

# **Global Privacy Platform (GPP) & US State Signals**



# What is the Global Privacy Platform (GPP)?

---

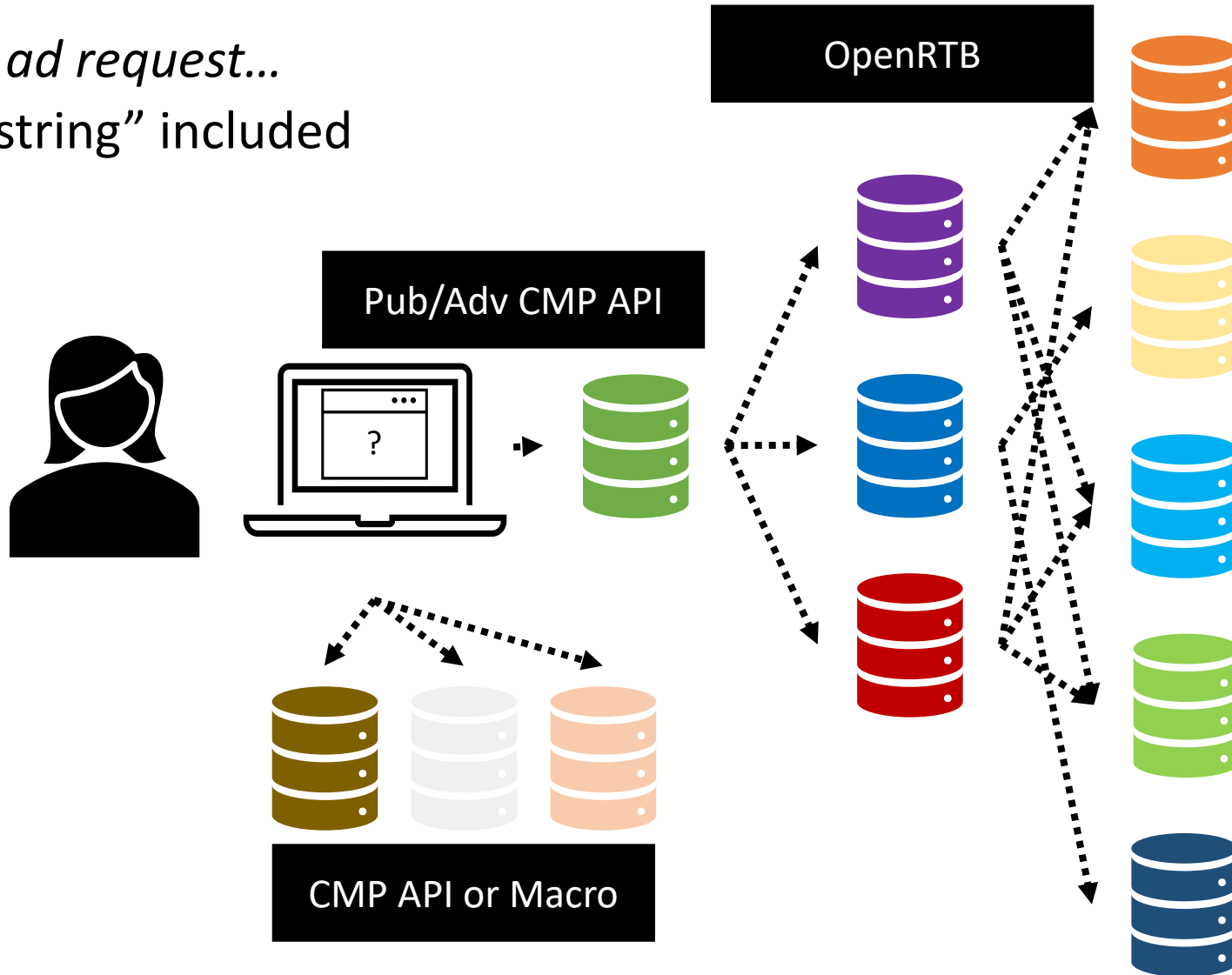
## What it is

- Adaptable, channel-agnostic protocol for signaling user privacy consent & choice down the ad supply chain
- Supports existing signals including IAB Europe's TCF
- Flexible architecture makes it ready to support new regional signals without the need to start from scratch each time

# Global Privacy Platform Privacy Signaling Concept

For one ad request...

.....> "string" included

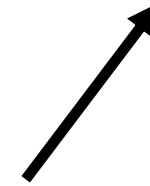
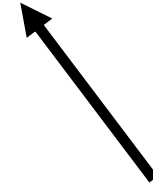


- Publisher ad server
- SSPs
- DSPs
- Advertiser ad server
- Creative server
- Verification vendor(s)
- Attribution vendor(s)
- ...

# Global Privacy Platform “String” Concept

---

`whatsInThisString~sectionOneEncodedValues~sectionFiveEncodedValues`



Header acting as a string  
“table of contents”

Discrete sections of privacy  
signals (regional, etc...)

# Transport Mechanisms

---

## Consent Management Platform API

- One "global" API that can be used to access consent information for any supported privacy signal
- Features a standard set of commands that can be used to retrieve the GPP String or section-specific information.
- Flexibility for regional sections to define set of non-generic commands via section extensions

## OpenRTB

- Field within the Regs object for passing the GPP string

## URL Parameters and Macros

- Standard parameters and macros to be used to pass the GPP string

# Summary of GPP

---

The Global Privacy Platform streamlines technical privacy signaling protocols with:

- GPP String - standardized way for privacy signals to be created
- Standard interfaces for transport of the GPP string including one CMP API, standard fields in OpenRTB, standard URL parameters and macros

# How does this relate to the MSPA?

Using the GPP allows:

- First Parties to pass the appropriate signals that communicate consumer choices to Downstream Participants providing information like, what mode the First Party is operating in and whether the Downstream Participant should be engaging as a "service provider" or "processor"
- Downstream Participants to receive the privacy signals to understand and honor consumer choices and to understand if they should be engaging as a "service provider" or "processor"

## Section IDs

Each section represents a unique privacy signal, usually a unique jurisdiction. Below are the supported discrete sections.

Section ID	Client-side API Prefix	Description
1	tcfeuv1	EU TCF v1 section (deprecated)
2	tcfeuv2	<a href="#">EU TCF v2 section</a> (see note below)
3		GPP Header section (REQUIRED, see note below)
4	--	GPP signal integrity section
5	tcfca	<a href="#">Canadian TCF section</a>
6	uspv1	<a href="#">USPrivacy String</a> (Unencoded Format)
7	usnat	US - national section
8	usca	US - California section
9	usva	US - Virginia section
10	usco	US - Colorado section
11	usut	US - Utah section
12	usct	US - Connecticut section

# Example GPP Strings

**iab.**TECH LAB



# Example – California Section

## Conditions

- MSPA Covered Transaction
- MSPA OptOut Option Mode
- Consumer was shown the appropriate notice
- Consumer did not opt out of Sale or Share of Personal Information
- Business is not using Consumer's Personal Information for advertising purposes that are unrelated for which the data was collected or processed
- GPC signal not detected

## Step 1

**Create the discrete section for California.**

In this example, the encoded California signal is created ("California string")

## Fields

Version = 1  
SaleOptOutNotice = 1  
ShareOptOutNotice = 1  
SensitiveDataLimitUseNotice = 0  
SaleOptOut = 2  
SharingOptOut = 2  
SensitiveDataProcessing = 0  
KnownChildSensitiveDataConsents = 0  
PersonalDataConsents = 0  
MSPACoveredTransaction = 1  
MSPAOptOutOptionMode = 1  
MSPA ServiceProviderMode = 0  
GPC = 0

## Bit representation

```
000001 010100 101000 000000 000000 000000  
000001 100000
```

## Encoded section for California

BUoAAABg.Q

# Example – California Section

## Conditions

- Includes the section for California

## Step 2

### Create the header section.

In this example, the encoded header is created indicating that the GPP string contains privacy signals for the California section (Section ID 8).

## Fields

Type = 3  
Version = 1  
Sections = 8

## Bit representation

000011 000001 000000 000001 000001 100000

## Encoded header section

DBABBg

# Example – California Section

## Conditions

- Includes the section for California
- MSPA Covered Transaction
- MSPA OptOut Option Mode
- Consumer was shown the appropriate notice
- Consumer did not opt out of Sale or Share of Personal Information
- Business is not using Consumer's Personal Information for advertising purposes that are unrelated for which the data was collected or processed
- GPC signal not detected

## Step 3

**Concatenate all the header section and the California section.**

In this example, the encoded header and the California section are concatenated with the “~” (tilde) delimiter.

## Encoded header

DBABBg

## Encoded section for California

BUoAAABg.Q

## GPP string

DBABBg~BUoAAABg.Q

# Thank you!

GPP Specification:

<https://github.com/InteractiveAdvertisingBureau/Global-Privacy-Platform>

