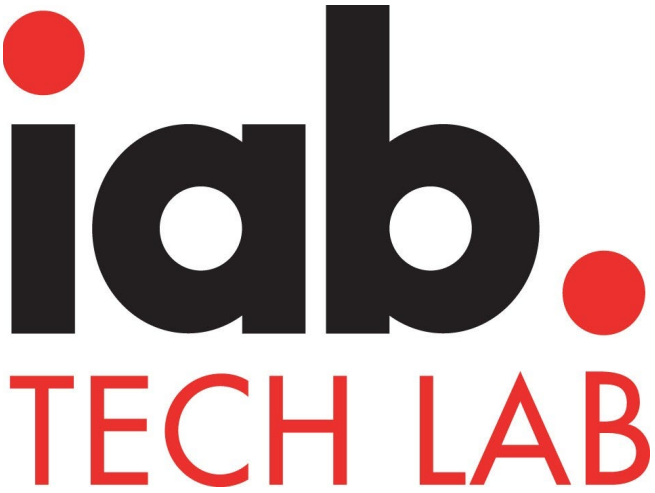

U.S. Privacy User Signal Mechanism "USP API"

(CCPA Compliance Mechanism)

Draft for Public Comment

October 22, 2019

Version 1.0

As part of the IAB CCPA Compliance Framework, this document is in public comment until November 5, 2019. Comments on technical specifications can be sent to privacy@iabtechlab.com.

Table of Contents

Introduction

License

Disclaimer

About IAB Tech Lab

About IAB CCPA Compliance Framework

Relevant Documents

Version History:

Requirements for U.S. Privacy User Signal API

What are you required to support?

What baseline functionality is required?

Where should the string be stored?

How is the API exposed?
    getUSPData

In-app support

Introduction

This document outlines technical mechanisms to support communication of U.S. Privacy signal. These signals contain information about disclosures made and choices selected by a user regarding consumer data privacy under U.S. Privacy regulation and are documented in a separate U.S. Privacy String specification. Version 1 of this U.S. Privacy User Signal API specification only supports signals pertaining to the California Consumer Privacy Act (CCPA).

This specification was created because Digital Properties need a scalable way to establish and persist U.S. Privacy signals. Additionally, downstream vendors need a reliable way to access U.S. Privacy signals when running within a Digital Property's website or app.

This document specifies a lightweight API that may be implemented by Digital Properties for web and mobile in-app to represent U.S. Privacy signals.

License

Disclaimer

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 DigiTrust identity service. Board members/companies are listed at https://iabtechlab.com/about-the-iab-tech-lab/tech-lab-leadership/. For more information, please visit https://www.iabtechlab.com.

About IAB CCPA Compliance Framework

The IAB Privacy & Compliance Unit, gathering legal, public policy, and tech experts from IAB, IAB Tech Lab, and member companies representing the digital advertising, marketing, and media ecosystem, developed the IAB CCPA Compliance Framework for Publishers and Technology Companies (Draft for Public Comment), which was released on October 22, 2019 for review and feedback by November 5. The IAB CCPA Compliance Framework comprises of policy and technical work to support CCPA compliance. The technical specifications in this document are the work product of the IAB Tech Lab's CCPA/U.S. Privacy Technical Working Group and refer to the guidance within the IAB CCPA Compliance Framework Draft.

Relevant Documents

Policies and information about IAB CCPA Compliance Framework: https://iab.com/ccpa

- IAB CCPA Compliance Framework Policies

Technical specifications: https://iabtechlab.com/standards/ccpa

- IAB Tech Lab U.S. Privacy String
- IAB Tech Lab U.S. Privacy User Signal API
- IAB Tech Lab U.S. Privacy OpenRTB Extension

Please send your comments on the technical specifications to privacy@iabtechlab.com by November 5, 2019.

Version History:

Date	Version	Comments
October 2019	1.0	Draft for public comment. Version 1 ONLY supports CCPA Compliance.

Requirements for U.S. Privacy User Signal API

The U.S. Privacy Signal component follows design patterns found in similar privacy compliance frameworks. The design pattern includes how the component is loaded into web pages or native apps and how vendors interact with the USP API. The USP component shall be loaded onto a Digital Property's site or app.

What are you required to support?

To support sending and receiving of the U.S. Privacy String within the User Signal Mechanism, the following functionalities:

- Desktop JavaScript API support
- Mobile local storage support, and An API (optionally Swift or Java, etc)
- Macro support (see U.S. Privacy String specification for details)

What baseline functionality is required?

As a baseline, Digital Properties must create a string and make it available to vendors via this API. This string indicates that CCPA does not apply, or signals whether the explicit notice has been provided and the user opted out.

Where should the string be stored?

The Digital Property is responsible for storing the string. It's recommended to store the string into a 1st party cookie, named "usprivacy", to and from where the library can write/read it. In case storing on a 1st party cookie is not possible or practical (e.g. on mobile native or if cookies are disabled), a different storage method can be adopted. The API provides individual methods to modify the value of each different section of the string.

How is the API exposed?

The following API function can be provided;

__uspapi(*Command, Version, Callback*)

__*uspapi()* **must always be a function** at all times, even at initialization – the API must be able to handle calls at all times.

Secondarily, the implementation must provide a proxy for postMessage events targeted to the __uspapi interface sent from within nested iframes. GUIDANCE TO COME on iframes for working with IAB SafeFrames.

At the minimum, the implementation must support the following API commands: `'getUSPData'`.

getUSPData

argument name	type	optional	value
command	string		`'getUSPData'`
version	number		`U.S. Privacy spec version`
callback	function		`function(uspData: uspdata, success: boolean)`

Example:

```
__uspapi('getUSPData', 1, (uspData, success) => {
  if(success) {
    // do something with uspData
  } else {
    // do something else
  }
});
```

If U.S. Privacy does not apply to this user in this context then the string in uspData object will contain "1--".

The callback shall be called immediately and without any asynchronous logic with whatever information is available in the current state of the library.

A value of `false` will be passed as the argument to the `success` callback when no uspData object could be returned.

The `callback` shall be invoked only once per api call with this command.

uspData Object

```
{
  "version": 1,            /* number indicating the U.S. Privacy spec
version */
  "uspString": "1YN"       /* string; not applicable: "1--" */
          /* number; 1 applies, 0 doesn't apply, -1 not set */
  }
```

In-app support

The encoded string and any related information must be stored on NSUserDefaults (iOS) or SharedPreferences (Android). This allows:

- Vendors to easily access the string information when they need to;
- The string and any related information to be persisted across app sessions;
- Pre-parsing of the string to enable all typical use-cases, with flexibility to act according to the user's choices.

Here is the list of the key value pairs provided:

Key / Field	Scope	Values	Description
IABUSPrivacy_String	**optional**	**String** E.g. "1YN"	Aligns with IAB OpenRTB CCPA Advisory. The String encodes all choices and information.