysis and feedback
- Selection of proposed alternative(s)

Phase 3 – Solution Design of Selected Alternative(s)

- Business and policy requirements
- Minimum standards required, including accountability mechanisms



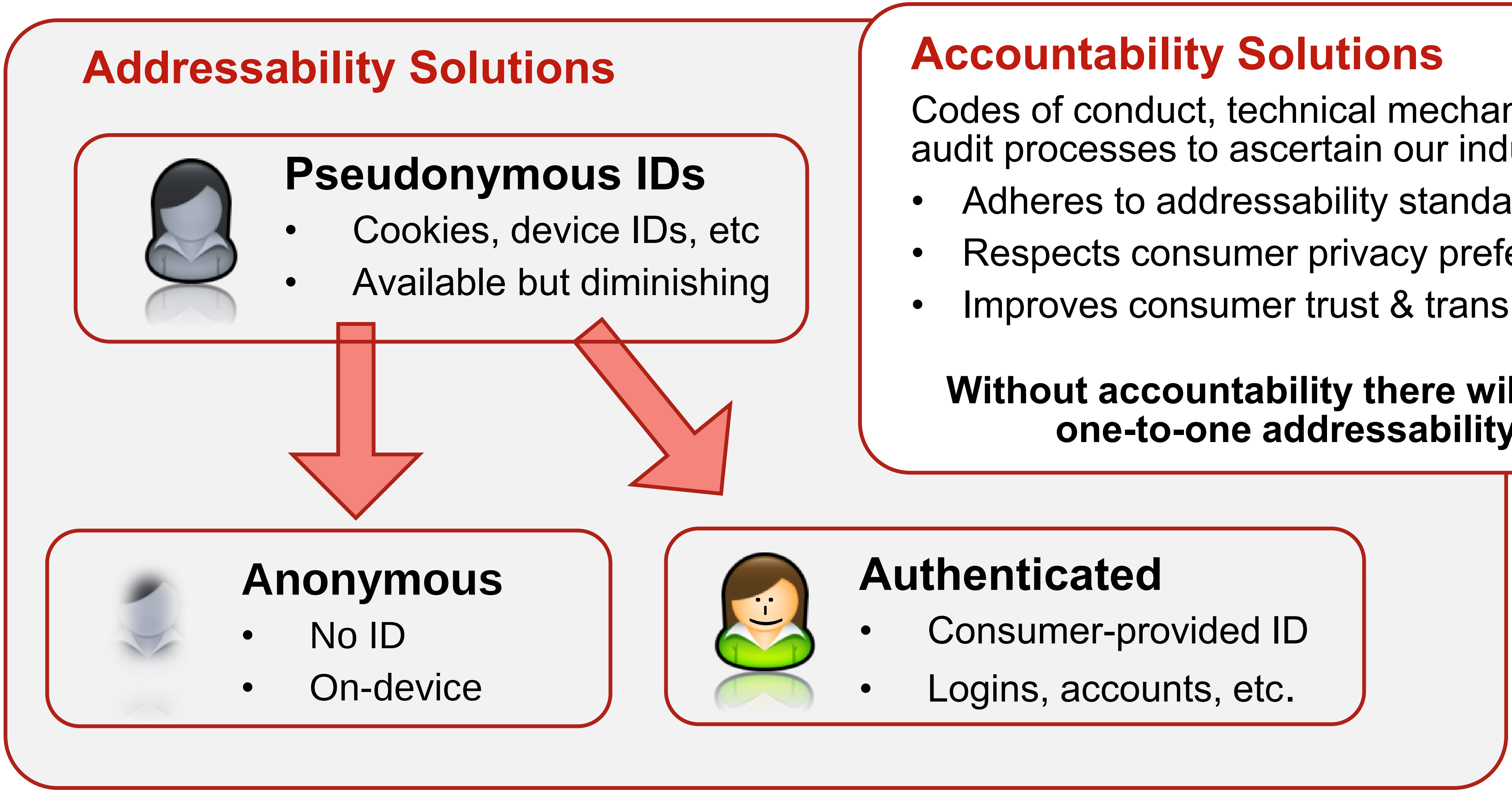
Understand Problem

Evaluate Technical Alternatives

Design Solution

* Drawing from work-in-process by other organizations and efforts.

Current Proposals in Active Discussion



Addressability Solutions

Pseudonymous IDs

- Cookies, device IDs, etc
- Available but diminishing

Anonymous

- No ID
- On-device

Authenticated

- Consumer-provided ID
- Logins, accounts, etc.

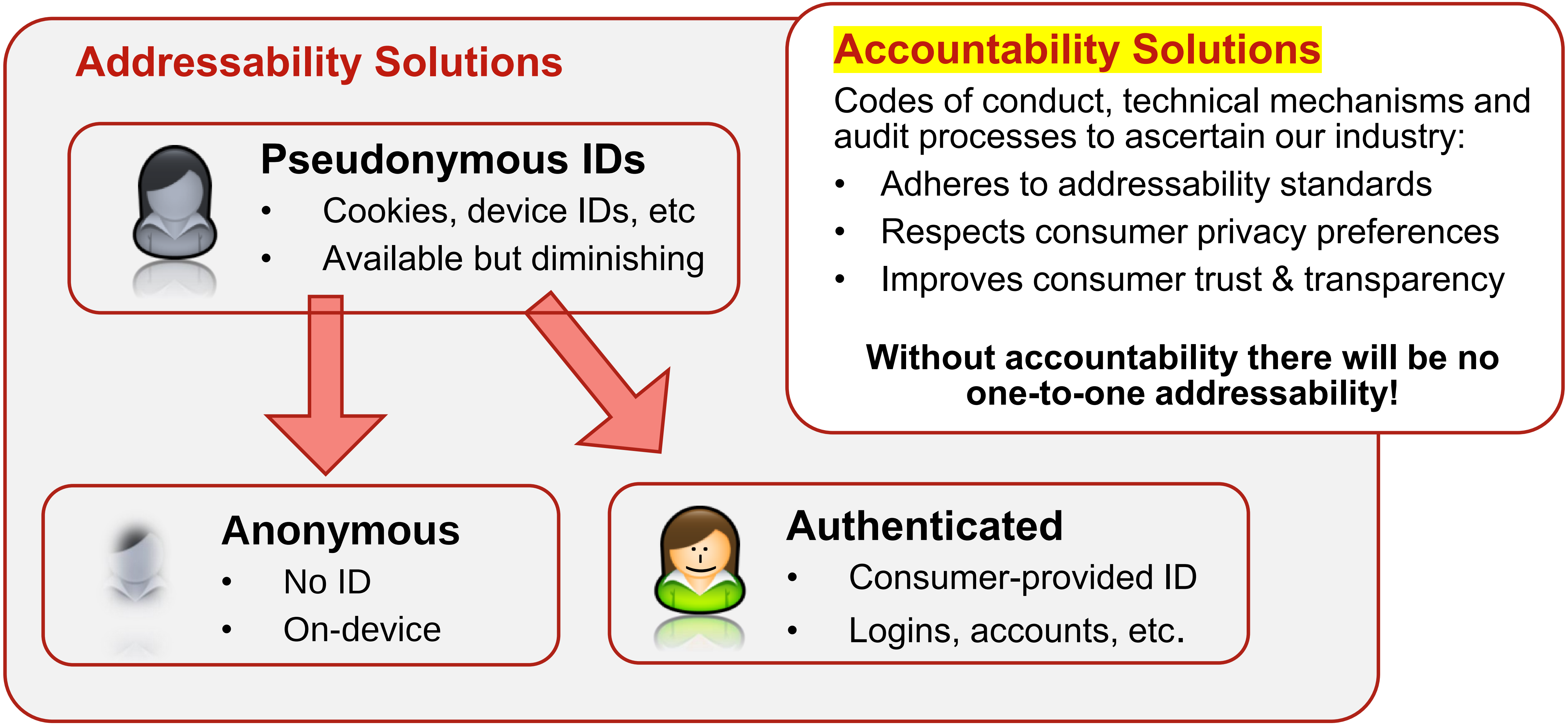
Accountability Solutions

Codes of conduct, technical mechanisms and audit processes to ascertain our industry:

- Adheres to addressability standards
- Respects consumer privacy preferences
- Improves consumer trust & transparency

Without accountability there will be no one-to-one addressability!

Current Proposals in Active Discussion



Addressability Solutions

Pseudonymous IDs

- Cookies, device IDs, etc
- Available but diminishing

Anonymous

- No ID
- On-device

Authenticated

- Consumer-provided ID
- Logins, accounts, etc.

Accountability Solutions

Codes of conduct, technical mechanisms and audit processes to ascertain our industry:

- Adheres to addressability standards
- Respects consumer privacy preferences
- Improves consumer trust & transparency

Without accountability there will be no one-to-one addressability!

Establishing Supply Chain Trust and Accountability

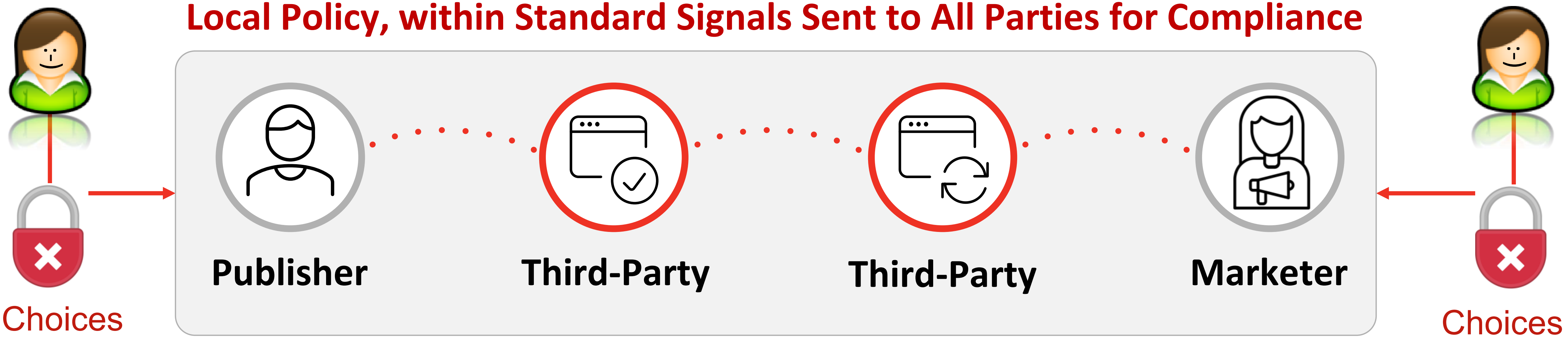
How do we consistently demonstrate (with data) supply chain accountability and adherence to consumers' data rights and privacy choices?

There are four areas of work coming together:

1. Global Privacy Framework (standardized, encoded consumer privacy signals)
2. Accountability program guidelines / best practices (rules)
3. Technical mechanisms (system-level, auditable data structures)
4. Attestation framework (methods and processes)

1. Global Privacy Framework

Local Policy, within Standard Signals Sent to All Parties for Compliance



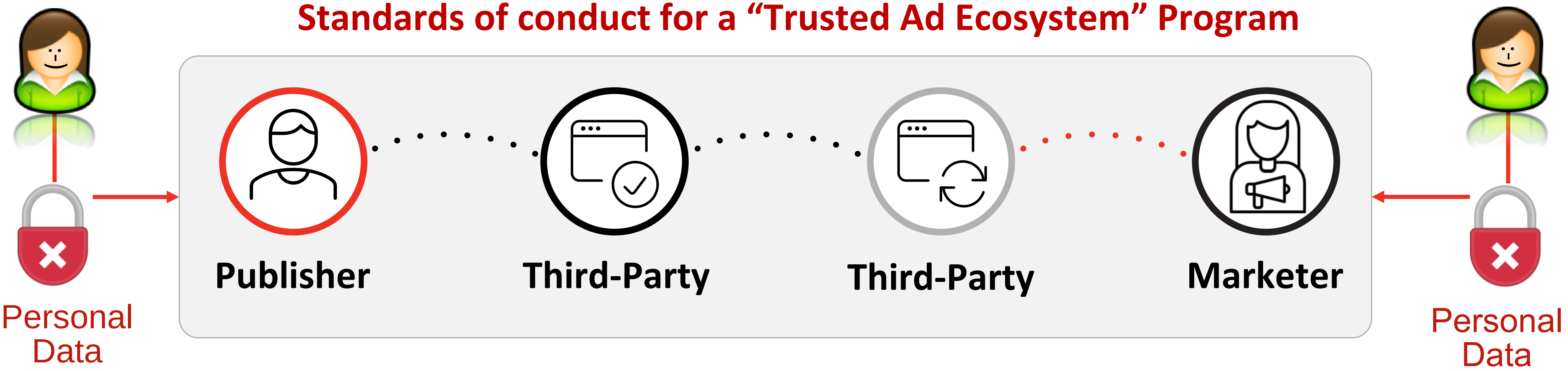
Privacy choices offered and encoded into a standard format based on jurisdiction.

All parties receive the "privacy string" and must comply with choices therein.

Privacy choices offered and encoded into a standard format based on jurisdiction.

- Global Privacy [Technical] Framework, building on TCF/CCPA work:
  - Common tech standards (modular schema, APIs, etc.) across jurisdictions
  - Global registry of companies, managed regionally
  - Reduce cost of compliance for industry members
  - Rapid adaption to regulatory & commercial market demands across channels

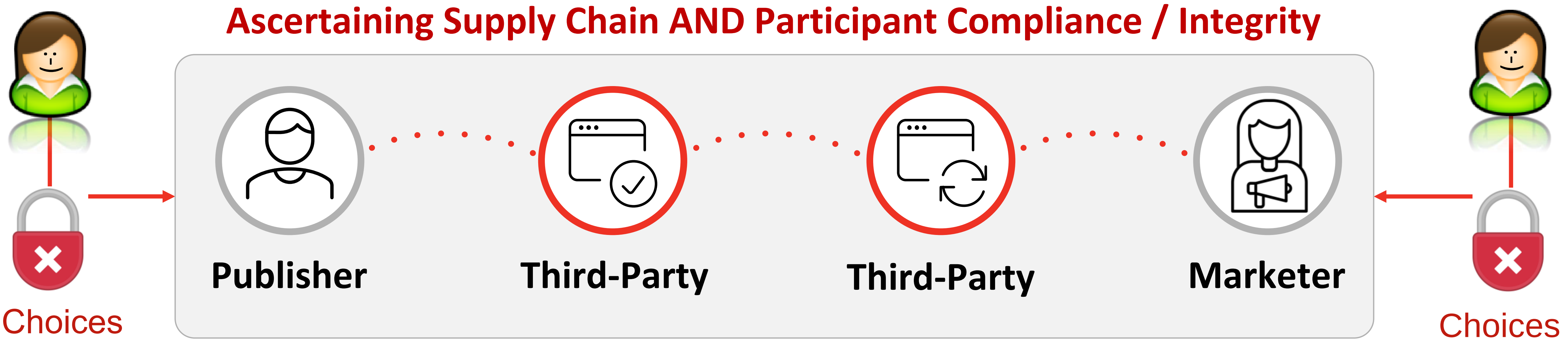
2. Accountability Program Guidelines



Only participants "in good standing" may access/use IDs + personal data, subject to:

- Relevant jurisdiction and rulesets for responsible data practices
- Non-sensitive/special category content
- Compliance with consumer privacy choices
- Identifier safeguarding via real-time shared oversight mechanisms
- Adherence to technical monitoring mechanisms

3. Technical Mechanisms + Auditable Data Structures

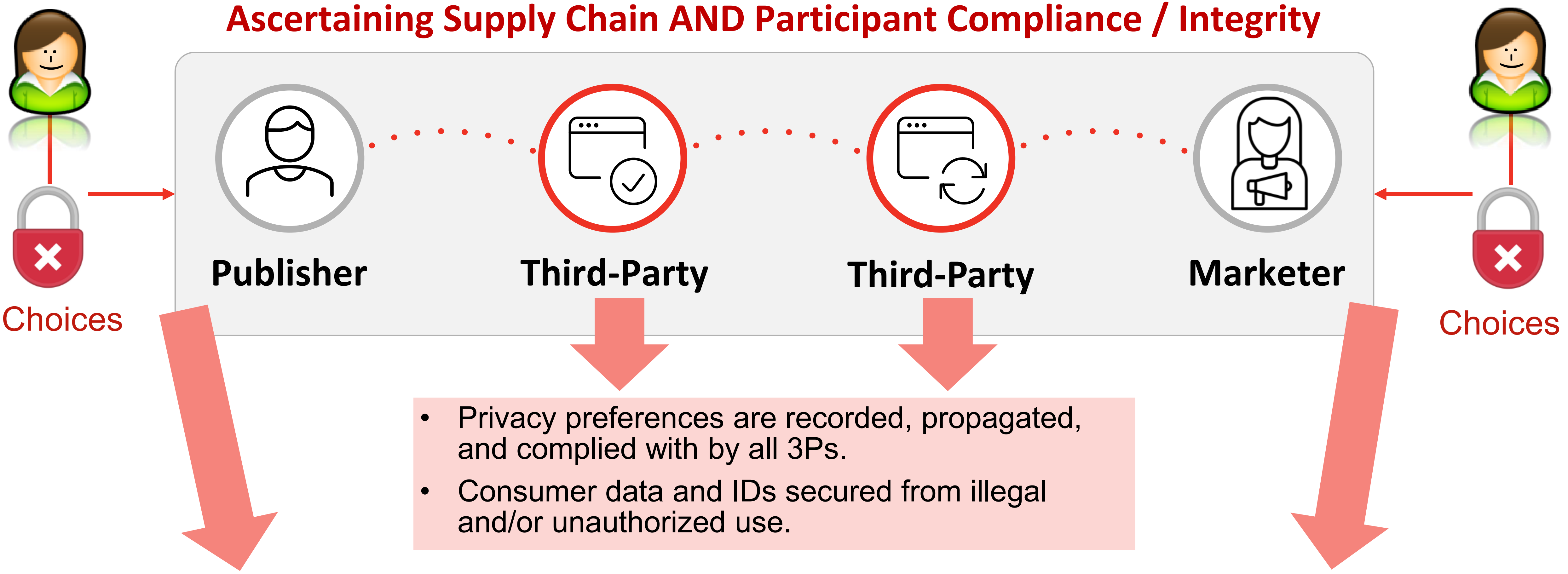

Ascertaining Supply Chain AND Participant Compliance / Integrity
Publisher
Third-Party
Third-Party
Marketer
Choices
Choices

Standardized, traceable, tamper-proof signals and data structures:

- Consent strings
- Transaction IDs
- Use declarations (beacons, ad responses, etc.)
- Chain of custody
- Log-level proofs for independent and open reviews/audits

4. Attestation Framework

Ascertaining Supply Chain AND Participant Compliance / Integrity



- Privacy preferences are recorded, propagated, and complied with by all 3Ps.
- Consumer data and IDs secured from illegal and/or unauthorized use.

- Offered appropriate choice, transparency and control; recorded correctly.
- Preferences are passed to every participant involved in the digital experience.

Accountability Compliance Program Components (Near-term Roadmap)

Schema

Firm up current properties to log and when

Sampling

Determine sampling methodology

Interface

Design how data will be submitted to audit service

Transaction IDs

Determine how transaction IDs will be created/linked

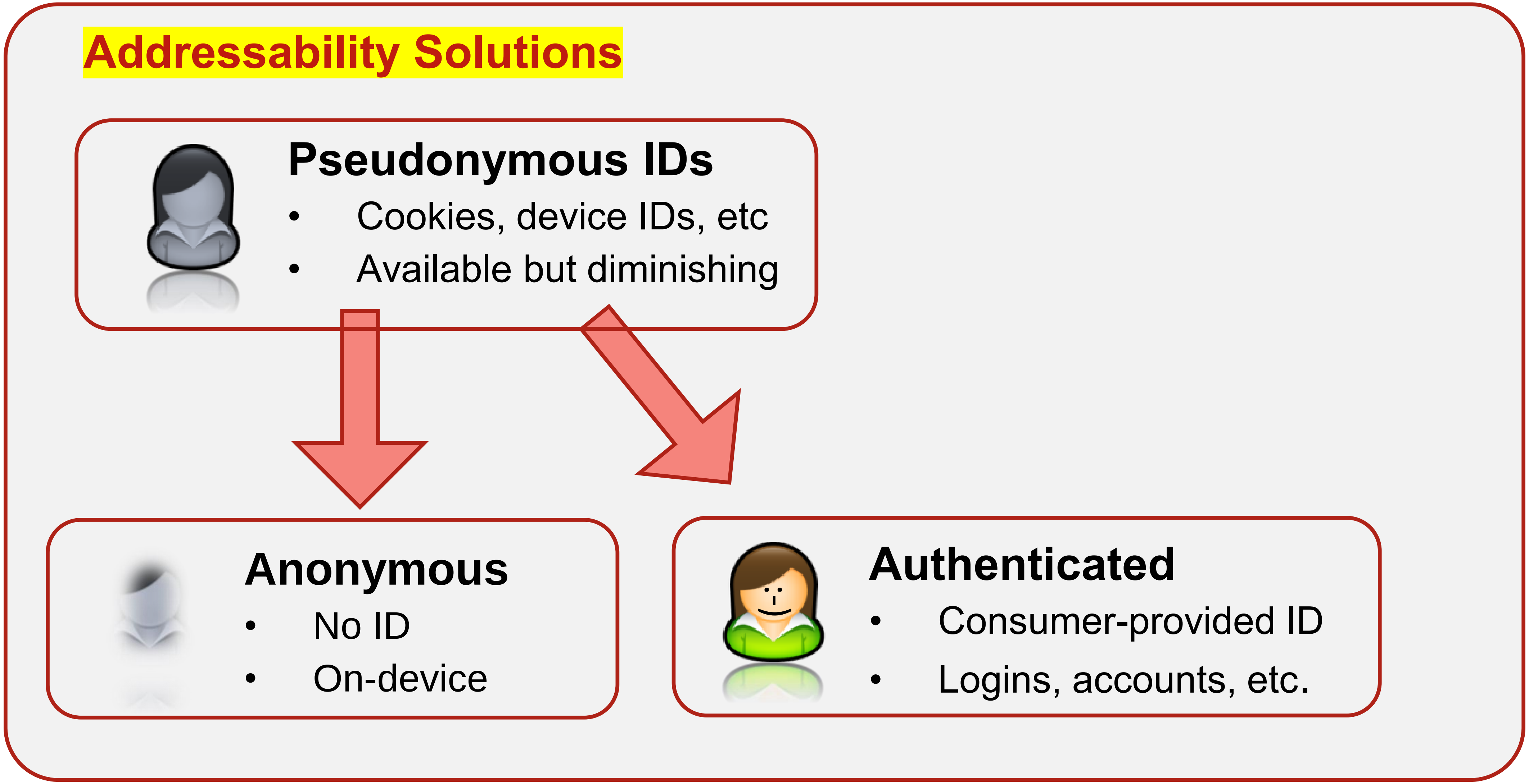
Code(s) of Conduct

Work with policy peers to determine rulesets and make sure tech designs can support > 1 code of conduct

Program Operations

Account for regional roles, governance, delivery model, etc…

Current Proposals in Active Discussion



Addressability Solutions

Pseudonymous IDs

- Cookies, device IDs, etc
- Available but diminishing

Anonymous

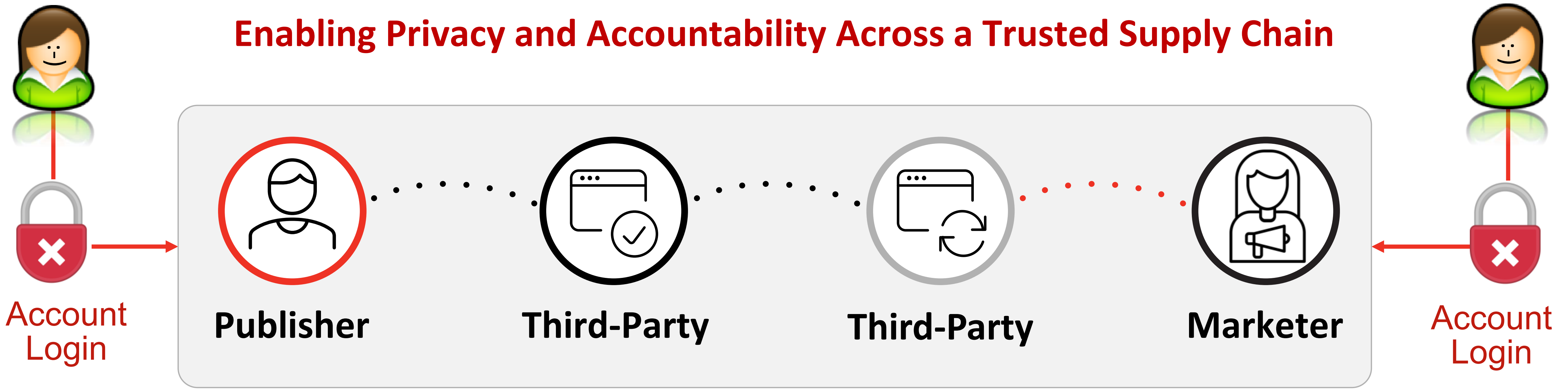
- No ID
- On-device

Authenticated

- Consumer-provided ID
- Logins, accounts, etc.

Standards for Authenticated Consumers

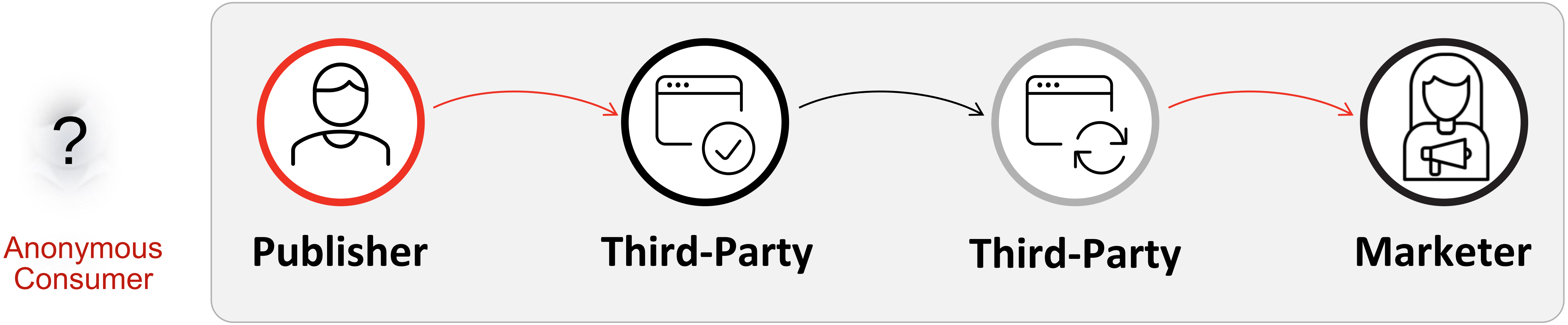
Enabling Privacy and Accountability Across a Trusted Supply Chain



- Ensure responsible use of consumer-provided identifiers.
- Allow third parties to execute on behalf of trusted first parties, without enabling unauthorized third-party tracking / data collection.
- Standardized consumer messaging, policies, disclosures, controls.
- Tech standards and accountability/compliance mechanisms.

Passing Content/Contextual Attributes When There's No 3P ID …

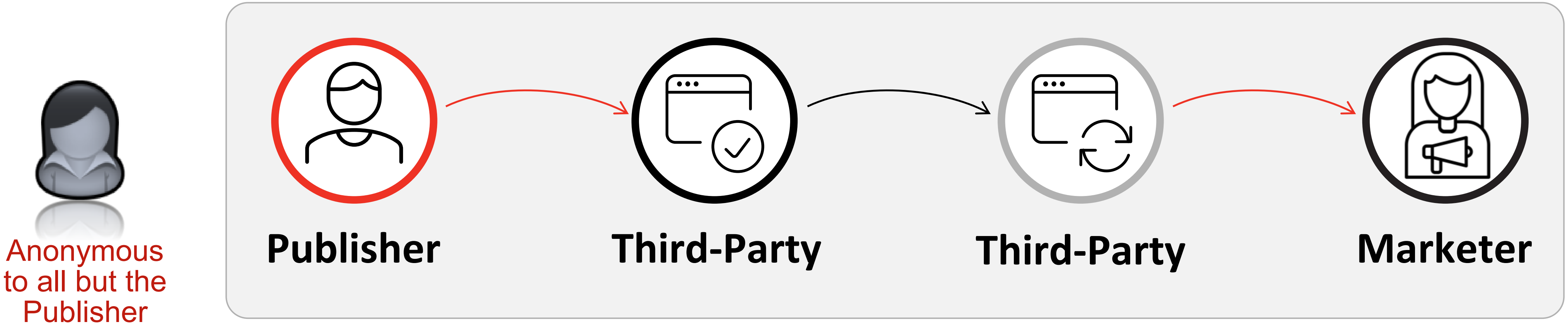
Standardized Taxonomy and Process Enables Scale for Sellers/Buyers



- Information about page, site, app, stream, etc. AND the context
- Passed within OpenRTB at seller's option (w/out user ID)
- Working in partnership with Prebid.js (code to deploy)
- Content Taxonomy is relevant
- Privacy, measurement and brand safety guidance

Passing 1P Audience Attributes When There's No 3P ID …

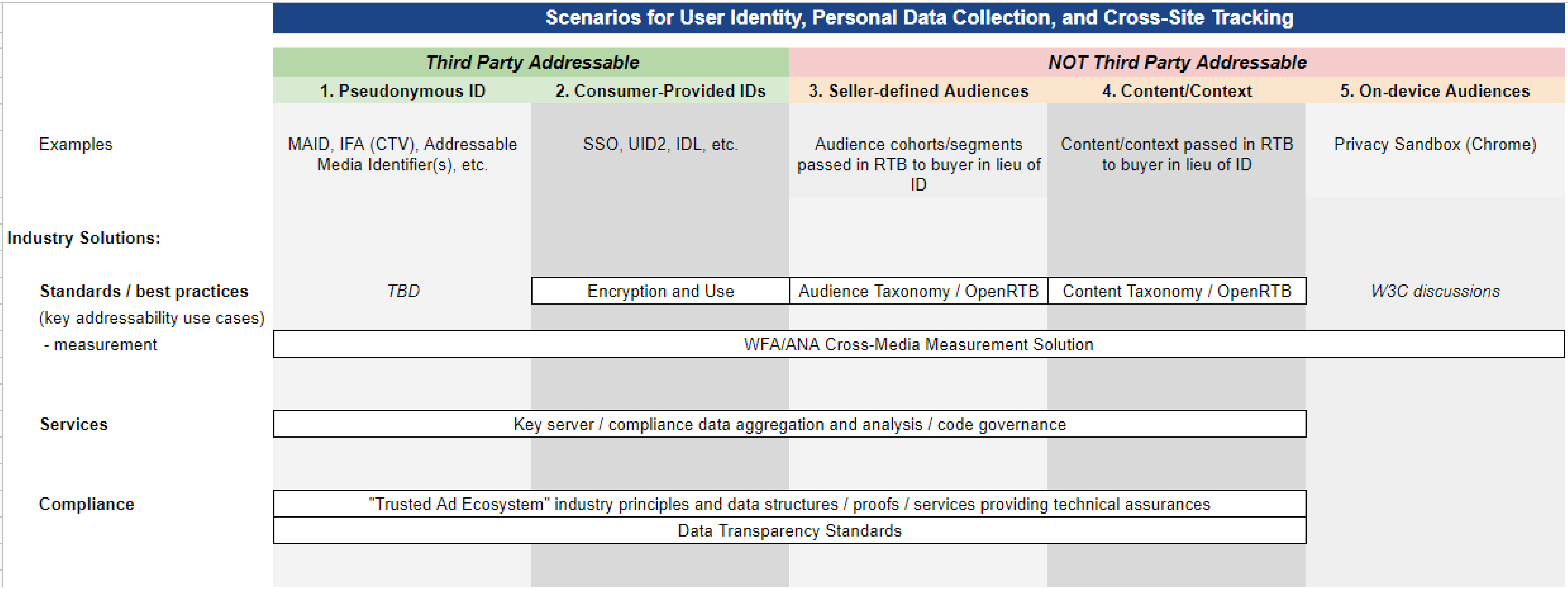
Standardized Taxonomy, Process, and Data Transparency Enables Scale for Sellers/Buyers



- Interests, behaviors, etc. defined by publishers
- Development of "cohorts" (groups)
- Passed within OpenRTB at seller's option (w/out user ID)
- Working in partnership with Prebid.js (code to deploy)
- Audience Taxonomy & Data Transparency Standard are relevant
- Privacy, measurement and brand safety guidance

Pulling This All Together with PRAM Workstreams …

- Aiming for a simple picture conveying how we fit all the pieces together.
- Lots of work left on the policy and tech standards front!



	Scenarios for User Identity, Personal Data Collection, and Cross-Site Tracking				
	Third Party Addressable		*NOT Third Party Addressable*		
	1. Pseudonymous ID	2. Consumer-Provided IDs	3. Seller-defined Audiences	4. Content/Context	5. On-device Audiences
Examples	MAID, IFA (CTV), Addressable Media Identifier(s), etc.	SSO, UID2, IDL, etc.	Audience cohorts/segments passed in RTB to buyer in lieu of ID	Content/context passed in RTB to buyer in lieu of ID	Privacy Sandbox (Chrome)
Industry Solutions:					
Standards / best practices	*TBD*	Encryption and Use	Audience Taxonomy / OpenRTB	Content Taxonomy / OpenRTB	*W3C discussions*
(key addressability use cases)					
- measurement	WFA/ANA Cross-Media Measurement Solution				
Services	Key server / compliance data aggregation and analysis / code governance				
Compliance	"Trusted Ad Ecosystem" industry principles and data structures / proofs / services providing technical assurances				
	Data Transparency Standards				

IAB TECH LAB

Related States of Play

- The latest on the UID2 proposal from The Trade Desk
- An update on the Partnership for Responsible Addressable Media
- W3C update

Unified ID 2.0 …. From The Trade Desk's Web Site

Relevant advertising enables content providers to produce the content we've all come to enjoy, whether it's mobile apps, streaming TV, or web experiences. This value exchange has not always been well understood, communicated, or managed. As the industry moves away from its reliance on the third-party cookie, there's an opportunity to create a new and better approach to identity for the open internet.

The Trade Desk is building on the work of leading industry partners and collaborating across the ecosystem to develop an open source ID framework. Built from hashed and encrypted email addresses, this ID will remain open and ubiquitous while introducing significant upgrades to consumer privacy and transparency. The Unified ID 2.0 initiative will be:

- **Open source and interoperable**: The ID framework will be open source and available for free for everyone.
- **Secured technology:** Emails will be hashed and encrypted to prevent abuse. Regular rotation of decryption keys will help enforce accountability measures.
- **Independently governed**: Participants will agree to a code of conduct as well as regular audits.
- **User transparency and privacy controls**: Consumers will be able to easily view and manage their preferences and opt out at any time.

Roles Being Discussed

1. Open-source code governance
2. Standards / best practices for encryption/use of a consumer-provided, authenticated ID
3. Operation of an encryption key provisioning/management service (as well as salt buckets) for parties to use to work together
4. Standards for what it means to be a “trusted ad ecosystem” participant, along with a compliance program
5. Data transparency standards and services, including potentially operating some/all components of the consumer-facing transparency/consent services

For long-term feasibility, standardized ID solutions must be coupled with relevant global tech standards, policy discussions, related privacy (tech) frameworks and cross-stakeholder industry alignment efforts.

iab.
TECH LAB

Related States of Play

- The latest on the UID2 proposal from The Trade Desk
- An update on the Partnership for Responsible Addressable Media
- W3C update

PRAM Refresher

ANA iab. WFA World Federation of Advertisers 4A's iab. TECH LAB NAI Network Advertising Initiative

The Working Groups …

- **Business Practices** – Will assemble a compendium of priority business use cases (and more TBD later)
- **Privacy, Policy & Legal** – Will advise on areas relevant to developing new standards and privacy principles to safely and effectively meet the use case requirements
- **Technology Standards (Project Rearc)** – Will define standards for addressability solutions that meet the use case requirements and ensure adherence to privacy principles
- **Communication & Education** – Will architect our narrative and provide materials for brands & partners to understand our changing landscape and enable them to efficiently & effectively optimize the use of data during & after these changes take place with standards, principles, processes & solutions

PRAM Business Practices Working Group Update

- **Objective** – Share, discuss, debate and ultimately assemble a compendium of Addressable Media business use cases to form the basis of the principles and solutions created by the Privacy, Policy & Legal and Technology Standards Working Groups.
- **Approach** – 4 Teams with Captains, Co-Captains, Mighty Scribes and 61 participants met for 3 hours 4 times over 8 weeks resulting in 700+ hours of qualified, diverse and passionate experts focused on the task.
  - 10/2 – Drafted 18 priority use cases with a pre-determined template and focused on 7 Key Topic Areas. Each diverse team addressed them in a different order to ensure their expertise and attention was evenly distributed.
  - 10/16 – Continued their efforts resulting in ~30 additional use cases and began refining prior work.
  - 10/30 – Integrated 14 use cases from prior Tech Lab efforts and began deduping, editing and honing all resulting in 54 use cases.
  - 11/13 – 2 new teams aligned 3 owners to each. With fresh eyes, we categorized them, (Planning, Activation, Measurement & Optimization) continued deduping, editing and honing them, and presented them to the entire team to expose more of the group to more of the work.
- **Next Steps**
  - By 12/1 – Reduce the tonnage. Teams are focused on re-organizing 54 use cases to a more manageable list of ~23
  - By 12/31 – Integrate ~30 publisher use cases from prior Tech Lab efforts and work with owners to fill in remaining gaps and make final edits on all
  - By 1/15 – Reassemble, format and be prepared to share with a broader audience to add, enhance & improve the LIVE document

TECH LAB

Related States of Play

- The latest on the UID2 proposal from The Trade Desk
- An update on the Partnership for Responsible Addressable Media
- W3C update

W3C Web Advertising Biz Group Update (Highly Summarized)

TURTLEDOVE and related audience targeting proposal **discussions continue in earnest**

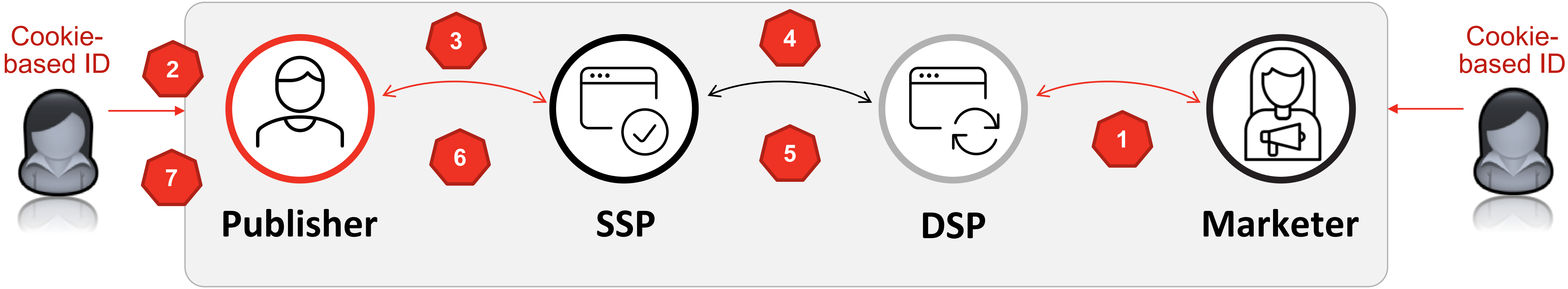
- First there was TURTLEDOVE
- Then there was SPARROW
- Then TERN from AdRoll
- DoveKey from Google Ads Team
- PARRROT from Magnite, now being combined with TERN from AdRoll
- MURRE from AdRoll, PELICAN from Neustar, SPURFOWL from NextRoll, etc.

Key Takeaways … This Is About:

- Where is data and who controls the final auction (browser, 3rd party or publisher)?
- How can data continue to feed machine learning models / decisioning?

How The Auction Works with User IDs – HUGELY simplified

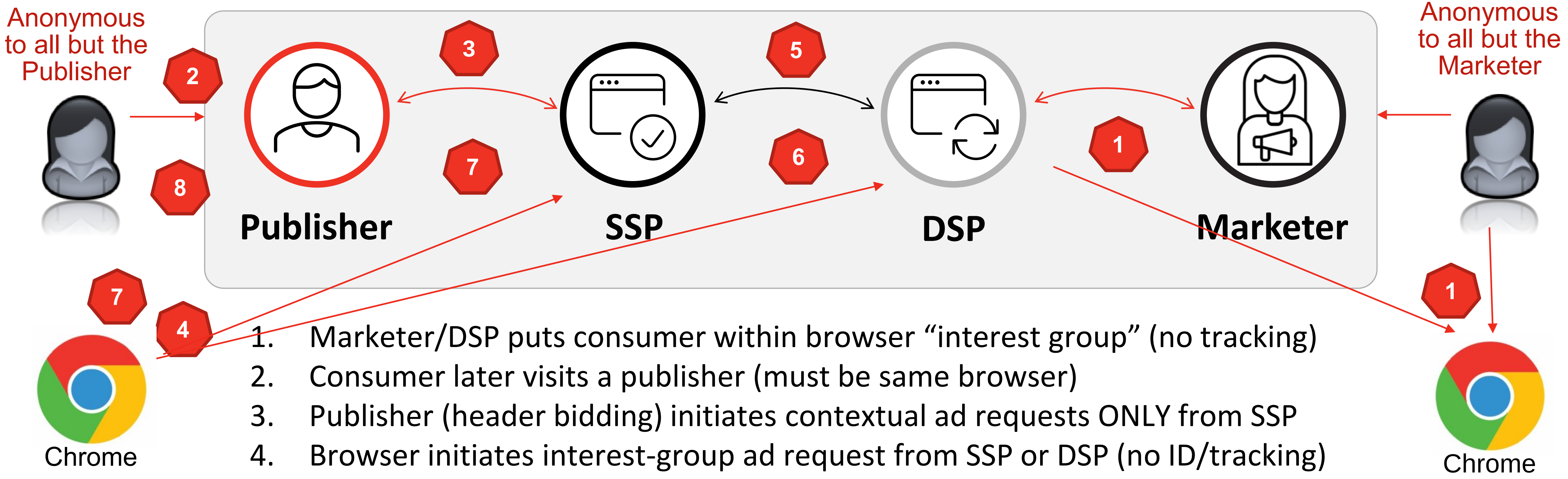
MANY auctions and algorithmic decisioning points



1. Consumer is placed into audience segment for targeting
2. Consumer later visits a publisher
3. Publisher (header bidding) initiates multiple requests for bids from SSP
4. SSP initiates multiple bid requests from DSP
5. DSP returns bid decision and value
6. SSP clears auction on behalf of publisher, in accordance with all sorts of rules
7. Publisher header bidder and ad server clears final auction, and ad is shown
8. **Any/all data flows used within machine learning algorithms**

Audience Targeting – TURTLEDOVE Proposal (by Chrome)

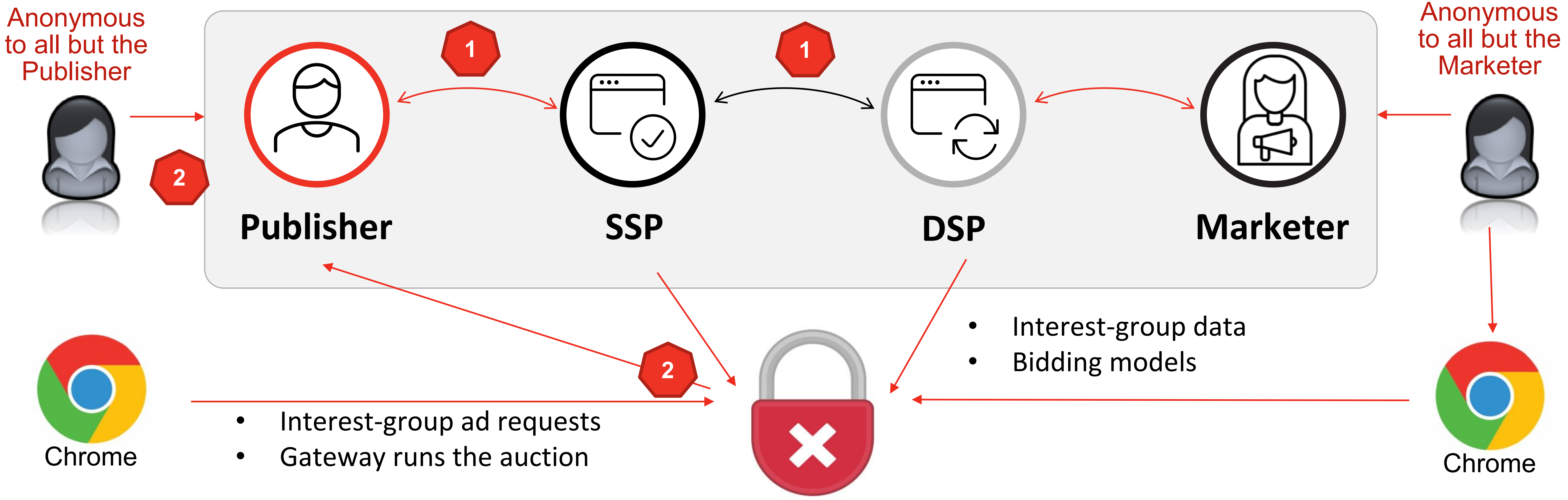
Chrome Browser controls interest data and auction decisions


Anonymous to all but the Publisher
2
8
Publisher
3
7
SSP
5
6
DSP
1
Marketer
Anonymous to all but the Marketer
1
7
4
Chrome
Chrome

1. Marketer/DSP puts consumer within browser “interest group” (no tracking)
2. Consumer later visits a publisher (must be same browser)
3. Publisher (header bidding) initiates contextual ad requests ONLY from SSP
4. Browser initiates interest-group ad request from SSP or DSP (no ID/tracking)
5. SSP initiates multiple bid requests from DSP
6. DSP returns bid decision and value (contextual and interest-group)
7. SSP clears whatever auction it can for Pub, passing back to browser. Browser makes final decision between contextual and interest-group ad.
8. Browser decision subject to final ad server decision, and ad is shown

Audience Targeting – SPARROW Proposal (by Criteo)

Proposes 3rd party “gateway” removing control by Chrome

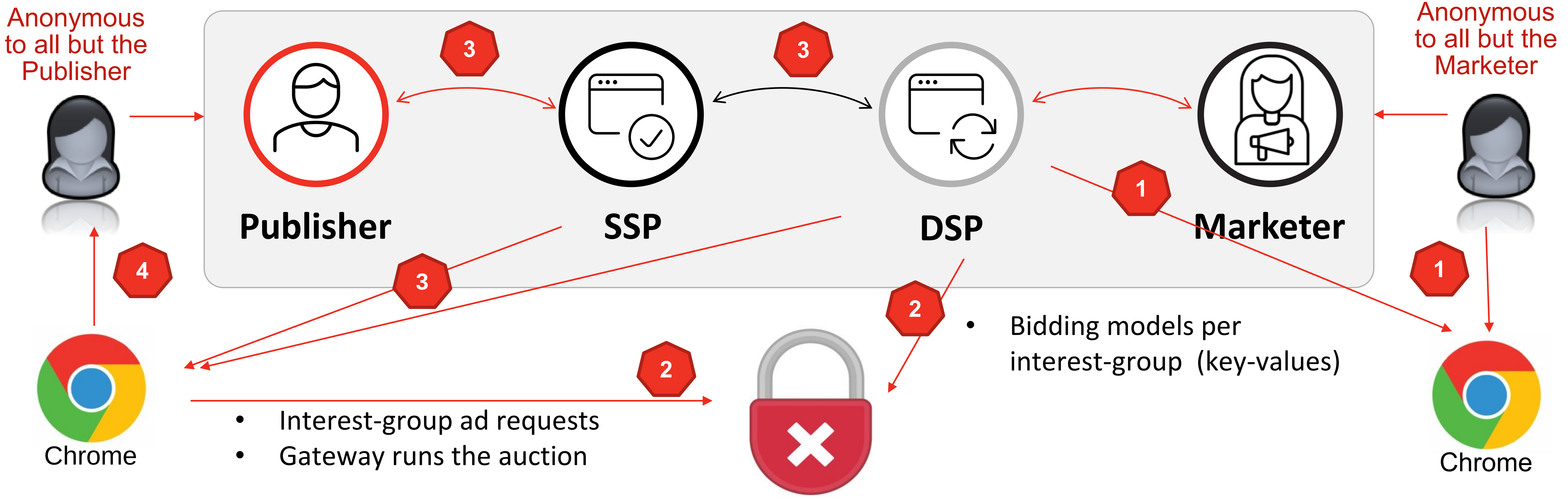

Anonymous to all but the Publisher
2
1
1
Publisher
SSP
DSP
Marketer
Anonymous to all but the Marketer
2
Chrome
Chrome
• Interest-group data
• Bidding models
• Interest-group ad requests
• Gateway runs the auction

Gateway holds interest data & runs the interest-group auctions instead of Chrome

1. Contextual ad flow happens as usual
2. Interest-group ads all flow through Gateway; final decision by ad server

Audience Targeting – DOVEKEY Proposal (by Google Ads)

Gateway data and auction control removed; back within Chrome



Anonymous to all but the Publisher

Anonymous to all but the Marketer

- Bidding models per interest-group (key-values)

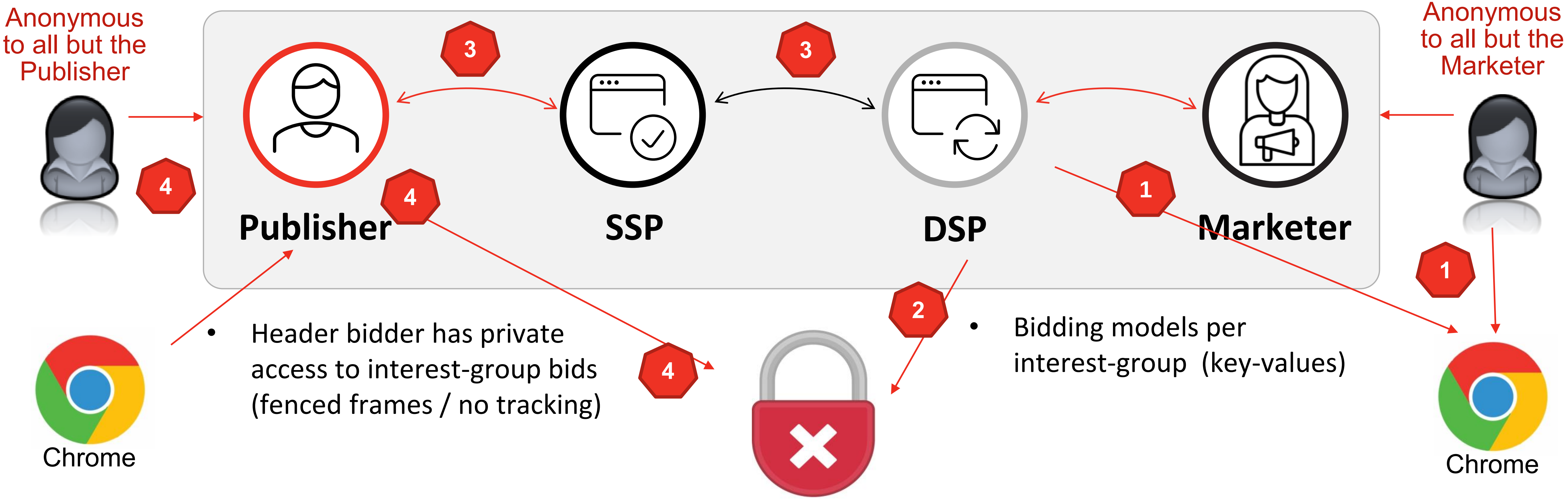
- Interest-group ad requests
- Gateway runs the auction

Gateway becomes a simple “lookup table” for interest-group bids

1. Interest-group data stored back on Chrome
2. Interest-group bids stored in key-value server
3. Contextual ad flow happens as usual, but sent back to Chrome
4. Interest-group ads requests and auction clearing by Chrome

Audience Targeting – PARRROT/TERN Proposal

Interest data within Chrome; auction decisioning within publishers



Anonymous to all but the Publisher
Anonymous to all but the Marketer
3
3
4
4
4
1
1
2
Publisher
SSP
DSP
Marketer
Chrome
Chrome

- Header bidder has private access to interest-group bids (fenced frames / no tracking)

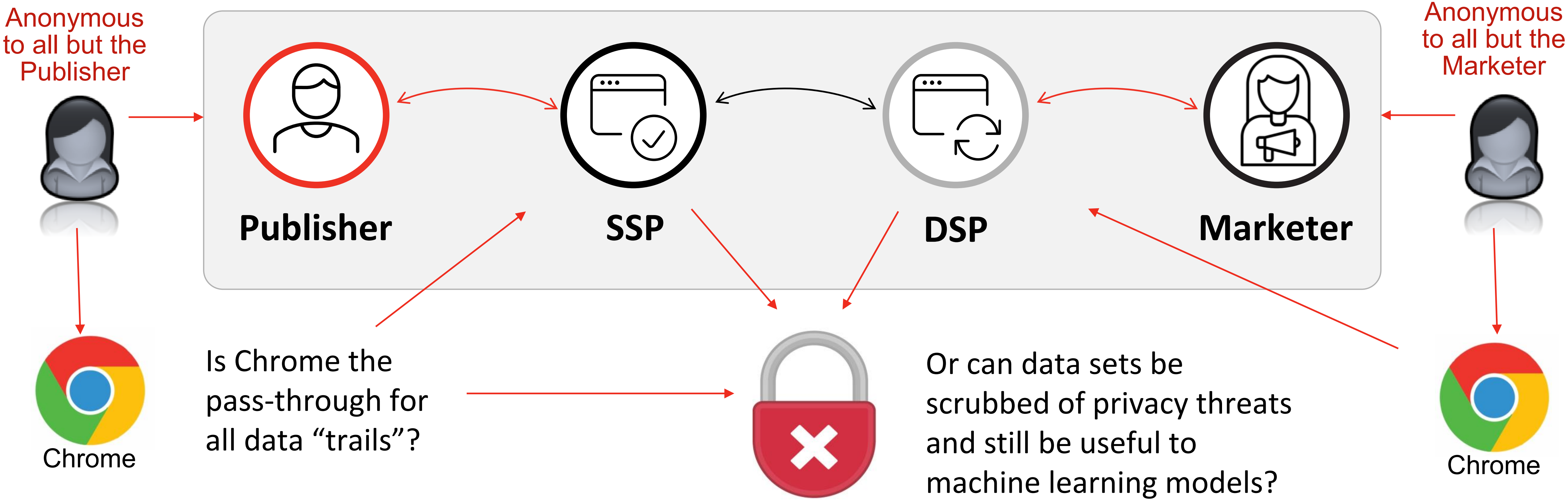
- Bidding models per interest-group (key-values)

Gateway still a simple "lookup table" for interest-group bids

1. Interest-group data stored in Chrome
2. Interest-group bids stored in key-value server
3. Contextual ad flow happens as usual, sent back to publisher header bidder
4. Interest-group ads requests and <u>auction clearing by publisher</u>

Data to Feed ML Models (multiple proposals)

Can data sets feed ML and still be privacy preserving?


Anonymous to all but the Publisher
Publisher
SSP
DSP
Marketer
Anonymous to all but the Marketer
Chrome
Chrome

Is Chrome the pass-through for all data "trails"?

Or can data sets be scrubbed of privacy threats and still be useful to machine learning models?

Machine learning example use cases

- Campaign optimization (clicks, conversions, etc.)
- Delivery optimization (SPO, infrastructure, etc.)
- Security, non-human traffic, fraud, etc.

W3C Privacy Community Group (Highly Summarized)

Meanwhile, browser vendors continue to discuss critical proposals for reducing tracking within the Privacy Community Group

- **First-party Sets** – how to limit tracking across sites owned by same party
- **IsLoggedIn** – how to alert the browser of persistent “logged in” states
- **Storage Partitioning** – how to separate client-side storage of tracking information from different parties
- **Fenced Frames** – how to limit tracking information between embedded documents and embedding page
- **IsKnown** – new proposal for supporting paywalls (counting number of limited visits / views)

Can provide deeper updates within future updates …

iab. TECH LAB

Feedback and/or Questions?

To participate, contact **IAB Australia**

Project Rearc:

An Industry Collaboration to Rearchitect Digital Marketing

iab.

iab. australia

iab. TECH LAB

iab.
australia