WILMERHALE

MEMORANDUM

+1 202 247 2328
+1 202 663 6363
monique.chettiar@wilmerhale.com

Date March 8, 2018

To ESPC Membership

From Reed Freeman
Monique J. Chettiar

Re **IAB Tech Lab's GDPR / ePrivacy Technology Town Hall on February 21, 2018: Transparency and Consent (Notes)**

1. European Regulatory Challenges

What is an IIP?

- Information related to an identified or identifiable natural person
- Identifiers, such as a name, number, location, online ID, or one or more factors specific to a natural person
- IP address, cookie ID, RFID tag, especially when combined with profiles

Consent:

- Informed, specific, freely given
- Clear affirmative act
- Demonstratable

Legitimate Interest:

- Only if data subject's interests & fundamental rights are not overriding
- Reasonable expectations are taken into account

Others:

- Contract
- Legal Obligation
- Vital Interest
- Public Interest

Transparency:
Who's collecting data?
What are they doing with it?
How long do they hold onto it?

Where can I go with questions or to request copy/delete it?
Territorial Scope:

- Applies to companies established in the EU/EEA
- Applies to certain companies established outside the EU/EEA, if
  - They offer goods or services in the EU/EEA, or
  - They monitor the behavior of natural persons in the EU/EEA

*Entered into force May 25, 2016
*Applicable May 25, 2018

E-Privacy**:**
Storing or accessing information on a device generally requires consent

- Already law (Directive)
- Regulation being passed now

Collection of data over the internet generally requires consent (to what extent and how to collect is being debated).

Processing of personal data already collected requires a GDPR legal basis, e.g. consent or legitimate interest.

Common Questions:
Am I a Controller or Processor? Do I need consent? What else do I need to do?

- Controller vs. Processor
- Legal basis or processing
- Proper consent (where necessary)

Determine Classification of Controller vs Processor

- Data mapping/inventory
- Determine classification
- Legal basis of processing
- Integrate the framework to handle transparency and consent

It's not all about Consent:

- Under GDPR, consent is only one of six "legal grounds" for processing personal data, and therefore not always needed
- For the purposes of access and storage of information on devices ePrivacy Directive consent requirements currently apply
- The Open Framework is designed to be flexible and accommodate different publisher and vendor needs centering on transparency, control and choice

Current Challenges:

- Data leakage
- Lack of Control and Transparency over partners and demand sources on page (and their partners)
- No single privacy policy
- ePrivacy
- GDPR requirements
- Continued monetization

Closed Ecosystem

Benefits:

- Control data leakage?
- Single privacy policy?
- Easier consent?
- Easier GDPR compliance?

Challenges:

- Control of data and reporting
- Control of third party partners
- Control of demand

Standard Framework:

- **Transparency for Consumers and Publishers** into partners that help monetize sites and apps

- **Control for Publishers** over partners operating on sites and apps and processing their users' data

- **Control for Consumers** over how their personal data is used and by which partners

- **Consent** and **Legitimate Interests** as a potential legal basis

- **Standardization** allowing publishers and partners to operate and communicate efficiently using a single, open source standard

- **Flexibility** for publishers and demand sources to build or work with various consent management providers

- **Minimize Disruption** of the Internet, benefiting consumers, publishers & supporting companies

Common FAQ' / IAB Europe's Answerss:

Q: Do Website operators have to facilitate transparency/consent for **all** vendors on vendor list?

> **A**: No—Website operators control which vendors they want to work with. They pick vendors to sport and users can further choose among vendors and purposes.

Q: Does the framework only support global (web-wide) consent?

> **A**: No—Framework supports service (site-specific), group (multiple controlled sites) and global (web-wide) transparency/consent.

Q: Does the framework support different purposes for different vendors?

> **A**: Current iteration supports control over vendors and over purposes but not different purposes for different vendors. Why? Per technical teams, payload is too large. Technical teams are re-visiting and spec-ing out a solution.

Q: Who will maintain prices of framework that need to be centrally managed (vendor list, disclosures and updates; policy; consent storage/dissemination reference protocol)?

> **A**: TBD. Stakeholders are determining the best course of governance.

Transparency and Consent Framework Technology

1. All vendors will need to register through a portal.

2. Industry Vendor List.
   - A centralized, dynamic list of vendors, their purposes, their privacy policy URL, *et al.*
   - Versioned to allow for audit trail
   - Publishers will use the vendor list as basis for disclosure and consent requests
   - Both vendors and publishers will need to adhere to baseline principles and minimum standards

Providing Transparency and Requesting Consent.

- A JavaScript library/API when enables publishers to customize the experience of providing transparency disclosures and requesting consent
  - Abstracts the complexities of consent checking and storage
  - Implements standardized minimum disclosure language
  - Ensures the vendor list and disclosure language stays updated to latest version

  - Integrates with consent identification mechanism
  - Makes approved vendor and consent data available for downstream usage via daisy chain

Storing Vendor and Consent Signals.

- Approved Vendor and Consent storage requires two-mechanisms:
  - a user identification method; and
  - a persistence method.
- Identification method
  - The identification needed for global consent to be made possible could be done via multiple mechanisms (e.g., id syncing).
  - Implementation to be determined by the publisher and vendor. API will standardize interaction, not implementation.
- Persistence method
  - Multiple storage options possible: cookie, mobile app SDK, login alliances, centralized registries, etc.
- Javascript library gives vendors the flexibility to implement storage in whatever mechanism they see fit, supporting both desktop and mobile.

Transmitting Approved Vendors and Consent.

- Value to be binary
- Values to be compressed into as small of a data structure possible.
- Data structure flexible
  - Policy requirements and technical feasibility will determine final implementation
- Transmitted via a Daisy Chain
  - Every upstream member will append a payload to all downstream requests.
  - OpenRTB to directly support transmission

Combined, They Enable:

- **Control** over the vendors enabled by publishers.
- **Transparency** into the supply chain for consumers & publishers.
- An **auditable consent trail** that gives all supply chain members confidence by providing a more efficient disclosure mechanism, enabling companies to "know" rather than "assume" their status with a user.
- A **better user experience** than if every part in the ecosystem were to try to solve the challenge on their own.

Implementation targets – completed:

- Publication of draft technical specifications – Complete
- Publication of draft policy standard – Complete
- Open RTB Extension specification (v1) – Complete

- Reference implementation (v1) – Complete

OpenRTB GDPR Advisory

Objective: To Provide a Common Method of Transmission of User Approved Purposes & Vendors

Method: OpenRTB Extension Mechanism vs. a New Version to Avoid Adoption Friction

Advisory: Since this affects everyone all at once, let's rally around using the same extensions

Call to Action: Technology Focus

- CMP developers: build and make your CMP available
- Publishers and marketers: plan on integrating a CMP, Contact your adtech, adtech analytics partner, or IAM Tech Lab for guidance
- Exchanges/AdServers: review the GDPR transparency & consent specs and samples and implement support to get, handle and pass through the consent information.

Call to Action: Participation

- Policy Respresentatives:
  - Join the IAB Europe GDPR Implementation Group
- Technology representatives:
  - Join the IAB Tech Lab GDPR Technical Working Group