Global Privacy Control (GPC)

Proposal 22 March 2024

▼ **More details about this document**

Latest editor's draft:
https://privacycg.github.io/gpc-spec/

History:
Commit history

Editors:
Sebastian Zimmeck (Wesleyan University)
Peter Snyder (Brave Software)
Justin Brookman (Consumer Reports)
Aram Zucker-Scharff (The Washington Post)

Former editors:
Robin Berjon (Protocol Labs) (The New York Times until Sep 2022)
Ashkan Soltani (Independent)
David Harbage (DuckDuckGo)

Feedback:
GitHub privacycg/gpc-spec (pull requests, new issue, open issues)

Abstract

This document defines a signal, transmitted over HTTP and through the DOM, that conveys a person's request to websites and services to not sell or share their personal information with third parties. This standard is intended to work with existing and upcoming legal frameworks that render such requests enforceable.

Status of This Document

This document is a specification proposal.

Table of Contents

§ 1. Introduction

This section is non-normative.

Building websites today often requires relying on services provided by businesses other than the one which a person choses to interact with. This result is a natural consequence of the increasing complexity of Web technology and of the division of labor between different services. While this architecture can be used in the service of better Web experiences, it can also be abused to violate privacy ([Privacy-Principles]). While data can be shared with service providers for limited operational purposes, it can also be shared with third parties or used for behavioral targeting in ways that many users find objectionable.

Several legal frameworks exist — and more are on the way — within which people have the right to request that their privacy be protected, including requests that their data not be sold or shared beyond the business with which they intend to interact. Requiring that people manually express their rights for each and every site they visit is, however, impractical.

> Given the ease and frequency by which personal information is collected and sold when a consumer visits a website, consumers should have a similarly easy ability to request to opt-out globally. This regulation offers consumers a global choice to opt-out of the sale of personal information, as opposed to going website by website to make individual requests with each business each time they use a new browser or a new device. [CCPA-AG-FINAL-STATEMENT]

This specification addresses the issue by providing a way to signal, through an HTTP header or the DOM, a person's assertion of their applicable rights to prevent the sale of their data, the sharing of their data with third parties, and the use of their data for cross-site targeted advertising. This signal is equivalent, for example, to the "global privacy control" in the CCPA [CCPA-REGULATIONS].

§ 2. Definitions

A ***do-not-sell-or-share interaction*** is an interaction with a website in which the person is requesting that their data not be sold to or shared with any party other than the one the person intends to interact with, or to have their data used for cross-site ad targeting, except as permitted by law.

A ***do-not-sell-or-share preference*** is when a person requests that their data "not be sold or shared" for instance by activating a Global Privacy Control setting with their user agent or by using tools that default to such a setting (possibly because this setting matches the most common expectations of that tool's users). When set, this preference indicates that the person expects to browse the Web with do-not-sell-or-share interactions.

§ 3. Expressing a Do Not Sell Or Share Preference

§ 3.1 Expression Format

A Global Privacy Control preference should be conveyed for all HTTP requests (in the form of the HTTP header) and all websites (in the form of the Web API property).

If set, this preference is expressed as a single value of `1` or equivalently `true` according to context.

In the absence of regulatory, legal, or other requirements, websites *MAY* interpret an expressed Global Privacy Control preference as they find most appropriate for the given person, particularly as considered in light of the person's privacy expectations, context, and cultural circumstances. Likewise, websites might make use of other preference information outside the scope of this protocol, such as site-specific person preferences or third-party registration services, to inform or adjust their behavior when no explicit preference is expressed via this protocol.

User agents are expected to convey person preferences as accurately as they can. User agents *SHOULD* strive to represent what the user agent best believes to be the person's preference for the Global Privacy Control value.

§ 3.2 Preference Caching

The preference *MUST* be cached on each top-level navigation to ensure consistency in communication of the person's request that their data "not be sold or shared." This means that if the preference changes during or after a top-level navigation, it will not be reflected until the next navigation.

A top-level browsing context has a ***gpcAtNavigation*** boolean. It is initially `false`.

The value of `gpcAtNavigation` *MUST* reflect the preference of the person when the top-level browsing context's active document began loading. It will be `true` if the person's preference was enabled, and `false` if the person's preference was disabled or had not been set.

If preference is changed to be inconsistent with some `gpcAtNavigation` cached in a top-level browsing context, the user agent *SHOULD* inform the user of any inconsistent tabs and provide the option to reload them, refreshing the cached `gpcAtNavigation` to reflect the current preference.

§ 3.3 The `Sec-GPC` Header Field for HTTP Requests

The ***Sec-GPC*** header field is a mechanism for expressing the person's preference for a do-not-sell-or-share interaction in an HTTP request (for any request method).

The syntax ([ABNF]) of the field is:

```
Sec-GPC-field-name  = "Sec-GPC"
Sec-GPC-field-value = "1"
```

A user agent *MUST NOT* generate a `Sec-GPC` header field if top-level browsing context's `gpcAtNavigation` is `false`.

A user agent *MUST* generate a `Sec-GPC` header field with a field-value that is exactly the numeric character "1" if top-level browsing context's `gpcAtNavigation` is `true`.

A user agent *MUST NOT* generate more than one `Sec-GPC` in a given HTTP request and *MUST NOT* use a `Sec-GPC` field in an HTTP trailer.

A server processing an HTTP request that contains a `Sec-GPC` header *MUST* ignore it and process the request as if that header had not been specified unless the field value is exactly the character "1". If there are multiple `Sec-GPC` headers and at least one has a field value of exactly "1" then the server *MUST* treat the request as if there were only one `Sec-GPC` header with a field value of "1"; and as if there were none otherwise.

HTTP intermediaries *MUST NOT* remove a `Sec-GPC` header set to "1", but they *MAY* remove `Sec-GPC` headers that contain other values. Additionally, an HTTP intermediary that has reasons to believe the the person originating a given HTTP request has a do-not-sell-or-share preference, *MAY* insert a `Sec-GPC` header set to "1".

> EXAMPLE 1: Example GPC Request
>
> ```
> GET /something/here HTTP/2
> Host: example.com
> Sec-GPC: 1
> ```

§ 3.3.1 Extensibility of the Sec-GPC Field Value

The `Sec-GPC` is deliberately defined without an extension mechanism. Experience with previous similar headers shows that people tend to rely on string equality instead of parsing the value when testing for their presence, especially when extensions do not yet exist. Such checks would of course fail in the presence of extension content, which would in turn render the mechanism moot. Should extensions prove necessary to this standard, they will need to be implemented through other headers, which may in time supersede this one.

§ 3.4 JavaScript Property to Detect Preference

The `globalPrivacyControl` property enables a client-side script to determine what `Sec-GPC` header field value was sent when loading the top-level browsing context's active document.

WebIDL

```
interface mixin GlobalPrivacyControl {
  readonly attribute boolean globalPrivacyControl;
};
Navigator includes GlobalPrivacyControl;
WorkerNavigator includes GlobalPrivacyControl;
```

The value is `false` if no `Sec-GPC` header field would be sent; otherwise, the value is `true`.

The value of `globalPrivacyControl` *MUST* be the top-level browsing context's `gpcAtNavigation`.

The `globalPrivacyControl` property is available on the `navigator` object in both regular and worker contexts, and so can be checked reading from `navigator.globalPrivacyControl`.

EXAMPLE 2: checking GPC in script

```
if (!navigator.globalPrivacyControl) {
  // wonderful, we can sell this person's data!
}
```

§ 4. GPC Support Resource

A site *MAY* produce a resource at a .well-known URL in order for a site to represent the fact that it abides by GPC requests, at least where required to do so. The purpose of a GPC support resource is for a site to convey its awareness of and support for the Global Privacy Control. The support resource is not intended to convey whether the site abides by GPC requests from the user agent accessing the resource. By default, an origin's support is *unknown*.

A GPC support resource has the well-known identifier `/.well-known/gpc.json` relative to the origin server's URL [RFC8615].

An origin server that receives a valid GET request targeting its GPC support resource responds either with a successful response containing a machine-readable representation of the site-wide tracking status, as defined below, or a sequence of redirects that leads to such a representation (which *MAY* be provided by a server at another origin).

§ 4.1 GPC Support Representation

The origin server *MUST* return the GPC support resource as a valid representation using the `application/json` media type [RFC8259], otherwise the origin's support is unknown.

The GPC support representation *MUST* be an JSON object, otherwise the origin's support is unknown. Members of this JSON object not in the list below have no meaning in this specification and *MUST* be ignored. Members include:

- A `gpc` member. The value of the `gpc` member *MUST* be either `true`, to indicate that the server intends to abide by GPC requests at least to the extent it is legally obligated to do so, or `false`, to indicate that it does not. For any other value the origin's support is unknown.
- A `lastUpdate` member. The value of the `lastUpdate` member *MUST* be an RFC3339 `full-date` (YYYY-MM-DD) or `date-time` (YYYY-MM-DDTHH:mm:ss.sssZ) [RFC3339]. This indicates the time at which the statement of support was made, such that later changes to the meaning of the GPC standard should not affect the interpretation of the resource for legal purposes. If the member is not in a valid RFC3339 format, the last update date and time is unknown.

EXAMPLE 3: example.org abides by GPC

```
GET /.well-known/gpc.json HTTP/2
Host: example.org
User-Agent: whatever


Content-Type: application/json

{
  "gpc": true,
  "lastUpdate": "1997-03-10"
}
```

§ 5. Legal Effects

This section is non-normative.

Receiving a GPC signal may have legal effects, depending on factors such as the location of the individual sending the signal, the scope of the applicable law, as well as any separate agreement between the recipient of the signal and the individual. For additional details on legal effects, consult the explainer.

For example, the use of the GPC signal by an individual will be intended to communicate the individual's intention to invoke the following rights, as applicable:

§ 5.1 Calfornia Consumer Privacy Act (CCPA)

Under the CCPA, the GPC signal will be intended to communicate a Do Not Sell request from a global privacy control, as per [CCPA-REGULATIONS] §999.315 for that browser or device, or, if known, the consumer.

Where the GPC signal conflicts with the existing privacy settings a consumer has with the business, the business shall respect the GPC signal but may notify the consumer of the conflict and give the consumer an opportunity to confirm the business-specific privacy setting or participation in the financial incentive program [CCPA-REGULATIONS] §999.315(c)(2).

§ 5.2 Colorado Privacy Act (CPA)

The CPA gives consumers the legal right to opt out of both the sale of their information as well as the use of their data for cross-site targeted advertising, including through the use of "universal opt-out mechanisms that clearly communicate a consumer's affirmative, freely given, and unambiguous choice to opt out." Under the CPA, the GPC signal will be intended to communicate a request to opt out of both the sale of their personal information and the use of their personal information for targeted advertising.

§ 5.3 Connecticut Data Privacy Act (CDPA)

Similarly, the CDPA gives consumers separate opt-out rights for data sales and targeted advertising, including through an "authorized agent by way of, among other things, a technology, including, but not limited to, an Internet link or a browser setting, browser extension or global device setting." Under the CDPA, the GPC signal will be intended to communicate a request to opt out of both the sale of their personal information and the use of their personal information for targeted advertising.

§ 5.4 Nevada Revised Statutes Chapter 603A (NRS 603A)

Under NRS 603A, a GPC signal will be intended to communicate a Do Not Sell My Personal Information request [SB220].

§ 5.5 EU General Data Protection Regulation (GDPR)

The GDPR requires that "Natural persons should have control of their own personal data" ([GDPR], Recital 7). The GPC signal is intended to convey a general request that data controllers limit the sale or sharing of the person's personal data to other data controllers ([GDPR] Articles 7 & 21). This request is expressed with every interaction that the user agent has with the server.

Note that this request is not meant to withdraw a person's consent to local storage as per the ePrivacy Directive ("cookie consent") ([EPRIVACY-DIRECTIVE]) nor is it intended to object to direct marketing under legitimate interest ([GDPR]).

§ 5.6 Other Jurisdictions and Privacy Rights

GPC could potentially be used to indicate rights in other jurisdictions as well.

Other US state privacy laws, such as those in Virginia and Utah, give consumers new opt-out rights around data sales and targeted advertising but are silent on the legal effect of global opt-out signals. Regulators enforcing those statutes may determine that a user activating a signal such as GPC may be sufficient to legally exercise opt-out rights in those jurisdictions.

However, GPC is not necessarily intended to invoke every new privacy right in every jurisdiction. For example, GPC is not intended to globally invoke data deletion rights on every website visited by the user. GPC is also not intended to limit a first party's use of personal information within the first-party context (such as a publisher targeting ads to a user on its website based on that user's previous activity on that same site). For that reason, GPC should not be interpreted as exercising the CCPA's right to limit the use of sensitive information in a first-party context.

Given the complexities of existing consent frameworks, publishers who accept the GPC signal should disclose how they treat the GPC signal in that jurisdiction and how they deal with conflicts between the signal and other specific privacy choices that the person has already made directly with the publisher, including instances where third party sharing may be permitted such as sharing to service providers/processors, sharing at law or at the direction of the individual.

§ 5.7 User Interface Language

User agents *SHOULD* strive to represent what the user agent best believes to be the person's preference for the Global Privacy Control value. While studies have shown that people do not want their data sold or shared, some jurisdictions have enacted "opt-out" legal frameworks where consumers have to take an affirmative action to express a preference to limit data sharing of the use of their data for targeted advertising.

Different jurisdictions have different prerequisites before a platform can enable a universal opt-out. For example, the most recent regulations promulgated under the California Consumer Privacy Act state:

> The platform, technology, or mechanism that sends the opt-out preference signal shall make clear to the consumer, whether in its configuration or in disclosures to the public, that the use of the signal is meant to have the effect of opting the consumer out of the sale and sharing of their personal information. The configuration or disclosure does not need to be tailored only to California or to refer to California ([CPPA-REGULATIONS], §7025(b)(2)).

Colorado and other jurisdictions are more prescriptive about requirements for a valid universal opt-out signal. For example, Colorado's regulations explicitly provide "a Universal Opt-Out Mechanism may not be the default setting for a tool that comes pre-installed with a device, such as a browser or operating system" ([COLORADO-REGULATIONS], Rule 5.04(a)).

Currently California and Colorado are the only jurisdictions in the United States that empower regulators to issue detailed regulations on topics such as universal opt-outs. Other statutes state relatively high level legal requirements that may be augmented by informal guidance (such as an FAQ) or through enforcement.

The legal landscape around global opt-outs is also changing. In 2023, several new states passed laws that include requirements to honor global opt-outs, though some of those states' provisions differ considerably. Additionally states may revise their legal requirements as California has already amended the original CCPA that was passed in 2018.

In addition to the United States, other jurisdictions may recognize universal privacy signals and may impose their own requirements before such signals are deemed legally bindinging.

For more information on the latest legal requirements, please review the implementation guide which will provide more up-to-date information about the latest legal guidance around global opt-outs.

User agents are expected, where required, to present all the appropriate notices to people to ensure that the rights they wish to avail themselves of are effectively binding.

§ 6. Privacy Considerations

Exposing a user's preference (in the HTTP header field or

`navigator`

object) potentially divides users into two groups in a way that might increase the information available for fingerprinting. This extra information is available unless the signal perfectly correlates with other signals. Depending on the browser and implementation, the GPC signal may impose a privacy cost, though one intended to be justified by the privacy benefit of sending the signal.

§ 7. Conformance

As well as sections marked as non-normative, all authoring guidelines, diagrams, examples, and notes in this specification are non-normative. Everything else in this specification is normative.

The key words *MAY*, *MUST*, *MUST NOT*, and *SHOULD* in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

§ A. Implementation Considerations

It is worth considering that a GPC signal will be attached to every HTTP request made to a given site. Rendering a page on the Web often requires making dozens such requests. As such it can prove impractical for GPC signals to trigger full-blown opt-out procedures with costly audit trails for every single GPC interaction as that will cause a large amount of processing, including for resources served from a content delivery network (CDN) that must be executed as efficiently as possible.

Regulations that intend to support GPC are encouraged to consider such implementation difficulties. One way of addressing them is to differentiate between user interface affordances given to people for the purpose of requesting a do-not-sell-or-share interaction preference to persist on the site, and the provision of a do-not-sell-or-share interaction signal the state of which is maintained with the user agent. In the latter case, the interaction can be processed as if the person had previously requested such a do-not-sell-or-share interaction preference and were interacting with that preference already active.

§ B. Acknowledgments

This specification relies on concepts developed in large part by the Tracking Protection Working Group and others who contributed to Tracking Preference Expression (DNT).

§ C. References

§ C.1 Normative references

[ABNF]

Augmented BNF for Syntax Specifications: ABNF. D. Crocker, Ed.; P. Overell. IETF. January 2008. Internet Standard. URL: https://www.rfc-editor.org/rfc/rfc5234

[html]

HTML Standard. Anne van Kesteren; Domenic Denicola; Dominic Farolino; Ian Hickson; Philip Jägenstedt; Simon Pieters. WHATWG. Living Standard. URL: https://html.spec.whatwg.org/multipage/

[RFC2119]

Key words for use in RFCs to Indicate Requirement Levels. S. Bradner. IETF. March 1997. Best Current Practice. URL: https://www.rfc-editor.org/rfc/rfc2119

[RFC3339]

Date and Time on the Internet: Timestamps. G. Klyne; C. Newman. IETF. July 2002. Proposed Standard. URL: https://www.rfc-editor.org/rfc/rfc3339

[RFC8174]

Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words. B. Leiba. IETF. May 2017. Best Current Practice. URL: https://www.rfc-editor.org/rfc/rfc8174

[RFC8259]
The JavaScript Object Notation (JSON) Data Interchange Format. T. Bray, Ed.. IETF. December 2017. Internet Standard. URL: https://www.rfc-editor.org/rfc/rfc8259

[RFC8615]
Well-Known Uniform Resource Identifiers (URIs). M. Nottingham. IETF. May 2019. Proposed Standard. URL: https://www.rfc-editor.org/rfc/rfc8615

[webidl]
Web IDL Standard. Edgar Chen; Timothy Gu. WHATWG. Living Standard. URL: https://webidl.spec.whatwg.org/

§ C.2 Informative references

[CCPA-AG-FINAL-STATEMENT]
California Attorney General CCPA Final Statement of Reasons. URL: https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-fsor.pdf

[CCPA-REGULATIONS]
CCPA Regulations. URL: https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-final-text-of-regs.pdf?

[COLORADO-REGULATIONS]
Colorado Regulations. URL: https://coag.gov/app/uploads/2023/03/FINAL-CLEAN-2023.03.15-Official-CPA-Rules.pdf

[CPPA-REGULATIONS]
CPPA Regulations. URL: https://cppa.ca.gov/regulations/pdf/cppa_regs.pdf

[EPRIVACY-DIRECTIVE]
Directive 2009/136/EC (ePrivacy Directive). URL: https://edps.europa.eu/data-protection/our-work/publications/legislation/directive-2009136ec_en

[GDPR]
General Data Protection Regulation (GDPR). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN

[Privacy-Principles]
Privacy Principles. Robin Berjon; Jeffrey Yasskin. W3C. URL: https://w3ctag.github.io/privacy-principles/

[SB220]

Nevada SB220 (NRS 603A). URL: https://www.leg.state.nv.us/NRS/NRS-603A.html

↥