Introduction

A U.S. Privacy String contains information about disclosures made and choices selected by a user regarding consumer data privacy under U.S. Privacy regulation. Version 1 of this specification only supports signals pertaining to the California Consumer Privacy Act (CCPA).

To facilitate CCPA compliance, the U.S. Privacy String signals whether or not the U.S. Privacy Regulations apply to the consumer, if an "explicit notice" legal disclosure has been established with a consumer, and if the consumer has chosen to opt out of the sale of their personal data.

If U.S. Privacy Regulations apply, Digital Property Owners (e.g. website publishers or app publishers) are expected to send the U.S. Privacy String as a payload with each impression to all third parties who use personal data on their property. Third parties interpret the signals presented in a U.S. Privacy String to determine if they are able to process a user’s personal data.

The string data format enables standard persistent storage of user’s preferences by Digital Property Owners and supports transport of that data to relevant parties.
License

U.S. Privacy String and API technical specifications governed by the IAB Tech Lab is licensed under a Creative Commons Attribution 3.0 License. To view a copy of this license, visit creativecommons.org/licenses/by/3.0/ or write to Creative Commons, 171 Second Street, Suite 300, San Francisco, CA 94105, USA.

Disclaimer

THE STANDARDS, THE SPECIFICATIONS, THE MEASUREMENT GUIDELINES, AND ANY OTHER MATERIALS OR SERVICES PROVIDED TO OR USED BY YOU HEREUNDER (THE “PRODUCTS AND SERVICES”) ARE PROVIDED “AS IS” AND “AS AVAILABLE,” AND IAB TECHNOLOGY LABORATORY, INC. (“TECH LAB”) MAKES NO WARRANTY WITH RESPECT TO THE SAME AND HEREBY DISCLAIMS ANY AND ALL EXPRESS, IMPLIED, OR STATUTORY WARRANTIES, INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AVAILABILITY, ERROR-FREE OR UNINTERRUPTED OPERATION, AND ANY WARRANTIES ARISING FROM A COURSE OF DEALING, COURSE OF PERFORMANCE, OR USAGE OF TRADE. TO THE EXTENT THAT TECH LAB MAY NOT AS A MATTER OF APPLICABLE LAW DISCLAIM ANY IMPLIED WARRANTY, THE SCOPE AND DURATION OF SUCH WARRANTY WILL BE THE MINIMUM PERMITTED UNDER SUCH LAW. THE PRODUCTS AND SERVICES DO NOT CONSTITUTE BUSINESS OR LEGAL ADVICE. TECH LAB DOES NOT WARRANT THAT THE PRODUCTS AND SERVICES PROVIDED TO OR USED BY YOU HEREUNDER SHALL CAUSE YOU AND/OR YOUR PRODUCTS OR SERVICES TO BE IN COMPLIANCE WITH ANY APPLICABLE LAWS, REGULATIONS, OR SELF-REGULATORY FRAMEWORKS, AND YOU ARE SOLELY RESPONSIBLE FOR COMPLIANCE WITH THE SAME.

About IAB Tech Lab

About IAB Technology Laboratory

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 improving the digital advertising supply chain, measurement, and consumer experiences, while promoting responsible use of data. 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 include ExtremeReach, Facebook, Google, GroupM, Hearst Digital Media, Index Exchange, Integral Ad Science, LinkedIn, LiveRamp, MediaMath, Microsoft, Oracle Data Cloud, Pandora, PubMatic, Quantcast, Rakuten Marketing, Telaria, The Trade Desk, Verizon Media Group, Xandr, and Yahoo! Japan.

About IAB CCPA Compliance Framework

The IAB CCPA Compliance Framework comprises of policy and technical work to support CCPA compliance. This document is the work product of the IAB Tech Lab’s CCPA/U.S. Privacy Technical Working Group. Policy requirements were developed by a legal affairs group at IAB in the US. The technical specifications documents refer to the guidance within IAB CCPA Compliance Framework Policies.

More information about the Framework is available at iab.com/guidelines/ccpa-framework and technical specifications are available at iabtechlab.com/ccpa.

Final v1.0 Specifications

Final v1.0 technical specifications for the IAB CCPA Compliance Framework may be re-released when the Limited Service Provider Agreement is released to the industry. Furthermore, in the future, the technical component of the Framework may support the communication of data deletion requests.

Relevant Documents

IAB CCPA Compliance Framework Policies
IAB Tech Lab U.S. Privacy String
IAB Tech Lab U.S. Privacy User Signal API
IAB Tech Lab U.S. Privacy OpenRTB Extension

Version History:

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 2019</td>
<td>1.0</td>
<td>Draft for public comment. Version 1 ONLY supports CCPA Compliance.</td>
</tr>
<tr>
<td>November 2019</td>
<td>1.0</td>
<td>Published final public version. Added support for Limited Service Provider Agreement (LSPA) signal.</td>
</tr>
</tbody>
</table>
What information is stored in a U.S. Privacy String?

This current version of the U.S. Privacy String only supports CCPA Compliance. The U.S. Privacy String contains the following information:

1. **General metadata**: the version of this string specification.
2. **Explicit Notice and Opportunity to Opt-Out of Sale of Data**
3. **Opt-Out of Sale**: Whether the consumer has opted out of sale of their personal data
4. **Support for Limited Service Provider Agreement**

Who should create a U.S. Privacy string?

Digital Property Owners are responsible for generating, persisting, and passing the U.S. Privacy string.

When should a U.S. Privacy string be created?

When a sale of data may occur, for example on an impression opportunity, the string should be created. A string can be created to indicate CCPA applies, or to signal the Digital Property owner has determined that CCPA does not apply.

U.S. Privacy String

The U.S. Privacy string consists of the following components.

<table>
<thead>
<tr>
<th>String Component</th>
<th>Expected Values</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specification Version</td>
<td><strong>Number</strong> (1 char in string)</td>
<td>The version of this string specification used to encode the string</td>
</tr>
<tr>
<td>Explicit Notice/Opportunity to Opt Out</td>
<td><strong>ENUM</strong> <em>(N = No, Y = Yes, - = Not Applicable)</em></td>
<td>Has explicit notice been provided as required by 1798.115(d) of the CCPA and the opportunity to opt out of the sale of their data pursuant to 1798.120 and 1798.135 of the CCPA</td>
</tr>
<tr>
<td>Opt-Out Sale</td>
<td><strong>ENUM</strong> <em>(N = No, Y = Yes, - = Not Applicable)</em></td>
<td>Has user opted-out of the sale of his or personal information pursuant to 1798.120 and 1798.135</td>
</tr>
</tbody>
</table>
In situations where the Digital Property has determined that the consumer does not fall within a U.S. Privacy jurisdiction (e.g. CCPA), the Digital Property may signal this with hyphens in the second through fourth character positions in the following manner: “1---”. Otherwise, when signals are present, the consumer falls within a U.S. Privacy jurisdiction.

Examples

A Digital Property has determined to use a U.S. Privacy string and that CCPA applies to the transaction. The Digital Property is using version 1 of the U.S. Privacy string specification. The Digital Property has provided explicit user notice. The user has not made a choice to opt out of sale. The Digital Property does not intend the transaction to operate within the Limited Service Provider Agreement.

1YNN

A Digital Property has determined to use a U.S. Privacy string and that CCPA applies to the transaction. The Digital Property is using version 1 of the U.S. Privacy string specification. The Digital Property has not provided explicit user notice. The user has made a choice to opt out of sale. The Digital Property does intend the transaction to operate within the Limited Service Provider Agreement.

1NYY

A Digital Property has determined to use a U.S. Privacy string version 1 and that CCPA does not apply to the transaction.

1---

URL Parameters

A URL-based service that requires U.S. Privacy signals should accept U.S. Privacy string according to the following URL parameter specification. A creator of a URL should ensure that
the `us_privacy` URL parameter exists only once in the URL, and the URL-based service accepting the request is capable of interpreting a U.S. Privacy string and propagating it to other services.

<table>
<thead>
<tr>
<th>URL parameter</th>
<th>Possible values</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>us_privacy</td>
<td>string</td>
<td>N/A</td>
<td>URL-encoded U.S. Privacy string format as specified above.</td>
</tr>
</tbody>
</table>

Substitution macros following naming and values consistent with this specification can be optionally supported.

Naming convention for this macro:

${US_PRIVACY}