A Proposal for Enhanced Accountability to Consumer Privacy within the Digital Marketing Industry

Request for Collaboration to Improve Consumer Trust and Experience with Technology Standards for Consumer Privacy

Table of Contents

Executive Summary 2
Objectives and Intentions 3
Who is Behind This Proposal? 3
About IAB Tech Lab 3
About Network Advertising Initiative (NAI) 3
Our Objectives 4
Our Process, Agenda and Scope 5
Proposed Methods for Enhanced Accountability 6
An Encrypted, Revocable Token 6
Joint Accountability System 7
Controlled Container for Ad Delivery 8
Proposed Next Steps 8
Deeper Use Case Evaluation and Feasibility Analysis 9
Consumer Privacy Use Cases 9
Industry Transactional/Operational Use Cases 10
Organizational, Governance and Enforceability Considerations 10

Executive Summary

The Digital Marketing industry recognizes that improved consumer experience and trust is essential to the growth of our industry, growth of the web as a public benefit, and to assuring a vibrant, inclusive, open, global and healthy internet. We recognize our responsibility to contribute towards a more secure, trusted user experience that respects consumer privacy (as a fundamental consumer right). We also recognize the challenge of doing so while supporting the economic viability of a diverse publisher landscape, with consumption models that support quality content and open access for consumers.

The current operational and political environments, combined with the constraints inherent within established internet protocols, implies that the digital marketing industry and browser community must collaborate if we are to meaningfully improve the consumer experience and consistently honor consumer privacy rights and preferences. Our industry's trade associations, which lead standards and best practices for our industry, have discussed programs and support for solving these issues responsibly that we would like to present for discussion, collaboration and joint problem-solving.

With a better consumer experience and the preservation of the global open internet as our joint objective and common ground, we ask for browsers' cooperation on a technology-based solution and standards that bind:

- consumer privacy preferences, and ...
- regulatory settings (consent strings, timestamps, permissions flags, etc.), to a …
- restricted identifier(s), in a way that is ...
- verifiable and non-forgeable.

We understand that participants within the browser and privacy community may not trust our industry to consistently respect consumers' privacy rights and preferences. However, we cannot do so without mechanisms to reliably persist and communicate those preferences, and we understand that trust is necessary for collaboration and progress. To enhance trust in our industry, and facilitate good faith cooperation around this effort, we are prepared to:

- Rigorously honor and propagate the privacy preferences attached directly by consumers to a standardized mechanism in the context of their interactions with trusted brands/publishers, as a condition of access to the standardized token.
- Introduce technical mechanisms for building enhanced accountability to consumer privacy and security into the fabric of our ecosystem, systematically ensuring ongoing responsible and compliant use of identifiers and data in strict accordance with the consumer preferences attached to the standardized token.
- Jointly govern the use of this mechanism with the browser and privacy community, and continue to collaborate and iterate around the rules (and features) of its use.

Collaboration around a better consumer experience, and strict adherence to consumer privacy rights and preferences, is the most favorable route for all involved (especially consumers). The relationship between the advertising industry and the browsers (and operating systems) is at a unique point, at is pertains to consumer data collection, security and privacy. Our ability to willingly move forward in cooperation, and discontinue the arms race between “browser tech and ad tech”, is clearly the right choice for consumers. Conversely, our failure to work together will very clearly result in a less secure, less trusted internet experience for consumers, with their privacy rights and preferences unable to be recognized or respected, along with other unfavorable, unintended consequences.

Objectives and Intentions

Who is Behind This Proposal?

This proposal represents the perspective of IAB Technology Laboratory and Network Advertising Initiative, as well as its many members that drive the digital marketing industry globally. We believe additional perspective is necessary, especially with those outside our industry, to achieve the best outcomes.

About IAB Tech Lab

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 develops solutions for brand safety and ad fraud; identity, data, and consumer privacy; ad experiences and measurement; and programmatic efficiency and 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, DigiTrust identity service, and in partnership with IAB Europe the Transparency & Consent Framework.

About Network Advertising Initiative (NAI)

Founded in 2000, the Network Advertising Initiative (NAI) is the leading self-regulatory association comprised exclusively of third-party digital advertising companies. As a non-profit organization, the NAI promotes the health of the online ecosystem by maintaining and enforcing high standards for data collection and use for advertising online and in mobile. Our organization also educates and empowers consumers to make meaningful choices about their experience with online advertising through an easy-to-use opt-out mechanism.

Our Objectives

Our objectives are **more trusted, secure and faster consumer experiences**, with **100% consumer transparency and control over data collection practices and privacy preferences.** We believe a better consumer experience can be achieved **while supporting the economic viability of trusted first-party publishers and brands** that rely on third-party vendors.

We care about consumer privacy, believe that access to quality online content and services is a fundamental human right, and that paid access is a privilege of some, but not all. For those consumers who agree to ad supported (rather than paid) digital services, our objectives are to ensure trusted ad supported digital services:

- Reinforce and uphold the direct relationships between consumers and the publishers/brands they trust,
- Provide consumers with simple, durable and effective privacy controls,
- Adequately and consistently record, respect and propagate consumer privacy preferences,
- Enable innovation around new consumer features that offer better control over their ad experiences, and
- Require significantly fewer third-party trackers/domains on every page, *while also*
- Allowing publishers to personalize, measure, frequency cap, and attribute ads, etc. (via the use of third-party vendors, if they choose to), and
- Allowing advertisers to deliver the best ad experiences.

We would like to end the current arms race between browser tech and ad tech, and forge cooperation around consumer identifiers, privacy, data, security and accountability. Our concern is this arms race is causing a level of misdirected innovation with unintended results:

- Multiple, redundant, and continual interruptions to the user experience in order to establish consent and/or a sign-on -- non-standardized and inconsistently applied.
- Inability to adequately record and honor consumer consent (or any other consumer rights or preferences), resulting in fragmented, ephemeral and/or inconsistently respected consumer preference signals.
- Inability to innovate around new consumer features that offer privacy-safe, personalized control over ad experiences (such as ad suppression, like/dislike, etc.)
- Further growth of detrimental content models (fake news, fraud, bots, etc.), due to the deteriorating economics of high-quality content production.
- Severe functional and economic constraints to the ongoing development of a vibrant, diversified ecosystem of high-quality publishers, content and services.
- Continued pockets of proprietary innovation around opaque audience recognition techniques, including probabilistic IDs, fingerprinting, carrier-assigned IDs, email hashes, and further bloated ID sync techniques.

Our Process, Agenda and Scope

In recognition that participants within the browser and privacy community may not trust our industry, and that trust is necessary for collaboration, we brought together leading product development and privacy influencers within our industry to discuss how we enhance accountability, and rebuild trust.

The agenda was to brainstorm potential technical mechanisms for building enhanced accountability to consumer privacy into the fabric of our ecosystem, and ascertaining compliant use of a standardized user token. In doing so, we aim to:

- Improve the consumer experience by supplanting thousands of proprietary cookie-based identifiers and “trackers” with a better mechanism and consumer controls, which offer faster experiences and better security.
- Enable consumers with simple, durable and effective privacy controls, with technical systems and assurances (to accompany our commitment) that they will be respected.
- Be better stewards of consumer privacy. Improve privacy compliance for our industry, and establish shared liability/responsibility.
- Alleviate concerns from regulators and privacy advocates.
- Establish credibility with the browsers and operating systems, and end the browser-tech / ad-tech arms race.

The brainstorming session was, by design, agnostic to region and the ongoing evolution of policy across regions, the technical mechanisms available for identifiers, the specific privacy preferences afforded or required by law, etc. Our industry understands that the importance of collaboration around accountability now transcends all other considerations of technology and policy, which will most certainly evolve.

As such, we chose to specifically exclude the following considerations from our initial scope, not because they are unimportant but rather because they are too important to consider without additional perspective (outside our industry) at the table:

- Privacy policy, consumer rights, and related regional considerations / evolutions
- Proprietary ownership of any technology or standards considered/proposed
- Device considerations
- Governance
- Legal enforceability
- Consumer privacy features and settings, and related UX/UI

Proposed Methods for Enhanced Accountability

We propose several technical mechanisms for building enhanced accountability to consumer privacy into the fabric of our ecosystem, and ascertaining privacy-compliant use of a standardized identifier mechanism.

Each of the three mechanisms relies on a framework for producing interfaces that facilitates transparency -- between consumers, publishers, brands and third parties -- about data processing purposes and provides choice over which purposes and vendors are allowed. There can be no consumer-centric approach without offering consumers a simple, clear, standardized set of choices, which are then recorded within a standardized connection to the ecosystem delivering ad-supported content and services. The framework to power interfaces could be based on the IAB Europe / Tech Lab Transparency and Consent Framework (TCF) version 2.0. A TCF modified for global use and the additional enforcement mechanisms provided below, while still supporting regional evolutions, creates the foundation for serious discussion.

The TCF as currently designed is used to broadcast standardized signals about what consumers have seen and the preferences they've expressed for a given publisher's interface. We propose to add enhanced enforcement in a new flavor of TCF to hold vendors to processing allowed by the transparency and consent signals created by consumers' choices. We recommend three methods for achieving that enforcement:

1. An encrypted, revocable token, tied to a
2. Joint accountability system, with a
3. Controlled container for ad delivery.

An Encrypted, Revocable Token

We propose **a standardized, persistent token that contains a unique identifier and privacy preferences, with access to the token conditioned upon respect of those privacy preferences**.

A standardized user token in browser environments would eliminate the need for "cookie syncing" across 1000s of proprietary cookies, a process that noticeably impacts consumer experience via increased page load times, and introduces 100s of third parties onto sites where they do not need to be present. This standardized token would not need to log or store any data itself outside of consumer preference signals, and would be designed solely as a persistent mechanism to store, communicate, and adhere to consumer preferences. Consumers convey their privacy preferences, which are stored within this shared token, and the digital marketing industry must propagate, respect and jointly enforce those preferences in return for the privilege of access to an associated identifier (or identifiers) for any purpose.

While existing industry self-regulation offers levels of accountability and oversight into ad tech vendor behavior, we believe real-time protections would enhance trust in our ecosystem. We propose a public/private key encryption mechanism to verify and regulate access to the token, and mitigate the possibility of forged identifiers or preferences. Participants within the "joint accountability system" (see below) would have access to decryption keys, in return for agreeing to a set of rules (including not to generate or utilize unapproved consumer identifiers) and the keys could be revoked under certain conditions of non-compliance (specificity of which is TBD).

For clarity, there is no assumption of a "new global identifier" to be provided by browsers; we are simply suggesting the availability of an identifier or identifiers, with encryption to ensure access only to responsible companies, subject to consumer preferences. The idea is that without access to the token, companies would not have access to any consumer identifier and therefore be unable to collect, process, track, share, sell or buy personal data, nor be in a position to provide basic analytics, measurement, attribution, etc. This provides economic incentives for the ecosystem to comply with expected behaviors and regulations.

Joint Accountability System

The linchpin of our proposal is **enhanced accountability at the technology/system level**, in addition to policy-based mechanisms (self-regulation), legislation, etc. Building in accountability at the system level enables malicious or erroneous non-compliance activity to be surfaced and rectified quickly.

Our proposed approach would be designed to emulate income tax reporting and accountability systems in place globally, which rely on multiple sources of reporting and a centralized system to match/verify the data and look for outlier behavior. Within the US, for instance, the IRS requires companies to file reports (W-2s, 1099s and the like) for the individuals they pay, and for individuals to separately file tax returns which report their income. This allows IRS systems to review both sets of reporting to easily find discrepancies. In addition, tax return filers are also reviewed against the entire data set to look for obvious inconsistencies -- compared to either previous returns for the same person, or to all returns for those within the same location, demographic, income types, life-stage, etc.

This approach requires an ongoing understanding of specific consumer privacy preferences (and what compliance vs. non-compliance means exactly) as well as the transactional and operational processing of consumer data that takes place within our industry. IAB Tech Lab already stewards the standards for many of these use cases, for which the companies spearheading the development of this proposal are all intimately familiar and involved.

The proposal is that all participants in the Joint Accountability System, as a condition of access to the shared token, regularly contribute to a central data store a sample of their logs from all activities involving the shared token and/or any personal data. An example of these activities

include server to server bid requests, bid responses, data collection events, data transfers, etc. If a “blood sample” of n% from each company were collected every day, it would be entirely feasible for a centralized processing system to surface discrepancies. Further, the centralized system could surface outlier behavior that prompts questions or an audit -- such as, “Company X is bidding 3x the industry average (all other factors equal) for a set of consumers that have opted out of tracking entirely”.

The centralized system could also introduce classic “honey pot” scenarios, purposely generating specific tokens and consumer preference data sets so that vendors caught “with their hands in the honey pot” could be excluded from participation via agreed-upon enforcement mechanisms.

An added benefit of such a system would be centralized transparency to all the companies that are transacting and/or operating with the consumer token, and what exactly they’re doing. This enables consumers to make privacy requests, and for the industry to meet those requests more easily, quickly and accurately.

Controlled Container for Ad Delivery

Lastly, we recognize the need to tightly control the execution of client-side code in order to limit security, performance and tracking concerns, particularly unbridled use of third party javascript on a given page load. We propose the **introduction of a standardized, controlled container for ad delivery** when an ad relies on advertiser controlled javascript for rendering. We believe AMP Ads to be an example of a safe ad container in the market today. Where iframes have failed to inhibit unwanted and unexpected intrusion from third-party scripts, AMP Ads is expressly designed with the ads and the ad tech ecosystem in mind. It offers a way to limit the execution of scripts and defines structured methods for asking for data. The best example is the API for requesting viewability information about an ad. AMP Ads could be enhanced to offer some control over access to a restricted identifier(s). If not AMP Ads then something like it.

Proposed Next Steps

Under no circumstances is this proposal meant to convey completeness in design, a premature conclusion of feasibility, inflexibility or pride of authorship. Rather, our intention is simply to convey a good faith willingness to collaborate further with the browser and privacy community. In that collaboration, we would be pleased to delve further into the critical details below, all of which we feel are necessary to establish trust and consider feasibility.

Deeper Use Case Evaluation and Feasibility Analysis

An enhanced accountability system is only as strong as its weakest component, and our intentions are indeed to quickly surface companies in our ecosystem that are either maliciously or erroneously non-compliant.

Therefore, a critical next step would be to enumerate both potential consumer privacy use cases (what privacy preferences may be offered by and/or required of our industry, and what does compliant vs. non-compliant mean) and all the ways in which our industry processes / operationalizes consumer identifiers and data today. **For each of the privacy use cases, our intentions would be to ascertain the design of automated outputs within a joint accountability system that ascertain compliance and surface non-compliance.**

Consumer Privacy Use Cases

Since the specific definitions and interpretations of consumer privacy law (and related obligations of our industry) are still evolving regionally, we explicitly removed that from the scope of this document and related considerations. Instead, for the purposes of deeply evaluating the feasibility of a joint accountability system, we would propose to simply focus on consumer privacy features that our industry may need to prepare for, based on current and/or potential regulation.

For example, it's not unreasonable to consider one or more of the following consumer privacy use cases to be considered as potential compliance requirements for our industry at some point, within one or more regions globally:

- The ability for a user to understand who is collecting what data about them, and how it's being used, processed, shared, bought, sold, etc., and for what purpose.
- The ability for a user to either opt in or opt out, either entirely (for any purpose) or in part (specific to a company and/or purpose, such as measurement or personalized advertising).
- The ability for a user to make data deletion, addition or edit requests.
- The ability for a user to change the identifier or identifiers for their device.

A joint accountability system, centered around a standardized user token coupled to consumer privacy preferences, enables consumers to make privacy requests, and for the industry to meet those requests more easily, quickly and accurately.

NOTE: The privacy regulation situation globally is not only complex and regionalized, but also politically charged and highly evolutionary. Our efforts as a technical standards organization, as conveyed in this document, are solely to consider technical mechanisms and systems for enhanced accountability and trust globally, at any given policy specification, region and state of evolution. We respectfully leave it to other stakeholder groups to set privacy policies appropriate to their regions.

Industry Transactional/Operational Use Cases

Consumer identifiers and data are processed today on a highly fragmented B2C and B2B basis. Ideally, we would introduce enhanced accountability measures with the least amount of impedance to existing systems and processes, thereby facilitating broad and rapid adoption and therefore a virtuous cycle of consumer data privacy, security and innovation.

Fortunately, the participants in this broad effort to improve accountability and trust are intimately familiar with all the ways in which consumer identifiers and data are utilized today, and the system/log files generated as a result. For the purposes of evaluating the feasibility of a joint accountability system, we would consider each consumer privacy use case individually, and consider standardized system-level outputs that ascertain compliance (and surface non-compliance) within each transactional/operational use case. Those use cases may include, but are not limited to:

- An HTTP or HTTPS request and response
- An RTB bid request and response
- Page, site and app-level data collection events
- Consumer segmentation
- Personalization events (delivering personalized content and adverts)
- Advertisement verification events (fraud, viewability, attribution, etc.)
- Server to server data transfers (all sharing, buying, selling of consumer data)
- Internal processing and refinement, including the use of Artificial Intelligence
- Identifier resolution and/or cross-device inferences

The hypothesis is that every one of these events produces evidence of itself via system logs, which may be sampled and evaluated for non-compliance on an automated, ongoing basis.

Organizational, Governance and Enforceability Considerations

We believe that the enhanced accountability described in this proposal enhances privacy protections for consumers, compels the industry to hold themselves to a high standard of transparency and respect for consumer data, and benefits publishers who rely on advertising to provide a wide array of content to consumers without charge. However, we recognize that the commitments we make here are only as good as the governance and enforceability mechanisms we put in place to verify responsible data practices. Our industry will need to be collaborative, flexible, and adaptable as we work together on governance and enforceability; and we are committed to building a strong program that utilizes and builds on existing mechanisms, existing and newly created technology, and organizational governance structures that include all players in the marketplace. Initially, we will need to consider the following questions:

- Would a shared token be owned or controlled by a certain entity or entities? How would its evolution be governed for optimal trust across all stakeholder groups?

- What entity(s) or organization(s) would run the proposed joint accountability system? How would this be governed?
- Would the entity(s) or organization(s) be in a position to legally enforce compliance on a global basis? How exactly?

While these questions are beyond the scope of this initial exercise, industry participants stand ready to collaborate with key constituencies to create an effective governance and enforceability program. If we're able to draw in additional perspective from outside our industry, and jointly collaborate on feasibility analysis, we believe the next step would be the system design where we collaborate on appropriate organizational design.