Best Practices for User-Enabled Identity Tokens

March 2021

Draft Open for Public Comment Through May 7, 2021

This document has been developed by the Rearc Addressability Working Group, in cooperation with the Partnership for Responsible Addressable Media (PRAM).

With impending disruption to the identifier landscape, Project Rearc is a global call-to-action for stakeholders across the digital supply chain to re-think and re-architect digital marketing to support core industry use cases, while balancing consumer privacy and personalization. *The Rearc Addressability Working Group* is responsible for the evaluation of alternative technical standards and guidelines to drive "privacy by design" advertising, informed by input from the global business and policy dialogue within the Partnership for Responsible Addressable Media. The Addressability Working Group evaluates responsible technology alternatives to today's short-lived addressability mechanisms, and develops the technology foundations for tomorrow's consumer-centric solutions for ad targeting, measurement and optimization, while enhancing consumer transparency and industry accountability.

Rearc Addressability Working Group Roster

The Rearc Addressability Working Group Roster is made up of 295 individuals representing 146 organizations. Full roster details can be viewed here.

About IAB Tech Lab

Established in 2014, the IAB Technology Laboratory (Tech Lab) is a non-profit consortium that engages a member community globally to develop foundational technology and standards that enable growth and trust in the digital media ecosystem. Comprised of digital publishers, ad technology firms, agencies, marketers, and other member companies, IAB Tech Lab focuses on solutions for brand safety and ad fraud; identity, data, and consumer privacy; ad experiences and measurement; and programmatic effectiveness. Its work includes the OpenRTB real-time bidding protocol, ads.txt anti-fraud specification, Open Measurement SDK for viewability and verification, VAST video specification, and Datalabel.org service. Board members/companies are listed at https://iabtechlab.com/about-the-iab-tech-lab/tech-lab-leadership/. For more information, please visit https://iabtechlab.com.

IAB Tech Lab Contacts
Benjamin Dick
Sr. Director of Product – Identity & Data

Jordan Mitchell
Senior Vice President, Privacy, Identity & Data

Feedback on this RFC can be submitted to addressability@iabtechlab.com

Goal/Scope

This document establishes guidelines for the encryption and use of **user-provided IDs** - notably email addresses and phone numbers - in scenarios when online publishers or marketers offer personalized content or services tied to a user-provided email or phone number. It focuses on the minimization of privacy threats to consumers when identity tokens are generated from these values and passed to partners to support addressability use cases. This document is intended to be agnostic to proprietary system designs, and leverages existing industry feedback on foundational addressability principles, design constraints and requirements for the supply-chain.

Relevant Definitions

Below are definitions of terms and concepts used within this document. These are intended to provide specificity, convey nuance, and establish consistency in the language used below, however are not entirely based on broad industry consensus.

- **First Parties:** Producers of digital content on both the “buy” and “sell” sides of the ecosystem. This includes marketers and publishers that actively work to develop experiences for users on their domains and apps.
- **Personal Data:** Any information directly or indirectly related to an identified or identifiable natural person including Personally Identifiable Information, Pseudonymous or Pseudonymized information, and unique tokens
- **Personally Identifiable Information**: Information that directly identifies or describes a specific person’s offline identity including, but not limited to, a person’s name, physical residential or mailing address, email address, phone number, government issued identifiers, or customer identifiers.
- **Pseudonymous**: The processing of personal data in such a way that the data can no longer be directly attributed to a specific user’s Personally Identifiable Information without the use of additional information that is maintained separately.
- **Token or Tokenize**: A pseudonymized, unique identifier that does not allow an entity to infer, discover, or otherwise identify the individual.

Proposed Best Practices

The following are a set of proposed best practices intended to outline clear expectations related to four components of user provided ID acquisition and minting of tokens: 1) consumer transparency and control, 2) data security, 3) use cases that are excluded, and 4) regional expectations around data access and use. These best practices reflect

consensus within IAB Tech Lab Rearc Working Groups around addressability principles, constraints and supply chain requirements (see additional detail in appendix).

1. **First-party Obligations for Transparency and Control**

   A First Party that collects personal data, constructs it into a Pseudonymous Token (i.e., through hashing, encryption, etc.), and shares it with third parties for targeted advertising (such processes collectively referred to as "Addressability") must provide the user with transparency and control subject to the relevant legal requirements in the applicable jurisdiction.

   a. **Transparency** reflects the first party's choices about the vendors they use to support their campaigns and monetization, as well as the data uses they allow of those vendors.
   b. **Control** is a functional mechanism to allow a user to further restrict data processing the first party discloses as a part of their transparency expectations.

2. **Security**

   Below are expectations to enforce data security and privacy when minting tokens:

   a. Personally Identifiable Information must be pseudonymized by the First Party, or a vendor under direct contract with them, before sharing with third parties for Addressability use cases.
   b. Tokens should not be directly linkable to Personally Identifiable Information unless the user was given notice of such "re-identification" by the First Party and, if required by law, the user has given legal consent. Linking of pseudonymized data to PII shall only be done by the First Party or a vendor under direct contract with a first party.
   c. The principle of least privilege should be applied for all levels of access to personal data.
   d. Role based access controls should be in place to ensure appropriate segregation of duties to protect against re-identification, when and where it should not occur.
   e. Raw personally identifiable information must be stored in a separate environment from Tokens.
   f. Data sets should not include less than a specified minimum threshold of individuals to reduce risk of re-identification when and where it should not occur. This threshold needs to be based on forthcoming industry policy consensus. See IAB Tech Lab's "Taxonomy and Data Transparency

Standards to Support Seller-defined Audience and Context Signaling" primer for an overview of key considerations when determining this threshold.

g. Where applicable, prohibit the use of cross-temporal queries that may be used to triangulate individuals for re-identification, when and where it should not occur.
h. Auditing and logging of security events must be enabled for all local, network, cloud and remote access connections.
i. User Tokens generated from personal data must be sufficiently encrypted and hashed such that it cannot be reverse engineered back to the original personal data.
j. Only First Parties, or a vendor under contract with them directly, may perform the encryption or hashing of consumer personal data for subsequent use by third parties.
k. To the extent possible, the encryption and/or hashing function should be done within the environment of the first party, to limit the transfer of personal data.
l. Encryption methods used in transit and at rest must align with industry standard encryption levels or better.
m. Sufficient technical mechanisms must also be in place to greatly limit the ability for the vendor ecosystem to maintain mapping tables that allow for unauthorized access to Tokens.
n. Data Retention schedules must be defined, observed and minimized, subject to the relevant legal requirements in the jurisdiction.
o. Data localization must be observed subject to the applicable legal requirements and applicable jurisdiction.

3. **Exclusions**

No consumer personal data may be constructed into a Token or passed to third-party vendors in cases where the consumer is known to be a child.

4. **Access and Use**

No third-party may access or utilize a Token (generated from personal data) for any reason unless they comply with all applicable regional laws, consumer preferences, codes of conduct, and these rules.

Appendix

Established Principles For Addressability

Over the past year, IAB Tech Lab's Rearc working groups, with the help of external policy guidance, have undergone a systematic review of the business and technical disruption across the addressability landscape. This included an evaluation of the industry forces driving industry conversations and the underlying rationale informing their positions, proposals, and technology designs. While it's clear that the primary actors influencing the conversation - privacy engineers within browser and OS platforms, consumer privacy advocates, lawmakers, and digital media trade groups (incl. IAB Tech Lab) - are all doing so on the basis of improving consumer privacy and data protection, there are material differences in the core set of expectations and values these groups want to see reflected in a reimagined digital media supply chain.

Re-architecting open standards around consumer privacy and data protection is an important opportunity for the industry to deepen trust in the digital media supply chain and educate consumers on how it functions. It's also a powerful argument for structural change that provides a platform to re-litigate the economic values and consumer participation we want to enable within the open web, which over the past twenty years has been a transformative force within our societies, politics and economics. IAB Tech Lab Rearc working groups have enumerated the following positions, which have informed our work to date by acting as constraints / guardrails on our evaluation of technology approaches:

1. **Advertisers and publishers should be able to make choices about which companies they use to run campaigns or monetize inventory, and those choices should be clear to consumers and allow consumers to further restrict them.** Transparency is a function of 1st party choices about which ad technologies to use. When consumers are provided this transparency, they can make further limitations on what can be done with data.

2. **Consumers can exercise meaningful, informed control over data uses via first parties**
    a. At a minimum these controls need to conform to the requisite consumer transparency and control features defined by local law and policy interpretation.
    b. In markets where there are no explicit consumer choice or transparency expectations at reasonable levels of granularity - with respect to the first or

third parties that are accessing data - the minimum benchmark should be FIPPs (Fair Information Practice Principles).

3. **Consumers deserve technical safeguards that hold industry parties accountable to their preferences, and which allows the actions of 1st and 3rd parties to be reviewable and actionable by consumers.** Commercial addressability system designs leveraging user provided IDs should consider integration with IAB Tech Lab's Accountability Platform, which establishes meaningful tools to evaluate the extent to which organizations are abiding by consumer preferences.

4. **In order to consistently respect consumers' preferences across the supply chain, it is essential for addressability systems to establish secure, persistent approaches to capturing and communicating consumer privacy preferences between supply chain intermediaries.** This is because of known supply-chain security gaps (OpenRTB and other ad request fields are fungible as calls hop from one party to the next), which could jeopardize the integrity of consumer privacy signals that might be attached to an identifier and propagated to partners. Organizations that operate in the digital media supply chain should consider adoption of cryptographic signal signing techniques like those Tech Lab is developing in its Programmatic Security Working group as well as adopting the Accountability Platform design currently in public comment.