Global Privacy Control application for inclusion in Colorado's UOOM registry

1. What is the name of the proposed UOOM?

Global Privacy Control (GPC).

2. What are the names of the individual(s) or organization(s) submitting this application?

This application is being submitted on behalf of Consumer Reports, DuckDuckGo, Robin Berjon (former editor of the GPC spec), Raptive, Digital Content Next,[1] and Sebastian Zimmeck (Assistant Professor of Computer Science, Wesleyan University and GPC co-founder).

3. Please provide a general overview of the UOOM, in plain English.

Global Privacy Control is a browser-level privacy signal designed to allow Internet users to notify businesses of their preference to not have their data be sold or shared, or used for cross-context behavioral advertising. People can activate GPC by toggling a browser privacy setting or installing an extension for their browser.

When people have turned on GPC, the browser or extension will automatically send a signal to each website the user visits broadcasting that user's preference not to have their information sold or shared, or used for cross-context behavioral advertising. A user agent's Global Privacy Control setting is attached to HTTP requests as the Sec-GPC request header. This header's value will be "1" if enabled, and not present otherwise.

4. Please provide the specification for the UOOM.

The Global Privacy Control spec is available at: https://privacycg.github.io/gpc-spec/.

5. What steps would a Consumer have to take to use the UOOM? Please include whether the UOOM will be a default setting for a tool that comes pre-installed with a device.

The GPC specification states that "User agents are expected to convey [a] person['s] 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."[2] It

---

[1] Digital Content Next is the only trade organization dedicated to serving the unique and diverse needs of high-quality digital content companies that manage trusted, direct relationships with consumers and marketers. The organization was founded in June 2001 as the Online Publishers Association (OPA). Its members are listed on its website. *See* Current Members, Digital Content Next, https://digitalcontentnext.org/membership/members/.

[2] Global Privacy Control, World Wide Web Consortium Privacy Community Group GitHub repository (hereinafter "Global Privacy Control Spec"), at §3.1, https://privacycg.github.io/gpc-spec/.

further states: "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."[3] Because GPC is an open-source standard and freely available for companies to use and adapt as they wish, specific decisions about user interfaces are made by implementing user agents.

Several browsers and browser extensions support GPC functionality, including Firefox, Brave, and DuckDuckGo. On Firefox, people can enable GPC via a checkbox in the settings to "[t]ell websites not to sell or share my data." GPC is currently turned on by default in browsers such as Brave and DuckDuckGo, as they are marketed as privacy-preserving browsers or explicitly make people aware of GPC being turned on. None of these browsers come pre-installed with a device. People would make an active choice by downloading and installing them on their devices.
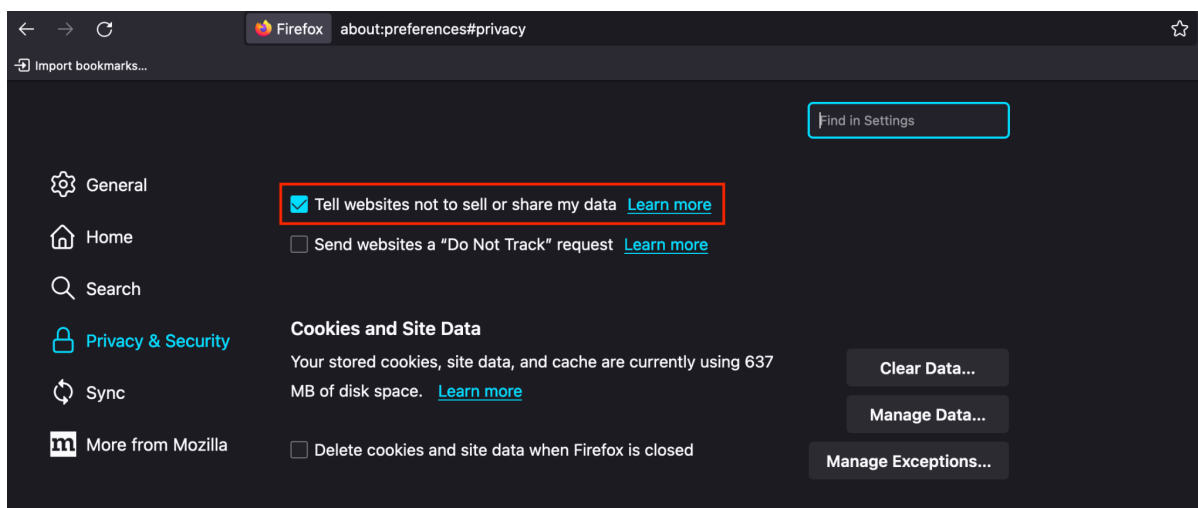
Alternatively, people can download a dedicated browser extension to allow browsers, such as Google Chrome, that do not support GPC natively to send GPC signals.[4] GPC is also enabled by other general-purpose privacy extensions (e.g., Privacy Badger, DuckDuckGo Privacy Essentials), which offer broader functionality in addition to sending GPC requests (e.g., sending Do Not Track requests and blocking trackers). Some browser extensions enable GPC by default while others do not. Some extensions also enable people to make site-by-site choices by only sending GPC to certain sites (or by whitelisting sites as exempted from GPC).

Implementers are able to provide additional information to consumers during the install process or in other documentation. For example, DuckDuckGo states on its Android app store page:

> Signal Your Privacy Preference with Global Privacy Control (GPC) – Built into our app, GPC intends to help you express your opt-out rights automatically by telling

---

[3] Global Privacy Control Spec at §5.1, https://privacycg.github.io/gpc-spec/.
[4] *E.g.*, OptMeowt, OptMeowt GitHub repository, https://github.com/privacy-tech-lab/gpc-optmeowt.

websites not to sell or share your personal information. Whether it can be used to enforce your legal rights (for example, current or future CCPA, GDPR requirements) depends on the laws in your jurisdiction.[5]

6. What steps would a Controller have to take to detect the UOOM?

Global Privacy Control offers an easy method for people to transmit a universal request to opt out in a way that is readily detectable by any website visited by a user. Detecting a GPC signal is easy for a controller to do. GPC is aligned with the structure of the online ad ecosystem thereby reducing controllers' implementation work.

First, a user's GPC status is transmitted by their browser in all outgoing HTTP requests as the Sec-GPC request header. This header's value will be "1" if enabled, and not present otherwise. Additionally, the navigator.globalPrivacyControl DOM property enables a client-side script to determine a user agent's Global Privacy Control setting. This value mirrors the value sent in the Sec-GPC header: it will equal true if the Sec-GPC header sent is equal to "1", and false otherwise.

Controllers can choose whether they want to comply by looking for either header- or DOM-based GPC signals. Sample implementations for both header- and DOM-based GPC detection are available on the Global Privacy Control website.[6]

Once the GPC signal is detected by the controller, it can stop sharing data with third parties, or it can propagate the user-expressed preference downstream to ad networks, analytics services, and other third parties whose code is embedded in the controller's website. In this case, the controller will be relying upon these third parties to comply with the user's GPC instruction. This downstream propagation is not GPC-specific but rather based on the general structure of the online ad ecosystem. One important mechanism to propagate the GPC signal that many websites use is to change consent strings that are used to indicate to third parties that a user has opted out, such as as provided for in the Interactive Advertising Bureau's Global Privacy Platform.[7]

Most if not not all privacy compliance vendors also provide plugin solutions for websites for detecting GPC signals and propagating the signal downstream.[8]

---

[5] DuckDuckGo Private Browser, Google Play Store, https://play.google.com/store/apps/details?id=com.duckduckgo.mobile.android&pli=1.
[6] Interacting with Global Privacy Control, Global Privacy Control, https://global-privacy-control.glitch.me/.
[7] Global Privacy Platform, Interactive Advertising Bureau Github repository, https://github.com/InteractiveAdvertisingBureau/Global-Privacy-Platform.
[8] *See infra* Question 8.

7. When your UOOM is used by a Consumer, how can a Controller determine that the consumer using the UOOM is a Resident of the State of Colorado and that the use represents a legitimate request to opt out of the Processing of Personal Data?

Many companies currently comply with similar location-bounded privacy obligations by approximating geolocation based on IP address.[9] Otherwise, websites and apps would need to institute counterproductively privacy invasive means to establish residency of their users. GPC does not transmit any additional information to controllers about the location of the individuals who have enabled it.

The Department of Law should interpret the Colorado Privacy Act to mean that estimating residency based on IP address is generally sufficient for determining residency and legitimacy for purposes of the CPA, unless the company has a good faith basis to determine that a particular device is not associated with a Colorado resident or is otherwise illegitimate. Further, the Department of Law should interpret the law to mean that additional data processing to confirm residency or legitimacy absent specific evidence to the contrary is prohibited. Without such an interpretation, controllers could respond to each UOOM signal with a request for a driver's license or other means of verification, which would render UOOMs practically unusable and ineffective.[10]

8. What are the costs of use, implementation, and detection of the UOOM by Consumers and Controllers?

GPC is completely free to use for consumers, free for user agents to implement, and is designed to be extremely simple for businesses to detect and process.

The costs to controllers depend mostly on development organization overhead. One company has described that the task of adding GPC support amounted to adding a single line of JavaScript code to an existing "Do Not Sell" feature already required by state law. (In addition to the minimal direct costs of the small amount of code, that company also incurred the ordinary fixed costs of testing and managing any software change.) Another developer has described GPC as "easy and straightforward for us to implement."[11]

---

[9] E.g., Press Release, OneTrust Cookie Consent Upgraded with Recent ICO, CNIL and Country- and State-Specific Guidance Built-in, Aug. 15, 2019, OneTrust, https://www.onetrust.com/news/onetrust-updates-cookie-consent-ico-cnil/.
[10] Initial Comments of Consumer Reports In Response to the Colorado Department of Law's Proposed Draft Rules Interpreting the Colorado Privacy Act by Justin Brookman, Director of Technology Policy, Consumer Reports, Nov. 7, 2022, https://advocacy.consumerreports.org/wp-content/uploads/2022/11/CR-comments-on-initial-CPA-regs-Nov-2022-4.pdf.
[11] Aram Zucker-Scharff, *On the Characteristics of an Effective Consent Signal*, Fight with Tools by AramZS, May 5, 2022, https://aramzs.github.io/written-for-the-washington-post/2022/05/05/comments-to-california-privacy-protection-agency.html.

Most if not all major privacy compliance vendors available to publishers to facilitate legal compliance offer support for GPC. For example, OneTrust, the world's largest privacy compliance platform, has produced a video showing how customers can easily configure their sites to respond differently to GPC in different jurisdictions in less than thirty seconds.[12] Other major compliance vendors also provide clear guidance to customers on how to enable support for GPC signals.[13]

The developers of Global Privacy Control have also authored an implementation guide to provide specific instructions to publishers looking to configure their sites manually to respond to GPC signals.[14]

9. Is the UOOM based on an open system or standard that is free for adoption without permission or on fair, reasonable, and non-discriminatory terms?

Yes, the GPC standard and reference implementation are licensed under the Creative Commons Attribution 4.0 International license.[15]

10. How will personal data collected in connection with the Consumer's utilization of the UOOM be used, disclosed, or retained? Please include whether the UOOM will be used as part of a digital fingerprint.

GPC was designed to allow people to transmit the signal pseudonymously without providing any new information to the user agent (other than a preference to turn on GPC). It is of great importance to browser vendors participating in the design of GPC to keep the device fingerprinting risk as low as possible, which is one reason that GPC was designed to be a binary signal.

We are not aware of any implementations that require consumers to submit additional information before activating the signal. Some jurisdictions, including Colorado, provide that user agents sending GPC requests may not use data associated with transmitting such a

---

[12] Global Privacy Control, Twitter.com, Oct. 20, 2021, https://twitter.com/globalprivctrl/status/1450897561158668290?s=20.
[13] *See*, *e.g.*, Consent Management: Configuring Global Privacy Control, Ethyca, https://docs.ethyca.com/tutorials/consent-management-configuration/global-privacy-control; Global Privacy Control, Transcend.io, https://transcend.io/glossary/global-privacy-control; Ultimate Guide to Preference and Consent Management, and the Global Privacy Control, Wirewheel.io, https://wirewheel.io/blog/ultimate-guide-to-preference-and-consent-management-and-the-global-privacy-control/; Global Privacy Control (GPC), Osano, https://docs.osano.com/global-privacy-controls-gpc.
[14] Aram Zucker-Scharff and Sebastian Zimmeck, *How to Implement Global Privacy Control (GPC) for Publishers*, Global Privacy Control, https://globalprivacycontrol.org/Implementing%20GPC%20for%20Publishers.pdf.
[15] landing-page / LICENSE, Global Privacy Control Github repository, https://github.com/globalprivacycontrol/landing-page/blob/main/LICENSE; reference-server-express / LICENSE, Global Privacy Control Github repository, https://github.com/globalprivacycontrol/reference-server-express/blob/main/LICENSE.

request for other purposes;[16] the GPC spec notes that companies sending GPC are expected to honor legal requirements of jurisdictions recognizing universal opt-out signals.[17]

While people are able to transmit GPC pseudonymously, the scope of their opt out may be limited if the recipient of the signal is unable to associate them with other sessions or information. For example, if a GPC user has not logged into a website's account, the publisher may only be able to apply the opt-out rights to a particular web browsing session, and not more broadly to an account associated with an email address or other persistent identifier. For this reason, some jurisdictions, including Colorado[18] and California[19] have said that publishers may ask consumers sending UOOM signals for optional additional identifying information in order to apply the opt-out more persistently.

While GPC does not substantially increase the device fingerprinting risks, as any additional setting does, it will add some. The GPC developers discuss the issue of fingerprinting in the "Privacy Considerations" section of the spec.[20] It is acknowledged that offering the GPC signal does provide one additional bit of information that could potentially be used by publishers to fingerprint an individual. However, given the potential benefits to users in being able to take advantage of legal or optional opt-out rights, the developers considered the privacy benefits of offering the signal to outweigh the potential fingerprinting risk.

11. Has the UOOM been adopted by Consumers or Controllers?

Global Privacy Control is currently transmitted by a number of user agents including the Brave Browser, DuckDuckGo Privacy Browser, Privacy Badger by the Electronic Frontier Foundation, Firefox by Mozilla, OptMeowt by privacy-tech-lab, Abine, lockrmail by lockr, and Disconnect.me.[21] We conservatively estimate at least 75 million daily users, though that number is very likely considerably higher. Mozilla recently announced its intention to surface Global Privacy Control in Firefox's native privacy settings starting with Firefox version 120.[22]

Further, regulators in California have stated that companies covered by the CPPA (defined as companies that meet any of the following criteria: (1) more than $25 million in annual revenue, (2) buys or shares the information of over 100,000 California consumers, or (3) generates at

---

[16] CPA Rules, Rule 5.05(a), https://coag.gov/app/uploads/2023/03/FINAL-CLEAN-2023.03.15-Official-CPA-Rules.pdf

[17] Global Privacy Control Spec at §5.1, https://privacycg.github.io/gpc-spec/.

[18] CPA Rules, Rule 5.05(c), https://coag.gov/app/uploads/2023/03/FINAL-CLEAN-2023.03.15-Official-CPA-Rules.pdf.

[19] CCPA Rules, Section 7025 (c)(2), https://cppa.ca.gov/regulations/pdf/cppa_regs.pdf.

[20] Global Privacy Control Spec at §6, https://privacycg.github.io/gpc-spec/.

[21] Global Privacy Control, https://globalprivacycontrol.org/#orgs.

[22] Benjamin VanderSloot, "Intent to Ship: Global Privacy Control," dev-platform@mozilla.org Google Group, Oct. 27, 2023, https://groups.google.com/a/mozilla.org/g/dev-platform/c/373F82Jzcjs/m/ImZKgRNIAQAJ?pli=1.

least half of its revenue from sharing personal information) are required to detect and honor GPC signals as legally binding opt-out requests for California users.[23]

12. Has the UOOM been approved or is being actively considered by a widely recognized, legitimate standards body after multistakeholder participation in the standards-making process? If so, which?

The GPC is currently a work item for the World Wide Web Consortium's Privacy Community Group.[24]

13. Which individuals and organizations have been involved in developing the UOOM?

The original founding organizations of Global Privacy Control project are: Abine, Automattic (WordPress), Brave, Consumer Reports, Disconnect, DuckDuckGo, the Electronic Frontier Foundation, Meredith, Mozilla, the New York Times, Raptive (formerly known as CafeMedia), The Washington Post, and Wesleyan University.[25]

The current editors of the GPC specification are: Aram Zucker-Scharff (The Washington Post), Justin Brookman (Consumer Reports), Sebastian Zimmeck (Wesleyan University), and Peter Synder (Brave). Ashkan Soltani (independent), Robin Berjon (New York Times), and Dave Harbage (DuckDuckGo) are former editors of the GPC spec.[26]

14. How did you solicit and consider stakeholder input while developing the UOOM and/or this application?

Organizations involved in developing the GPC spec have informally consulted a wide range of stakeholders including publishers, ad tech providers, browser vendors, academics, civil society organizations, and regulators in the process of creating and revising the GPC spec. The spec was first published for public input on GitHub on October 7, 2020.[27]

---

[23] *See infra* Question 17. CCPA, §1798.140(d)(1), https://thecpra.org/#1798.140(d).
[24] World Wide Web Consortium Privacy Community Group GitHub repository, https://github.com/privacycg/.
[25] Global Privacy Control, https://globalprivacycontrol.org/#orgs.
[26] Global Privacy Control Spec at §5.1, https://privacycg.github.io/gpc-spec/.
[27] initial commit, Global Privacy Control Github repository, https://github.com/privacycg/gpc-spec/commit/c704b868a74ee9e3bb30b2ba137a4680b760ea13#diff-0eb 547304658805aad788d320f10bf1f292797b5e6d745a3bf617584da017051.

As part of the standardization process of GPC at the W3C, every interested person has the ability to participate in the discussion and development of GPC in written form[28] or in calls of the Privacy Community Group.[29]

15. Which stakeholders provided input on the UOOM?

The GPC GitHub page identifies fourteen unique contributors to the GPC codebase, as well as 38 raised issues (31 of which have been discussed and resolved)[30] and 19 pull requests (specific proposed suggested changes to the specification), of which only one is currently outstanding.[31] The W3C Privacy Community Group currently has 528 participants, many of whom have participated in discussions of GPC on regular community group calls.[32]

Global Privacy Control had early input and testing from Raptive, on behalf of about 4,000 mostly small independent websites, whose operators need to comply with privacy law while minimizing development and administrative costs.

Most stakeholders have implemented GPC on their own without providing explicit feedback to the GPC developers.

16. Is the UOOM likely to comply with the requirements of other jurisdictions that recognize universal opt-out mechanisms or signals by law?

We believe that GPC is likely to comply with the requirements of all other US jurisdictions that currently provide for universal opt-out mechanisms. First, as discussed below, California regulators have explicitly stated that GPC transmits legally binding opt-out requests under the California Consumer Privacy Act.[33]

Other states that have recently enacted privacy legislation with explicit provision for universal opt-out mechanisms include Connecticut, Montana, Texas, Delaware, and Oregon, though those statutes all give implementers additional time to adapt before becoming effective over the next few months and years. Texas's universal opt-out provision has a reciprocity clause stating that covered controllers must respond to universal opt out signals if they "process similar or

---

[28] *E.g.*, privacycg / proposals, Standardizing Global Privacy Control (GPC) #10, Global Privacy Control GitHub repository, Apr. 6, 2020, https://github.com/privacycg/proposals/issues/10/.

[29] *E.g.*, privacycg / agendas, 26 October 2023 Privacy CG Teleconference, https://github.com/privacycg/meetings/blob/a0d9d9ba04d40eaf5d630745b202aecaa144b19a/2023/telcons/10-26-agenda.md.

[30] privacycg / gpcspec, Issues, https://github.com/privacycg/gpc-spec/issues.

[31] privacycg / gpcspec, Pull Requests, https://github.com/privacycg/gpc-spec/pulls.

[32] Privacy Community Group, World Wide Web Consortium, https://www.w3.org/community/privacycg/.

[33] *See infra* Question 17.

identical requests the controller receives from consumers for the purpose of complying with similar or identical laws or regulations of another state."[34]

Other state UOOM provisions are textually very similar to Colorado's. For example, other state laws mirror Colorado's requirements that UOOMs not "unfairly disadvantage" certain controllers or not be enabled by default.[35] Further, other state UOOM provisions often explicitly state that regulators should strive to interpret them to be consistent with other states' interpretations of comparable laws.[36] Other states besides Colorado and California do not explicitly provide for interpretive rulemaking, so there may be ambiguity about which UOOM signals are deemed binding until those states' attorneys general take enforcement action or otherwise informally signal support for a particular UOOM.

17. Has the UOOM already been recognized by any jurisdiction?

Global Privacy Control has been recognized as a valid and legally binding opt out in California since at least January 28, 2021.[37] California regulators have since published FAQs clarifying that GPC signals must be interpreted as opt-out requests in California,[38] and brought an enforcement action against Sephora for failing to treat GPC signals as opt-out requests.[39] As part of the Final Judgment and Permanent Injunction, Sephora agreed: "DEFENDANT shall process CONSUMER requests to opt out signaled via the Global Privacy Control or the 'GPC.'"[40]

18. Is the UOOM flexible, especially in light of changing user preferences, business model changes, and shifts in the laws of other regulations?

---

[34] Texas Data Privacy and Security Act, Section 541.055 (e)(4), https://capitol.texas.gov/tlodocs/88R/billtext/pdf/HB00004F.pdf#navpanes=0.

[35] See, e.g., Connecticut Data Privacy Act, Section 6 (e)(1)(A)(ii)(I), https://www.cga.ct.gov/2022/act/Pa/pdf/2022PA-00015-R00SB-00006-PA.PDF; Montana Consumer Data Privacy Act, Section 6(3)(b)(i), https://leg.mt.gov/bills/2023/billpdf/SB0384.pdf.

[36] See, e.g., Oregon Consumer Privacy Act, Section 12, Sec. 5 (5)(c)(A), https://olis.oregonlegislature.gov/liz/2023R1/Downloads/MeasureDocument/SB619/Enrolled; Delaware Personal Data Privacy Act, Section 12D-106 (e)(1)(a)(2)(D), https://legis.delaware.gov/json/BillDetail/GenerateHtmlDocumentEngrossment?engrossmentId=35877&docTypeId=6.

[37] Archive - Attorney General Becerra, Twitter.com, Jan. 28, 2021, https://twitter.com/AGBecerra/status/1354850758236102656.

[38] Frequently Asked Questions, California Privacy Protection Agency, at 8.How to Submit Requests, https://cppa.ca.gov/faq.html.

[39] Press Release, *Attorney General Bonta Announces Settlement with Sephora as Part of Ongoing Enforcement of California Consumer Privacy Act*, State of California Department of Justice, Aug. 24, 2022, https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-settlement-sephora-part-ongoing-enforcement.

[40] Final Judgment and Permanent Injunction, *California v. Sephora, USA, Inc.*, CGC-22-601380, Aug. 24, 2022, https://oag.ca.gov/system/files/attachments/press-docs/Filed%20Judgment.pdf.pdf.

Yes, GPC is not statute-specific and designed to apply to different privacy laws that afford individuals the right to express a preference for a single data controller and to not have data shared or used across different contexts.

19. What is the scope of the UOOM? a. Does the UOOM function with phones, computers, and/or any other devices? Does the UOOM provide just one opt out right as opposed to both?

Global Privacy Control was initially developed for web browsers because of the relative ease of development and implementation. However, the basic syntax could easily be transported to other environments such as mobile operating systems, payment services, and other Internet of Things platforms.

Global Privacy Control is designed to be sent pseudonymously, so it may only apply to the immediate context if the controller is unable to associate a person with a particular account. However, if a user is logged in or otherwise authenticated to the controller, the controller should apply the GPC instruction universally for that individual.[41]

Global Privacy Control was developed to allow people to express a preference for a single controller and to not have their data sold, shared, or used across different contexts. The introduction to the GPC spec specifically states:

> 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.[42]

As such, GPC should be deemed to invoke both of Colorado's opt-out rights: the right to opt out of sale and the right to opt out of targeted advertising (defined as advertising targeted based on activity across nonaffiliated websites, applications, or other contexts).

In general, UOOMs should be interpreted as invoking both rights, unless an UOOM is specifically promoted as limited to just one opt-out right. This would allow Colorado's law to be interoperable with California and other jurisdictions that offer consumers slightly different formulations of legal rights.[43]

---

[41] *See supra* Question 10.
[42] Global Privacy Control Spec at §1, https://privacycg.github.io/gpc-spec/.
[43] Initial Comments of Consumer Reports In Response to the Colorado Department of Law's Proposed Draft Rules Interpreting the Colorado Privacy Act by Justin Brookman, Director of Technology Policy, Consumer Reports, Nov. 7, 2022, https://advocacy.consumerreports.org/wp-content/uploads/2022/11/CR-comments-on-initial-CPA-regs-Nov-2022-4.pdf.

20. Has the UOOM been vetted by expert reviewers? Has it been tested in laboratory or real world environments? a. If yes, please share the results of any tests or reviews.

Global Privacy Control has been deployed by user agents since September 2020 and has been recognized as legally binding in at least California since January 2021.[44] It has been vetted through the widespread implementation, informal consultation with stakeholders, open source collaboration, and W3C standardization process described in response to Questions 13-15 above.

Research on Global Privacy Control suggests that a large percentage of people would make use of it. In a usability survey 94% of the participants would turn on GPC. Further, 81% of the participants had a correct understanding of what GPC does ensuring that their intent is accurately represented by their choice.[45]

GPC settings and user interfaces can be implemented such that people only perceive minimal disruption, thus avoiding the usability problems of cookie choice interfaces. This is even true for site-by-site choices, which can be generalized from one site towards all sites visited in the future.[46]

21. Are there any additional factors that you would like the Attorney General to consider in reviewing your UOOM application?

We are happy to answer any questions or provide any additional documentation that would be useful. Please feel free to contact Justin Brookman at justin.brookman@consumer.org for additional information.

---

[44] *See supra* Question 17.
[45] Zimmeck et al, *Usability and Enforceability of Global Privacy Control*, Privacy Enhancing Technologies Symposium, 2023, https://petsymposium.org/popets/2023/popets-2023-0052.php.
[46] Zimmeck et al, Generalizable Active Privacy Choice: Designing a Graphical User Interface for Global Privacy Control, Privacy Enhancing Technologies Symposium, 2024, https://petsymposium.org/popets/2024/popets-2024-0015.php.