GLOBAL PRIVACY CONTROL

How to Implement **Global Privacy Control (GPC)** for Publishers

Aram Zucker-Scharff & Sebastian Zimmeck

This whitepaper is for informational purposes only and is not legal advice.

What's going on?

The California Attorney General's Office has **begun to enforce** the California Consumer Privacy Act (CCPA) and stated that sites need to comply with the **Global Privacy Control (GPC)** when it is used to state a Do Not Sell preference. According to **the CA Attorney General's website**:

> *"Opting out of the sale of personal information should be easy for consumers, and the GPC is one option for consumers who want to submit requests to opt-out of the sale of personal information via a user-enabled global privacy control.* ***Under law, it must be honored by covered businesses as a valid consumer request to stop the sale of personal information."*** *(emphasis added)*

This means that when a site must comply with CCPA, it must also parse and respect the GPC signal as another way users can opt out of the use of their personal data for a sale. Colorado and Connecticut have also passed legislation mandating compliance with global privacy signals, though those laws have not yet gone into effect.

What is GPC?

GPC is a way users can universally express, to all sites, their preference not to be tracked on the web. It is a browser-level signal, maintained either by a browser or browser extension, that a user or privacy-focused technology can set. The easiest way to think of GPC is as a robot that selects the Do Not Sell preference on a site on behalf of a user. The open source tool was developed by a coalition of advocates, academics, and companies to allow users to exercise new rights to opt out of data sharing at scale.

Sites that detect GPC may interpret the signal in a variety of ways depending on their interpretation of the privacy laws applicable to the site. Some sites use GPC to turn off all third party user tracking regardless of location, others use it as a tool to limit certain data sharing in only some jurisdictions. Regardless of such use, it is now recognized as a way to express Do Not Sell preferences under the CCPA. The effects of GPC may be different in other jurisdictions but this document is focused on California.

What does the enforcement of GPC mean for site maintainers?

Websites that employ third party systems for the tracking of users for ad targeting or other commercial purposes will now need to take steps to honor GPC choices, creating an automated flow that takes the signal and uses it to mark the session as Do Not Sell as defined under CCPA, potentially through using compatible systems like the IAB's **USP API**. If the business knows the identity of the user, the "Do Not Sell" applies to all uses of the person's information, not just the web session.

Because the GPC is on a window-level object and on request headers, its presence is the fastest way to handle decision-making around user privacy. GPC has been adopted by The Washington Post, The New York Times, and a variety of other publishers. It also is supported by a number of major Consent Management Platforms (CMPs), including OneTrust, SourcePoint, and WireWheel. GPC simplifies the process of user opt out. It does so without adding technical complexity that could slow ad execution. The ease of execution means that GPC is a positive development for helping sites follow CCPA regulations.

Expected Impact

As of the writing of this document over 50 million users are utilizing a browser or extension with GPC support. Some systems that allow the user to express their privacy preference with GPC are **Abine**, **Brave**, **DuckDuckGo**, **OptMeowt**, and **Privacy Badger**.

Impact on your site will depend on your interpretation of the CCPA and CPRA. There are open questions about what specific processing activities are covered by an opt-out request under those laws; the California Privacy Protection Agency is currently drafting rules to provide more clarity to implementers, but those rules have not been finalized. Not all of those 50 million users are in California, and if you limit your processing of GPC to California, the percentage of users using it will depend on how much of your traffic you get from California. However, if you accept GPC beyond California, it may result in a larger impact.

To understand the impact on your individual site, we generally recommend tracking the percentage of users activating a GPC signal as a non-user-identified metric in your site's analytics.

Implementation Guidance

What follows are known best-practices for site-owners and publishers to implement GPC parsing. A site may choose to further implement GPC by using the signal for other regions' regulations, or as a general user preference to be used across all sessions, but that functionality is highly varied from site to site and not described here.

Importantly, GPC is convenient to implement as a stateless protocol. Sites do not need to keep track of a user's status being opted out as every request will contain it.

Transparency: Implementing .well-known/gpc.json and Privacy Policy Update

GPC makes use of **.well-known identifiers** for sites to signal compliance with the **GPC specification**. The existence of this file indicates you are using GPC as part of your compliance with privacy laws. There may be a variety of tools for implementing .well-known files in your Content Management System (CMS) or website. Here is an example **for WordPress** and another **for Gatsby**. If you can find a method of implementing `.well-known/gpc.json` that is native to your CMS, we recommend you do so.
What follows is a basic example assuming you have the capability to designate a static folder and files for your site.

First create a folder named **`.well-known`** at the base of your site, so it would have a path of **`yoursite.com/.well-known/`**. In that folder create a file with the name of **`gpc.json`**. The file's value should then look something like this with `lastUpdate` set to the date you have last updated the file.

```
{
   "gpc": true,
   "lastUpdate": "2022-04-20"
}
```

This will give you a valid GPC file that states you comply with GPC within the context you understand it to apply.

Adopters will usually supplement the .well-known file with a statement in their Privacy Policy that states exactly how they interpret GPC within their own systems. The exact message in your privacy policy is up to you and may require review by your legal team. A suggested addition, similar to the **privacy policy of The New York Times**:

> *"Finally, if your browser supports it, you can turn on the Global Privacy Control to opt-out of the "sale" of your personal information under California's CCPA."*

Changing Data Sharing Practices: Implementing the GPC signal with the IAB's USP API

The USP API is a method of compliance recommended by the IAB. While there are other ways to comply with CCPA, the USP API is the most commonly used so instructions for syncing GPC with the USP API follow. If you use a CMP, it is highly likely that your use of the USP API is dependent on their system. Before moving forward with the guidance below, check with your CMP to see if they support **GPC** and if they provide a way to turn that support on. **If you are using OneTrust, here is a link to how you can turn on GPC support.** Your CMS may also include tools to comply with GPC. **Here's an example for Express-based NodeJS applications**.

What follows is a way to process the GPC signal, using the on-page signal set on the navigator object. In the current specification a signal is either null or set to Do Not Sell. We can reflect that in the adopted logic. You can also **process the GPC signal on the header of HTTP requests**.

The following example relies on the assumption that the page accepting the signal is doing so in concert with the IAB's CCPA Framework and has given the user explicit notice somewhere on their page. This sample script does not include other methods by which you may monitor and set the CCPA preference of a user. It should be placed as early on the page as possible to gain the maximum performance result from leveraging GPC.

```
// This will cover cases where it is set to null or set. In the case of older user agents, it should not be assumed that the lack of a signal is equivalent to permission to sell.

    if(navigator.globalPrivacyControl){
       var CCPAConsent = ''
          switch (navigator.globalPrivacyControl) {
              case "1":
                 // Y indicates the user has selected opt out
                 CCPAConsent = 'Y';
                 break;
              default:
                 // N indicates the user has not selected to opt out
                 CCPAConsent = 'N';
       }
       var uspFramework = {
           version: 1,
           notice: 'Y',
           optOut: CCPAConsent,
           // You will have other things besides GPC that are likely to set this value.
           lspa: 'Y'
       }
       // Will return a USP string like `1YYY`
       var uspString = Object.values(uspFramework).reduce((a, c) => { return a+c }, '')
          window.__uspapi = (command, version, callback) => {
           if (command === 'getUSPData' && version === 1) {
                 callback(uspString, true)
           }
       }
    } else {
    // Standard logic for handling CCPA without the navigator.globalPrivacyControl setting.
    }
```

Results

Because of its presence at the level of the browser and its immediate availability, requests with GPC where CCPA has to be followed have a significantly lower time to first ad load.

Aram Zucker-Scharff

Aram Zucker-Scharff is the Engineering Lead for Privacy & Security Compliance at The Washington Post. He develops open-source tools for publishers and was one of Folio Magazine's 15 under 30 in the magazine media industry.

Sebastian Zimmeck

Sebastian Zimmeck is an assistant professor of computer science at Wesleyan University focused on information privacy and security. He co-founded Global Privacy Control and is leading the privacy-tech-lab.