

August 3, 2026

The Honorable Rob Bonta
Attorney General, State of California

The Honorable Phil Weiser
Attorney General, State of Colorado

The Honorable Kathy Jennings
Attorney General, State of Delaware

The Honorable Austin Knudsen
Attorney General, State of Montana

The Honorable John Formella
Attorney General, State of New Hampshire

The Honorable Ken Paxton
Attorney General, State of Texas

The Honorable Jennifer M. Urban
Chair, California Privacy Protection Agency Board

The Honorable William Tong
Attorney General, State of Connecticut

The Honorable Anthony G. Brown
Attorney General, State of Maryland

The Honorable Mike Hilgers
Attorney General, State of Nebraska

The Honorable Jennifer Davenport
Attorney General, State of New Jersey

Dear Attorneys General and Chair Urban:

I want to begin by applauding your states for enacting important laws providing consumers with powerful privacy protections against tracking on the internet. Your legislatures have taken a monumental step toward rebalancing the scales of digital privacy in favor of everyday consumers. Now that these critical legal frameworks are in place, my goal is to partner with your offices to ensure that tens of millions of Americans receive the privacy protections to which they are entitled.

Your states have all enacted privacy laws that enable your residents to use universal opt-out mechanisms like Global Privacy Control (GPC) that are built into some, and soon all, web browsers to protect their personal information. However, many companies are undermining these rights by relying on flawed geolocation data to selectively ignore consumer opt-out requests. I write to urge you to issue clear guidance directing businesses to fully recognize and honor GPC privacy signals from your residents, and to take collective action to address these practices.

GPC is a technology that allows consumers to protect themselves from tracking by automatically notifying each website they access of their privacy choices, specifically opting out of the sale or sharing of their personal data. To date, the comprehensive privacy laws of a dozen states—including each of your states—provide consumers with the right to use a universal opt-out mechanism. Several of your states have explicitly recognized GPC as an approved opt-out technology. As the author of the Mind Your Own Business Act—which in 2019 proposed a mandatory, one-click universal opt-out—I have long championed GPC as a vital, common-sense tool for consumer autonomy and national security.

While some of the largest companies in America honor GPC signals from all visitors to their websites, other companies have chosen to honor GPC signals only from users they believe are physically located in states that require compliance. These companies rely on commercial GeoIP databases to guess a user's location based on their IP address and deduce which state laws apply. This practice deprives consumers of their rights under your states' laws: GeoIP databases are notoriously inaccurate and, even where this data is accurate, a user's temporary physical location does not dictate their state of residence and, consequently, does not dictate the extent of their privacy rights.

Ignoring a GPC signal based on a temporary out-of-state location unlawfully deprives consumers of their statutory rights. This practice strips away the rights of mobile populations, including out-of-state college students, business travelers, and interstate commuters. This practice also disproportionately affects military personnel who are residents of your states, but deployed or stationed away from home. For years, foreign adversaries have actively exploited commercial adtech data to surveil, profile, and target American service members. Companies that ignore GPC signals on this basis not only silently strip service members of their privacy rights, but also harm our national security. In addition, this practice leads many companies to ignore GPC signals from consumers using commercial Virtual Private Networks (VPNs) to protect their privacy. The IP address for such a user will appear to websites as that of the VPN server, which may be located in a jurisdiction without the same privacy rights. Because VPNs are heavily favored by the very privacy-conscious consumers most likely to seek out and enable GPC, relying on GeoIP filtering perversely punishes the exact residents who are more likely to exercise their rights under your states' laws.

As you know, state privacy rights do not vanish when residents temporarily cross state lines or when they use common tools like VPNs to protect their online privacy. For example, staff from the California Privacy Protection Agency have confirmed to my office that California consumers retain their rights under California's privacy law, including the right to opt out using GPC, regardless of where they are physically located. California's privacy regulations explicitly prohibit businesses from requiring identity verification for opt-outs—leaving companies liable if they disregard a California resident's GPC signal. Consequently, the most practical compliance path for businesses is to honor all GPC signals, rather than gambling on a user's residency. I urge your offices to establish a similarly clear posture to ensure your residents are not left unprotected.

Furthermore, not only are companies denying consumers the privacy rights to which they are entitled under state law, but they often do so in secret. Under California's privacy regulations, businesses are required to

display whether they have processed the consumer's opt-out preference signal as a valid request to opt out—such as through an "Opt-Out Request Honored" badge. However, businesses often only display the badge when the GPC signal is successfully processed and not when they disregard the signal. This asymmetric disclosure effectively morphs a transparency rule into a cloaking device for non-compliance. It creates a classic "dark pattern" where Americans are forced to guess their privacy status based entirely on the absence of a notice, leaving them completely oblivious to the fact that their privacy rights have been silently violated. My office has made some progress addressing this problem through recent oversight into major Consent Management Platforms (CMPs). These services are used by many businesses to manage their websites' compliance with privacy laws and provide pre-packaged functionality to respect or selectively ignore GPC based on the user's IP address. Some CMPs are already doing the right thing. Osano, Usercentrics, and Transcend told my office that they honor GPC signals from all users, regardless of their IP address. After engaging with my staff, Transcend also agreed to add a new, optional feature by the end of the year allowing customers to automatically classify visitors originating from U.S. government and military IP addresses as high-sensitivity users, instantly applying their most privacy-preserving protections.

In contrast, many other CMPs selectively ignore GPC signals from users based on their IP address, if configured to do so by a customer. Following conversations with my staff, OneTrust confirmed plans to provide a clear visual notification when a consumer's GPC signal is rejected. Furthermore, in the event OneTrust suspects a user is out-of-state, the platform will prompt users to affirm their residency, rather than silently rejecting the GPC signal. Ketch—which currently honors GPC by default for IP addresses associated with legally required states—has agreed to roll out new privacy features by the end of the year that will be enabled by default. Ketch will display a visual indicator when a GPC signal is disregarded and will provide overrides allowing consumers to correct their inaccurately inferred location or manually assert their true state residency. Finally, TrustArc has agreed to update the default configuration for clients who operate in states that enforce GPC or deploy a nationwide CMP banner. In both cases, TrustArc will include a GPC setup process, which, once completed, will honor GPC preferences. In addition, TrustArc has agreed to develop capabilities to automatically treat traffic from U.S. government and military IP addresses as if they come from California. TrustArc has also agreed to develop two optional features for clients: (a) a state-of-residency selector to allow consumers to manually correct a misidentified location and; (b) a visual indicator to inform users that a site honors GPC but the user has not enabled it.

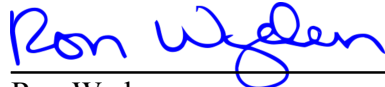
Several state privacy statutes explicitly tie a business's obligation to honor universal opt-out signals to what can be determined through "commercially reasonable" efforts. However, the technical commitments my office has secured from these CMPs undermine any claim that compliance beyond automated GeoIP tracking is unworkable. By deploying simple self-certification prompts and clear status indicators, these platforms prove that commercially reasonable mechanisms to verify residency and honor GPC signals exist today—rendering the practice of silently ignoring consumer requests based on GeoIP data entirely inexcusable.

Ultimately, addressing this systemic evasion of consumer privacy rights requires a coordinated response. I encourage you to issue public guidance to businesses clarifying that you expect companies to respect the GPC signals sent by your residents, regardless of their physical location or IP address—including when they

are using a VPN to protect their privacy. This guidance should inform businesses that selectively ignoring GPC signals based on IP address is impermissible unless they clearly notify users and provide them with a frictionless way to self-certify their true residency. I further urge your offices to establish a bipartisan, multistate Attorney General task force specifically dedicated to joint enforcement of GPC signals. A unified coalition of state regulators issuing joint investigative demands and coordinated compliance notices will send an unmistakable message: geographic filtering is a collective enforcement trigger, not a clever legal loophole.

Thank you for your attention to this important matter. If you have any questions about this request, please contact Chris Soghoian and Shreyas Gandlur in my office.

Sincerely,



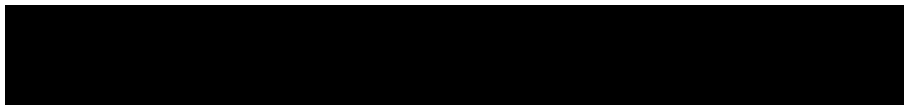
Ron Wyden
United States Senator

MEMORANDUM

July 31, 2026

To: Senator Ron Wyden
Attention: Chris Soghoian, Senior Advisor

From:



Subject: State Privacy Law and the Global Privacy Control

This memorandum¹ responds to your request for analysis on state privacy laws and the Global Privacy Control (GPC), a mechanism that allows consumers to send opt-out signals through their web browser.² The memorandum begins by providing an overview of GPC and how it functions. The memorandum next summarizes state privacy laws and the extent to which they require businesses to recognize GPC signals. The memorandum also explains how certain states enforce such requirements. The memorandum then discusses the extent to which businesses' obligations to respect GPC signals depend on their ability to identify whether consumers are residents of a particular state. The memorandum considers certain "edge cases" where a consumer's residence does not correspond to an Internet Protocol (IP) address of an online device the consumer used. It further considers whether it is "commercially reasonable" for a company to reject a GPC signal because an IP geolocation database used by the company indicates that the IP address of the consumer's device is not located in a state that requires compliance with GPC signals. The memorandum next considers the extent to which state privacy laws permit browsers to turn on GPC by default. Finally, the memorandum considers potential barriers to the adoption of GPC. CRS remains available to follow up in person or remotely, at your convenience.

Overview of the Global Privacy Control (GPC)

GPC is a draft technical standard developed by the Privacy Working Group of the World Wide Web Consortium (W3C). GPC provides a mechanism for user-agents³—that is, a computer program representing an individual, such as a web browser—to notify websites of the user's privacy preferences,

¹ Information in this memorandum is drawn from publicly available sources and may be of general interest to Congress. CRS may provide all or part of this information in memoranda or reports for general distribution to Congress. If so, CRS will preserve your confidentiality as a requester.

² This memorandum is an update to a previous version dated February 25, 2026.

³ *User Agent*, MOZILLA: MDN (June 11, 2025), https://developer.mozilla.org/en-US/docs/Glossary/User_agent [<https://perma.cc/3GZ8-A3BE>].

such as opting out of sharing the user's data with third parties.⁴ If a user's web browser supports GPC, the web browser can send GPC signals to a website as an HTTP header⁵ and an object that can be coded in the programming language of JavaScript and processed on a website server.⁶ Because web browsers can be used to visit any website, when GPC becomes an add-on feature within a web browser, the user can use GPC as a universal opt-out mechanism (UOOM) rather than providing privacy preferences to each website he or she visits through the browser. Users can choose to enable GPC for all websites or for certain websites specified by the user; users may also choose to disable GPC.⁷ GPC was first published on November 21, 2024⁸ and last updated on February 3, 2026.⁹

GPC allows users to indicate whether or not they want their personal data to be shared or sold.¹⁰ It is not designed to address every privacy right provided by comprehensive data privacy laws enacted by states.¹¹ For example, GPC does not allow users to request that their personal data be deleted from websites.¹² It also does not limit the use of personal information by the website a user visits; for example, GPC would not prevent a website from offering targeted ads to the user based on the user's previous activities on that website.¹³ GPC might enable additional information for browser or device fingerprinting, that is, identifying and tracking a user based on the specific properties of a web browser or device.¹⁴

Some web browsers on computers and mobile devices have incorporated GPC. For example, the web browser DuckDuckGo has enabled GPC as the default setting on its mobile applications (apps) and desktop browser extensions;¹⁵ Firefox and Brave allow users to enable GPC under their program settings; and Google Chrome and Microsoft Edge allow users to download an extension or add-on onto their desktop to enable GPC.¹⁶ Some organizations have developed browser extensions that can be used to enable GPC.¹⁷ For example, Electronic Frontier Foundation has developed a browser extension that can

⁴ A *web browser* is a piece of software installed on a computer or mobile device, which enables the user to access information hosted on a website. Google Chrome, Microsoft Edge, and Apple Safari are among the most commonly used web browsers.

⁵ An *HTTP header* is a field of an HTTP request or response (e.g., a request to provide information on a website) from the browser to a website's server that passes additional information about the request or response. For more information, see *HTTP Header*, MOZILLA: MDN (Dec. 21, 2025), <https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers> [<https://perma.cc/D8P7-AMXM>].

⁶ *Working with Objects*, MOZILLA: MDN (Dec. 21, 2025), https://developer.mozilla.org/en-US/docs/Web/JavaScript/Guide/Working_with_objects [<https://perma.cc/8ERT-VHEA>]; and *GPC Legal and Implementation Considerations Guide*, WORLD WIDE WEB CONSORTIUM (W3C), <https://w3c.github.io/gpc/explainer> [<https://perma.cc/685S-BWAX>] (last visited July 30, 2026).

⁷ *GPC Legal and Implementation Considerations Guide*, *supra* note 6.

⁸ *Global Privacy Control (GPC) Publication History*, W3C, <https://www.w3.org/standards/history/gpc/> [<https://perma.cc/Z7JN-X6VN>] (last visited July 30, 2026).

⁹ W3C, *GLOBAL PRIVACY CONTROL (GPC) (editor's draft, June 11, 2026)*, <https://w3c.github.io/gpc/> [<https://perma.cc/8546-GMZD>].

¹⁰ *Frequently Asked Questions*, GLOB. PRIV. CONTROL, <https://globalprivacycontrol.org/faq> [<https://perma.cc/T6MK-S5JM>] (last visited July 30, 2026); *GPC Legal and Implementation Considerations Guide*, *supra* note 6.

¹¹ *GPC Legal and Implementation Considerations Guide*, *supra* note 6.

¹² *Id.*

¹³ *Id.*

¹⁴ W3C, *supra* note 8. For more information on browser or device fingerprinting, see CRS Report R47298, *Online Consumer Data Collection and Data Privacy*, by Clare Y. Cho and Ling Zhu (2022).

¹⁵ *Global Privacy Control (GPC) Enabled by Default in DuckDuckGo Apps & Extensions*, DUCKDUCKGO NEWS, (Jan. 28, 2021), <https://spreadprivacy.com/global-privacy-control-enabled-by-default/> [<https://perma.cc/U7SY-MMQ4>].

¹⁶ *Fly Your Privacy Flag with Global Privacy Control*, GLOB. PRIV. CONTROL, https://globalprivacycontrol.org/GPC_for_Users.pdf [<https://perma.cc/35R2-M2KL>] (last visited July 30, 2026); *Frequently Asked Questions*, *supra* note 10.

¹⁷ *Fly Your Privacy Flag with Global Privacy Control*, *supra* note 16; W3C, *supra* note 8.

be downloaded onto users' devices and added to the Firefox and Edge browsers available on desktops and the Android mobile platform.¹⁸

CRS did not find instances of mobile apps other than web browsers incorporating GPC. Developers could incorporate GPC into other mobile apps, which could affect a user's privacy settings within the app. To affect privacy settings across all apps on a mobile device, GPC would need to be incorporated in the operating system of the mobile device.

A GPC signal can potentially conflict with the privacy preference a user has previously indicated on a website. For example, a user might have agreed to allow a website to use their data for targeted advertising from third parties, but then that user enabled GPC for all websites. The GPC states that websites should look to the applicable state comprehensive privacy law to determine how to address conflicting privacy preferences from users.¹⁹

State Comprehensive Privacy Laws and GPC

In recent years, an increasing number of states have adopted comprehensive privacy laws that govern how a broad range of businesses handle most individual consumer information.²⁰ These laws typically allow consumers to obtain a copy of their personal data held by businesses, correct inaccuracies in their personal data, and request that businesses delete their personal data.²¹ Most relevantly, these laws require businesses to let consumers opt-out of the sale of their personal data.²²

The comprehensive privacy laws of at least fifteen states—in order of enactment, California,²³ Colorado,²⁴ Connecticut,²⁵ Montana,²⁶ Texas,²⁷ Oregon,²⁸ Delaware,²⁹ New Jersey,³⁰ New Hampshire,³¹ Maryland,³² Nebraska,³³ Minnesota,³⁴ Alabama,³⁵ Louisiana,³⁶ and Vermont³⁷—allow consumers to use UOOMs to

¹⁸ *Privacy Badger*, ELEC. FRONTIER FOUND., <https://privacybadger.org/> [<https://perma.cc/JB5U-JRBY>] (last visited July 30, 2026).

¹⁹ *GPC Legal and Implementation Considerations Guide*, *supra* note 6.

²⁰ For further discussion of these laws and their requirements, see CRS Report R48667, *Preemption and Privacy Law*, by Chris D. Linebaugh (2025).

²¹ *See, e.g.*, VA. CODE ANN. § 59.1-577 (West 2025); COLO. REV. STAT. § 6-1-1306 (2025); TEX. BUS. & COM. CODE ANN. § 541.051 (West 2025).

²² *See, e.g.*, CAL. CIV. CODE § 1798.120 (West 2025); COLO. REV. STAT. § 6-1-1306(1)(a)(B); TEX. BUS. & COM. CODE ANN. § 541.051(b)(5)(B).

²³ CAL. CIV. CODE §§ 1798.135(b), 1798.185(a)(18) (West 2025); CAL. CODE REGS. tit. 11, § 7025 (2026).

²⁴ COLO. REV. STAT. §§ 6-1-1306(1)(a), 6-1-1313 (2025); 4 COLO. CODE REGS. §§ 904-3:5.01–904-3:5.09 (2025).

²⁵ CONN. GEN. STAT. § 42-519 (2025).

²⁶ MONT. CODE ANN. § 30-14-2809 (West 2025).

²⁷ TEX. BUS. & COM. CODE § 541.055(e) (West 2025).

²⁸ OR. REV. STAT. §§ 646A.576, 646A.578 (2025).

²⁹ DEL. CODE ANN. tit. 6, § 12D-105 (West 2025).

³⁰ N.J. STAT. ANN. § 56:8-166.11 (West 2025).

³¹ N.H. REV. STAT. ANN. §§ 507-H:5, 507-H:6V (West 2025).

³² MD. CODE ANN., COM. LAW §§ 14-4706, 14-4707(f) (West 2025).

³³ NEB. REV. STAT. § 87-1111 (2025).

³⁴ MINN. STAT. ANN. § 325M.14 (West 2025).

³⁵ Alabama Personal Data Protection Act, Act. 2026 Ala. Acts 55 § 6 (2026).

³⁶ Louisiana Personal Data Protection Act, Act. No. 2026 La. Acts 502 (to be codified at LA. R.S. 51:1778).

³⁷ Vermont Data Privacy and Online Surveillance Act, 2026 Vt. Acts & Resolves No. 145 (to be codified at Vt. Stat. Ann. tit. 9, § 2415e).

opt-out of the sale of their data.³⁸ These laws typically say that consumers may use a browser setting or extension, or a global setting on an electronic device, to designate an authorized agent to opt-out on their behalf.³⁹

These laws require the UOOMs to meet certain requirements. Namely, these laws typically require that the UOOMs (1) not unfairly disadvantage another business, (2) not make use of a default setting but instead require the consumer to make an “affirmative, freely given, and unambiguous choice” indicating their intent to opt-out; and (3) be “consumer-friendly” and “easy to use by the average consumer.”⁴⁰ Most of the laws do not require businesses to comply with UOOM signals if the business is not able to verify, with “commercially reasonable effort,” the identity of the consumer and that the agent is authorized to act on the consumer’s behalf.⁴¹ Some state laws provide additional exceptions, such as when the UOOM signal is not communicated in a “clear and unambiguous manner” or when the covered entity “lacks the ability to process the request.”⁴²

To the extent a UOOM signal conflicts with a consumer’s existing privacy setting or voluntary participation in a loyalty or other program, these laws typically require the business to comply with the UOOM signal but allow the business to notify the consumer of the conflict and give the consumer an opportunity to confirm their existing privacy setting or participation in the program.⁴³

While most state privacy laws do not give rulemaking authority to any state agency, California’s and Colorado’s laws require the California Privacy Protection Agency (CPPA) and the Colorado Attorney General, respectively, to issue UOOM regulations.⁴⁴ The CPPA and Colorado Attorney General’s regulations provide additional detail on the technical requirements of UOOMs and on companies’ obligations.⁴⁵ For example, both states’ regulations specify that a UOOM signal shall be in a commonly used and recognized format, such as an “HTTP header field or JavaScript object.”⁴⁶ Both state regulations further specify that, when a consumer previously utilized a UOOM, businesses may not interpret the subsequent absence of a UOOM signal as consent to opt back in to the selling of their data.⁴⁷ California’s regulations further require businesses to display whether they have processed consumers’ UOOM signals. For example, businesses may display on their website “Opt-out Request Honored” and may display a consumer’s opt-out preference through a “toggle or radio button.”⁴⁸

While GPC is not specifically mentioned in any state comprehensive privacy laws or implementing regulations, several state agencies have expressly recognized GPC as a valid UOOM. The California

³⁸ Vermont Data Privacy and Online Surveillance Act, 2026 Vt. Acts & Resolves No. 145 (to be codified at Vt. Stat. Ann. tit. 9, § 2415e).

³⁹ See, e.g., CONN. GEN. STAT. § 42-519 (2025); TEX. BUS. & COM. CODE § 541.055(e) (West 2025); MD. CODE ANN., COM. LAW § 14-4706(a)(2).

⁴⁰ See, e.g., TEX. BUS. & COM. CODE § 541.055(f); COLO. REV. STAT. § 6-1-1313 (2025); MONT. CODE ANN. § 30-14-2809(3) (West 2025); see also CAL. CIV. CODE § 1798.185(a)(18) (West 2026).

⁴¹ See, e.g., TEX. BUS. & COM. CODE § 541.055(e); N.J. STAT. ANN. § 56:8-166.11 (West 2025); MD. CODE ANN., COM. LAW § 14-4706(b); NEB. REV. STAT. § 87-1111(5) (2025).

⁴² See TEX. BUS. & COM. CODE § 541.055(e)(2)–(3); NEB. REV. STAT. § 87-1111(5)(a), (c).

⁴³ See, e.g., CONN. GEN. STAT. § 42-520(e)(1)(B) (2025); MONT. CODE ANN. § 30-14-2809(4); DEL. CODE ANN. tit. 6, § 12D-106(e)(1) (West 2025); see also CAL. CODE REGS. tit. 11, § 7025(c)(3)–(4) (2026) (providing more granularity on businesses’ obligations depending on whether the UOOM request conflicts with an existing privacy setting or a financial incentive program).

⁴⁴ CAL. CIV. CODE § 1798.185(a)(18); COLO. REV. STAT. § 6-1-1313 (2025). New Jersey’s privacy law allows, but does not require, the Division of Consumer Affairs in the Department of Law and Public Safety to issue UOOM regulations. N.J. STAT. ANN. § 56:8-166.11 (West 2025).

⁴⁵ CAL. CODE REGS. tit. 11, § 7025 (2026); 4 COLO. CODE REGS. §§ 904-3:5.01–904-3:5.09 (2025).

⁴⁶ CAL. CODE REGS. tit. 11, § 7025(b)(1); 4 COLO. CODE REGS. § 904-3:5.06.

⁴⁷ CAL. CODE REGS. tit. 11, § 7025(c)(5); 4 COLO. CODE REGS. § 904-3:5.09.

⁴⁸ CAL. CODE REGS. tit. 11, § 7025(c)(6).

Attorney General’s website states that GPC is an “acceptable method” for consumers to opt-out of the sale of their information and that GPC signals “must be honored by covered businesses.”⁴⁹ Colorado’s Attorney General, which is obligated to keep a public list of recognized UOOMs, lists GPC as the only UOOM currently recognized under Colorado law.⁵⁰ The Connecticut Attorney General’s website also references GPC as an example of a UOOM that consumers can use, and it links to videos explaining the GPC to consumers and businesses.⁵¹ The websites of the Oregon Attorney General and the New Jersey Division of Consumer Affairs likewise both list GPC as an example of a UOOM that consumers may use to exercise their opt-out rights.⁵²

Enforcement of State UOOM Requirements

Violations of state UOOM requirements may result in civil enforcement actions. Most state comprehensive privacy laws give exclusive enforcement authority to the state’s attorney general.⁵³ These laws typically authorize the state attorney general to seek up to \$7,500 in penalties per violation.⁵⁴ Others provide that violations constitute violations of state consumer protection statutes, thus incorporating the penalties from those statutes.⁵⁵ California’s enforcement framework is distinct in that enforcement authority is shared between the state attorney general and the CPPA.⁵⁶ California’s law authorizes the Attorney General to bring civil suits and it empowers the CPPA to pursue administrative enforcement.⁵⁷ Both civil suits and administrative enforcement actions may result in penalties up to \$2,500 per violation or \$7,500 for each intentional violation involving the personal information of minors.⁵⁸ No state comprehensive privacy law grants consumers a private right of action (i.e., the right to bring a lawsuit) based on a company’s failure to comply with UOOM requests.⁵⁹

In August 2022, the Attorney General of California announced the first enforcement action based on a company’s failure to honor GPC signals.⁶⁰ The Attorney General alleged that Sephora, a beauty-product retailer, allowed third parties to collect information about consumers visiting its website in exchange for

⁴⁹ *Global Privacy Control (GPC)*, CAL. DEP’T OF JUSTICE, <https://oag.ca.gov/privacy/ccpa/gpc> [<https://perma.cc/4ULR-C7UT>] (last visited July 30, 2026).

⁵⁰ *Universal Opt-Out and the Colorado Privacy Act*, COLO. ATT’Y GEN., <https://coag.gov/opt-out/> [<https://perma.cc/38JB-WD55>] (last visited July 30, 2026).

⁵¹ *The Connecticut Data Privacy Act*, CONN. ATT’Y GEN., <https://portal.ct.gov/ag/sections/privacy/the-connecticut-data-privacy-act> [<https://perma.cc/U9DP-GN4J>] (last visited July 30, 2026).

⁵² *Privacy Law FAQs for Consumers*, OR. DEP’T OF JUST.: CONSUMER PROT., <https://www.doj.state.or.us/consumer-protection/id-theft-data-breaches/privacy/privacy-law-faqs-for-consumers/> [<https://perma.cc/LC34-2P8G>] (last visited July 30, 2026); *New Jersey Data Privacy Law FAQs*, N.J. DIV. OF CONSUMER AFFS. (Jan. 15, 2025), <https://www.njconsumeraffairs.gov/ocp/Pages/NJ-Data-Privacy-Law-FAQ.aspx> [<https://perma.cc/8KNN-Y4CZ>].

⁵³ See, e.g., CONN. GEN. STAT. § 42-525 (2025); UTAH CODE ANN. § 13-61-402 (West 2025).

⁵⁴ See, e.g., VA. CODE ANN. § 59.1-584 (West 2025); UTAH CODE ANN. § 13-61-402; IOWA CODE § 715D.8 (2026); TEX. BUS. & COM. CODE ANN. § 541.155 (West 2025); IND. CODE § 24-15-10-2 (2025); TENN. CODE ANN. § 47-18-3312 (West 2025); OR. REV. STAT. § 646A.589 (2025).

⁵⁵ See, e.g., CONN. GEN. STAT. § 42-525; 2024 Md. Laws ch. 455, § 1.

⁵⁶ CAL. CIV. CODE §§ 1798.155, 1798.199.90 (West 2025).

⁵⁷ *Id.*

⁵⁸ *Id.*

⁵⁹ California is the only state whose privacy law provides private right of action, but this private right of action is limited to certain circumstances where a security breach compromised the consumer’s personal information. CAL. CIV. CODE § 1798.150 (West 2025).

⁶⁰ Press Release, Cal. Dep’t of Justice, Attorney General Bonta Announces Settlement with Sephora as Part of Ongoing Enforcement of California Consumer Privacy Act (Aug. 24, 2022), <https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-settlement-sephora-part-ongoing-enforcement> [<https://perma.cc/VU7T-44A3>].

various benefits.⁶¹ Sephora, however, allegedly did not tell consumers it was selling their information and furthermore did not honor GPC signals.⁶² According to the complaint, Sephora’s “website was not confirmed to detect or process any global privacy control signals, such as the [GPC]” and “wholly disregarded consumers who communicated to the company, via a global opt-out signal, that Sephora should not sell their personal information.”⁶³ Sephora ultimately settled the allegations by agreeing to pay a \$1.2 million penalty and adopting a compliance program designed to ensure that it processes GPC signals.⁶⁴

In July 2025, the California Attorney General announced another GPC-related settlement.⁶⁵ In that case, Healthline.com, a website containing informational articles about health and wellness, allegedly used cookies and pixels to collect information about the consumers, including information about the articles they read.⁶⁶ Healthline.com shared this information with third-party advertisers, who used it to send targeted advertisements to consumers.⁶⁷ According to the complaint, Healthline.com shared this data with advertisers even when consumers had used GPC to opt-out of the sale or sharing of their data.⁶⁸ Healthline.com agreed to resolve the allegations by, among other things, paying \$1.55 million and agreeing to a compliance program to ensure that it processes GPC signals.⁶⁹

GPC also played a role in California’s recent enforcement action against Walt Disney Company (Disney).⁷⁰ On February 11, 2026, California’s Attorney General announced that Disney had agreed to settle allegations that it violated California privacy law by failing to fully effectuate consumer-opt-out requests, including those sent by GPC signals.⁷¹ Disney owns and operates several video streaming services: Disney+, Hulu, and ESPN+. ⁷² While Disney accepted GPC signals on its video streaming websites, it only honored these requests for the “specific service and device” the consumer was using when they sent the request, even if the consumer was logged into their account and Disney had account information that indicated the consumer was associated with other devices and services.⁷³ To resolve the allegations, Disney agreed to pay \$2.75 million and committed to fully effectuating opt-out requests, including by respecting GPC signals across all streaming services associated with consumers’ accounts.⁷⁴

⁶¹ Complaint at 2, *California v. Sephora USA, Inc.*, No. CGC-22-601380 (Cal. Super. Ct. Aug. 24, 2022) [hereinafter *Sephora Complaint*].

⁶² *Id.* at 3, 5.

⁶³ *Id.* at 3.

⁶⁴ *California v. Sephora USA, Inc.*, No. CGC-22-601380, 2022 WL 22913962, at *2–3 (Cal. Super. Ct. Aug. 24, 2022).

⁶⁵ Press Release, Cal. Dep’t of Justice, Attorney General Bonta Announces Largest CCPA Settlement to Date, Secures \$1.55 Million from Healthline.com (July 1, 2025), <https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-largest-ccpa-settlement-date-secures-155> [<https://perma.cc/GT2S-J92W>].

⁶⁶ Complaint at 1–2, *California v. Healthline Media, LLC*, No. CGC-25-626794 (Cal. Super. Ct. July 1, 2025) [hereinafter *Healthline Complaint*].

⁶⁷ *Id.* at 2.

⁶⁸ *Id.* at 5–6, 10.

⁶⁹ Final Judgment and Permanent Injunction at 4–5, 7, *California v. Healthline Media, LLC*, No. CGC-25-626794 (Cal. Super. Ct. July 28, 2025).

⁷⁰ Press Release, Cal. Dep’t of Just., California Won’t Let It Go: Attorney General Bonta Announces \$2.7 Million Settlement with Disney, Largest CCPA Settlement in California History (Feb. 11, 2026), <https://oag.ca.gov/news/press-releases/california-wont-let-it-go-attorney-general-bonta-announces-275-million> [<https://perma.cc/J3DR-GJXS>].

⁷¹ *Id.*

⁷² Complaint at 3, *California v. Disney DTC, LLC*, No. 26STCV04425 (Cal. Super. Ct. Feb. 11, 2026) [hereinafter *Disney Complaint*].

⁷³ *Id.* at 6.

⁷⁴ Final Judgment and Permanent Injunction at 6, *Disney*, No. 26STCV04425.

Some states have begun to coordinate their investigative and enforcement efforts. On September 9, 2025, the Attorneys General of Colorado and Connecticut announced that they were joining California enforcers in a joint investigative sweep into businesses' compliance with GPC signals.⁷⁵ The announcement explained that, as part of the sweep, the coalition of state enforcers was "contacting businesses that may not be processing consumer requests to opt-out of the sale of their personal information submitted via the GPC as required by law and requesting that those businesses comply."⁷⁶

Verification of Consumer Residence

Businesses are required to comply with a UOOM signal only if the signal is associated with a resident of one of the states recognizing UOOMs.⁷⁷ State law typically defines a "resident" as someone who is (1) "domiciled" in the state (i.e., who consider the state their permanent home, even if they are temporarily residing, working, or traveling outside the state), or (2) who is present in the state for a certain amount of time, such as six months.⁷⁸

Texas⁷⁹ and Nebraska,⁸⁰ do not require businesses to comply with UOOM signals if they are not able to determine the consumer's residency with "commercially reasonable effort." Connecticut,⁸¹ Montana,⁸² Oregon,⁸³ Delaware,⁸⁴ New Jersey,⁸⁵ New Hampshire,⁸⁶ Maryland,⁸⁷ and Minnesota⁸⁸ provide that the UOOM technology must enable businesses to "accurately determine" whether the associated consumer is a resident of the state; Minnesota's law further states that the use of an "Internet protocol address to estimate the consumer's location is sufficient to determine the consumer's residence."⁸⁹ Colorado's UOOM regulations provide that the UOOM technology is not obligated to authenticate that a consumer is a Colorado resident, but it may provide such authentication capabilities "if it chooses" and it "must not prevent" the business's ability to determine whether a consumer is a Colorado resident.⁹⁰ California's privacy law and implementing regulations are silent on how a business's ability to verify a consumer's residency impacts its UOOM obligations.⁹¹

⁷⁵ Press Release, Cal. Priv. Prot. Agency, California Privacy Protection Agency Announces Joint Investigative Privacy Sweep: CA, CO, and CT Investigate Business Refusing to Honor Consumers' Right to Opt-Out of the Sale of Their Personal Information (Sept. 9, 2025), <https://cpa.ca.gov/announcements/2025/20250909.html> [<https://perma.cc/BJB8-DWGS>].

⁷⁶ *Id.*

⁷⁷ See, e.g., COLO. REV. STAT. § 6-1-1303(6) (2025); TEX. BUS. & COM. CODE § 541.001(7) (West 2025); N.J. STAT. ANN. § 56:8-166.11 (West 2025); see also CAL. CIV. CODE § 1798.140(i) (West 2026) (defining "consumer" as a "natural person who is a California resident").

⁷⁸ See, e.g., 1 COLO. CODE REGS. § 201-2:39-22-103(8)(a) (2025) (defining a resident to include a natural person who is "domiciled" in Colorado or who satisfies a six-month residency rule).

⁷⁹ TEX. BUS. & COM. CODE § 541.055(e) (West 2025).

⁸⁰ NEB. REV. STAT. § 87-1111(5)(b) (2025).

⁸¹ CONN. GEN. STAT. §§ 42-520(e)(1)(V) (2026).

⁸² MONT. CODE ANN. § 30-14-2809(3)(b)(v) (West 2025).

⁸³ OR. REV. STAT. § 646A.578(5)(E) (2025).

⁸⁴ DEL. CODE ANN. tit. 6, § 12D-106(e)(1) (West 2025).

⁸⁵ N.J. STAT. ANN. § 56:8-166.11(b)(2)(e) (West 2025).

⁸⁶ N.H. REV. STAT. ANN. § 507-H:5.V(a)(1)(B)(v) (2025).

⁸⁷ MD. CODE ANN., COM. LAW § 14-4707(f)(4) (West 2025).

⁸⁸ MINN. STAT. ANN. § 325M.14(3)(a)(5) (West 2025).

⁸⁹ *Id.*

⁹⁰ 4 COLO. CODE REGS. §§ 904-3:5.03, 904-3:5.06 (2025).

⁹¹ See CAL. CIV. CODE §§ 1798.135(b), 1798.185(18) (West 2026); CAL. CODE REGS. tit. 11, § 7025 (2026).

GPC signals do not provide information about a user's location or residency. A business might be able to identify the state in which a consumer resides using various methods, such as comparing the internet IP address of a device used by the consumer to an IP geolocation database,⁹² using information the consumer provides on the website, and purchasing the consumer's address from a data broker. The accuracy of the information might depend on different factors, such as the source of the information and whether the consumer is using a virtual private network (VPN), which hides the device's real IP address and location by showing the IP address of a VPN server.⁹³

Consumer Residency “Edge Cases”

You asked about a number of “edge cases” where a consumer's state residency would not be apparent based on the IP addresses of the devices they used. In particular, you mentioned situations where residents are in their home state but their IP address indicates that they are located in a different state because, for example, they are using a VPN service or because their wireless carrier issues IP addresses to users in a geographical area spanning multiple states. You also mentioned situations where a resident is physically outside of their home state because, for example, they are working or going to school in another state, serving in the military, or serving in Congress.

Companies' obligations in these situations would likely depend on the particular state law and the existing information a company has about the consumer. As mentioned, Minnesota expressly allows companies to use IP addresses as a proxy for determining a consumer's residency.⁹⁴ Other states, however, might require companies to utilize information beyond IP addresses to determine a consumer's residency. If the company has other sources of information about the consumer at its disposal, such as information the consumer provided on the company's website, state enforcers may argue that it would be “commercially reasonable” for them to use this information to more accurately determine the consumer's residency.⁹⁵

Such edge cases, however, have not factored into state enforcement of UOOM requirements. As discussed, none of the state laws empower *consumers* to bring a lawsuit when companies unlawfully ignore their UOOM signals, which means consumer residency requirements are likely to be raised in enforcement actions only if raised by state attorneys general or state privacy agencies. To date, verification of consumer residency has not played a role in GPC-related enforcement actions. In both the Sephora and Healthline.com cases, violations appear to have been established based on how the companies treated *investigators'* GPC signals, rather than GPC signals associated with ordinary consumers.⁹⁶ Accordingly, the complaints did not address whether the businesses improperly ignored GPC signals associated with particular California residents because of their reliance on IP address information.⁹⁷ The California Attorney General's complaint against Disney likewise did not address consumer residency requirements.⁹⁸

⁹² An IP geolocation database aggregates data such as IP addresses, GPS data, and network information to determine the geographic location of certain IP addresses. See, e.g., *Free & Reliable IP Geolocation Data*, IP2LOCATION LITE https://lite.ip2location.com/?lang=en_US [<https://perma.cc/NV5V-3BM4>] (last visited July 30, 2026).

⁹³ *What Is a VPN?*, MICROSOFT, <https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-vpn> [<https://perma.cc/9NK7-DNH7>] (last visited July 30, 2026).

⁹⁴ MINN. STAT. ANN. § 325M.14(3)(a)(5) (West 2025).

⁹⁵ TEX. BUS. & COM. CODE § 541.055(e) (West 2025); NEB. REV. STAT. § 87-1111(5)(b) (2025).

⁹⁶ See Sephora Complaint, *supra* note 61, at 5; Healthline Complaint, *supra* note 66, at 6–8.

⁹⁷ See Sephora Complaint, *supra* note 61; Healthline Complaint, *supra* note 66.

⁹⁸ See Disney Complaint, *supra* note 72.

“Commercially Reasonable Effort” and Rejecting GPC Signals Based on IP Address

For states that incorporate a “commercially reasonable effort” standard into their laws, you asked if it would be considered a commercially reasonable effort if a company were to reject a GPC signal because an IP geolocation database used by the company indicates that the IP address of the consumer’s device is not located in a state that requires compliance with UOOMs. Specifically, you asked whether a company would be able to reject the GPC signal without notifying users and confirming their residency, particularly when some companies notify and prompt a user to affirm their residency before rejecting the GPC signal.

As mentioned, Texas and Nebraska do not require businesses to comply with UOOM signals if the business is not able to determine with “commercially reasonable effort” that “the consumer is a resident of [the] state.”⁹⁹ Other states do not require businesses to comply with opt-out requests from an “authorized agent” if the business is not able to verify, with “commercially reasonable effort,” the identity of the consumer and that the agent is authorized to act on the consumer’s behalf.¹⁰⁰

State privacy laws do not define what constitutes a commercially reasonable effort. The term “commercially reasonable” is commonly understood as conduct that is “in good faith” and consistent with “commonly accepted commercial practices.”¹⁰¹ The Uniform Commercial Code (UCC), for example, provides that the sale of collateral is considered “commercially reasonable” if it is “sold or disposed of”: (1) “in the usual manner on any recognized market,” (2) at a recognized market price, or (3) “otherwise in conformity with reasonable commercial practices among dealers in the type of property” in question.¹⁰²

What constitutes a commercially reasonable effort may further depend on the size and scope of the business.¹⁰³ For example, in *NetChoice v. Carr*, a federal district court invalidated on First Amendment grounds a Georgia law that required social media platforms to “make commercially reasonable efforts to verify the age of account holders with a level of certainty appropriate to the risks that arise from the social media platform’s information management practices.”¹⁰⁴ In the context of its First Amendment analysis, the court concluded that the law was not sufficiently tailored because, among other things, the “commercially reasonable” standard could apply differently to companies of different sizes.¹⁰⁵ The Court explained that, under the state’s own admission, “what is commercially reasonable for Facebook . . . one of the largest corporations in the world, might be different than what is commercially reasonable for Dreamwidth.”¹⁰⁶

Whether it is commercially reasonable for a company to use an IP geolocation database to determine a person’s residency would thus likely depend on whether it is a commonly accepted practice among companies of a similar size and scope. Some sources suggest that companies of various sizes commonly use IP geolocation databases, along with other data, for multiple purposes, such as to provide targeted

⁹⁹ TEX. BUS. & COM. CODE § 541.055(e) (West 2025); NEB. REV. STAT. § 87-1111(5)(b) (2025).

¹⁰⁰ See, e.g., TEX. BUS. & COM. CODE § 541.055(e); N.J. STAT. ANN. § 56:8-166.11 (West 2025); MD. CODE ANN., COM. LAW § 14-4706(b); NEB. REV. STAT. § 87-1111(5) (2025).

¹⁰¹ *Commercially Reasonable*, BLACK’S LAW DICTIONARY (12th ed. 2024).

¹⁰² U.C.C. § 9-627(b) (AM. LAW INST. & UNIF. LAW COMM’N 2022).

¹⁰³ See, e.g., *Elorac, Inc. v. Sanofi-Aventus Canada, Inc.*, 343 F.Supp.3d 789, 794 (N.D. Ill. 2018) (explaining that a license agreement defined “Commercially Reasonable Efforts” as “efforts consistent with those generally utilized by companies of a similar size”); *Shareholder Representative Servs. LLC v. Alexion Pharm., Inc.*, No. 2020-1069-MTZ, 2024 WL 4052343, at *14 (Del. Ch. Sept. 5, 2024) (explaining that a merger agreement defined “Commercially Reasonable Efforts” as “such efforts and resources typically used” by “companies similar in size and scope”).

¹⁰⁴ *NetChoice v. Carr*, 789 F.Supp.3d 1200, 1228 (N.D. Ga. 2025).

¹⁰⁵ *Id.* at 1228–29.

¹⁰⁶ *Id.* at 1228.

advertisements and to comply with federal, state, and local regulations.¹⁰⁷ CRS did not find any publicly available information that indicates whether particular companies use IP geolocation databases to determine whether a state privacy law applies to their users. CRS also did not find a comprehensive list of companies that notify and prompt users to affirm their residency before rejecting a GPC signal. It is therefore unclear whether a court would accept the use of an IP geolocation database as a commercially reasonable effort to determine a user's state location.

Privacy-By-Default Browsers and UOOM Requirements

You asked us how states with UOOM laws treat browsers that turn on GPC by default. The browser Brave, for example, employs a “privacy-by-default” model that “does not require users to change anything to start using the GPC to assert their privacy rights” but turns on “the [GPC] feature by default.”¹⁰⁸ Brave's website explains its belief that “anyone choosing to use Brave has already made an unambiguous expression that they do not want their data to be sold or shared online.”¹⁰⁹

Most states with UOOM laws require that UOOM signals reflect consumers' affirmative choice to opt out of data sharing. Most state laws say (in identical or nearly identical language) that UOOMs “may not make use of a default setting, but must require the consumer to make an affirmative, freely given, and unambiguous choice to indicate the consumer's intent to opt out of any processing of a consumer's personal data.”¹¹⁰ California's law similarly requires that UOOMs “clearly represent a consumer's intent and be free of defaults constraining or presupposing that intent.”¹¹¹

Some stakeholders have argued that these provisions preclude privacy-by-design web browsers from turning on UOOMs by default.¹¹² For example, several advertising industry trade associations co-wrote a letter urging the Colorado Attorney General to “promulgate rules ensur[ing] that a consumer must take an action to enable the UOOM before it can begin opting the consumer out of data transfers across the Internet.”¹¹³ The trade associations maintained that such rules followed from the statute's requirement that

¹⁰⁷ See, e.g., Patricia Callejo et al., “A Deep Dive into the Accuracy of IP Geolocation Databases and its Impact on Online Advertising,” *IEEE TRANSACTIONS ON MOBILE COMPUTING*, vol. 22, issue 18 (August 2023), <https://doi.org/10.1109/TMC.2022.3166785>; and Sheharyak Malik, “What is IP Geolocation? How It Works in 2026,” *IP GEOLOCATION*, April 14, 2026, <https://ipgeolocation.io/guides/what-is-ip-geolocation-how-it-works>.

¹⁰⁸ *Global Privacy Control, A New Privacy Standard Proposal*, BRAVE (last updated Sept. 8, 2023), <https://brave.com/web-standards-at-brave/4-global-privacy-control/>.

¹⁰⁹ *Id.*

¹¹⁰ COLO. REV. STAT. § 6-1-1313 (2025); CONN. GEN. STAT. § 42-520(e)(1)(A)(ii) (2026); MONT. CODE ANN. § 30-14-2809(3) (West 2025); TEX. BUS. & COM. CODE § 541.055(f) (West 2025); OR. REV. STAT. § 646A.578(5)(c)(B) (2025); DEL. CODE ANN., tit. 6, § 12D-106(e)(1) (West 2025); MD. CODE ANN., COM. LAW §§ 14-4707(f)(4)(v), (5)(ii) (West 2025); N.H. REV. STAT. ANN. §§ 507-H:6.V.(a)(1)(B)(ii) (2025); NEB. REV. STAT. § 87-1111(6)(b) (2025); MINN. STAT. ANN. §§ 325M.14(3)(a)(2) (West 2025).

¹¹¹ CAL. CIV. CODE § 1798.185(a)(18)(A)(iii)(II) (West 2025). New Jersey's law differs from the other laws by only restricting UOOMs from using “a default setting that *opts in* a consumer to the processing or sale of personal data.” N.J. STAT. ANN. § 56.8-166.11(8)(b)(2)(b) (West 2025) (emphasis added). New Jersey's law, however, permits, but does not require, the New Jersey Division of Consumer Affairs in the Department of Law and Public Safety to adopt “technical specifications for one or more universal opt-out mechanisms that clearly communicate a consumer's affirmative, freely given, and unambiguous choice to opt out of the processing of personal data” *Id.* § 56.8-166.11(c).

¹¹² See, e.g., CTIA, Comment In the Matter of California Privacy Rights Act of 2020 Rulemaking Process, at 18–19 (Nov. 21, 2022), https://coppa.ca.gov/regulations/pdf/comments_129_157.pdf (“The [statute] prohibits opt-out preference technology from turning the opt-out preference signal ‘on’ by default. But, the Regulations leave open the possibility that preference signal technology could do just that.”) (internal citations omitted).

¹¹³ Letter from Ass'ns of Nat'l Adverts. et al., Informal Pre-Rulemaking Comment on Colorado Privacy Act Regulations, at 4 (Aug. 5, 2022), <https://www.aaf.org/common/Uploaded%20files/Government%20Affairs/2022-08-05-AdTradeLetter-Input-%20CO-Privacy.pdf>.

UOOMs clearly represent the consumer’s “affirmative, freely given, and unambiguous choice to opt out.”¹¹⁴ They reasoned that that “allowing a consumer’s use of a marketed privacy feature to function as affirmative consent” was insufficient because “[t]ools and products are often bundled and marketed to consumers to feature numerous attributes, so attempts to discern which one of those attributes may or may not have spurred a consumer’s purchase, download, or use is an uncertain task.”¹¹⁵

The final regulations issued by the Colorado Attorney General, however, expressly allow such privacy-by-design browsers, provided they do not come “pre-installed with a device” and are “marketed as a tool that will exercise a user’s rights to opt out of the Processing of Personal Data using a [UOOM].”¹¹⁶ The regulations state that a consumer’s use of such a browser “shall be considered the Consumer’s affirmative, freely given, and unambiguous choice to use a [UOOM].”¹¹⁷

While California’s regulations do not expressly address privacy-by-design browsers, the regulations do require covered businesses to process UOOM signals that “make clear to the consumer, whether in its configuration or in its 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.”¹¹⁸ The CPPA has explained that this provision “allows for situations where consumers affirmatively choose products or services that include built-in privacy-protected features because these products or services are designed with privacy in mind.”¹¹⁹ According to the CPPA, a consumer’s “selection of privacy-by-design products or services is an affirmative step and sufficient to express the consumer’s intent to opt out of the sale and sharing of personal information.”¹²⁰

Attorneys general in the remaining states with UOOM laws do not appear to have opined on whether privacy-by-design browsers are consistent with their states’ UOOM requirements. Likewise, no court has had occasion to consider this question. Should it do so, the court would likely consider the extent to which a consumer’s use of the browser constitutes an “unambiguous” choice to opt-out of data sharing. This question could depend on the factual circumstances relevant to the browser in question, such as its marketing and disclosures to consumers.

Potential Barriers to Adoption

One potential barrier to adoption is that, as of the date of this memorandum, GPC is a draft technical standard that is subject to change.¹²¹ W3C includes the following statement:

An editor’s draft is a document allowing the Group to iterate internally on its content for consideration. Editor’s Drafts are works in progress inside a W3C Group and are not required to have the consensus of the Group participants. These drafts have not received formal review and are not endorsed by W3C.

These drafts MUST NOT be cited as W3C standards and may or may not become W3C standards.

¹¹⁴ *Id.*

¹¹⁵ *Id.*

¹¹⁶ 4 COLO. CODE REGS. § 904-3:5.04 (2025).

¹¹⁷ *Id.*

¹¹⁸ CAL. CODE REGS. tit. 11, § 7025(b)(2) (2026).

¹¹⁹ CAL. PRIVACY PROT. AGENCY, FINAL STATEMENT OF REASONS, app. A, at 179 (Mar. 29, 2023), https://cppa.ca.gov/regulations/pdf/20230329_final_sor_app_a_comments.pdf.

¹²⁰ *Id.*

¹²¹ W3C, *supra* note 8.

Software MAY implement these drafts at their own risk. Implementation is neither discouraged nor encouraged but can contribute to proposals for further action on a specification.¹²²

The draft nature of GPC might discourage some websites, browsers, and internet users from using it. Browsers implementing the draft version of GPC might need to incorporate changes as GPC is updated and might enable unintended effects, such as privacy concerns related to browser or device fingerprinting. On the other hand, browsers that implement the draft version of GPC may be able to provide UOOM more quickly, potentially attracting users who are concerned about data privacy.

Although desktop extensions allowing users to enable GPC were available for most browsers, fewer were available for browsers on mobile devices. DuckDuckGo appears to be the only browser on Apple's iOS mobile platform that allows users to enable GPC, based on information CRS found about GPC.¹²³

Additionally, the number of internet users utilizing GPC might affect the number of websites and user-agents who choose to adopt the GPC and vice versa. About fifty million users were utilizing a browser or extension with GPC support, according to two editors of the most recent draft of GPC; at the time CRS accessed the report, it did not specify when this estimate was calculated.¹²⁴ One source estimates that there were 322 million individuals using the internet in the United States at the start of 2025.¹²⁵ Combining this estimate with the reported number of GPC users suggests that about 16% of internet users in the United States used GPC.

Changes in state law could require browsers to adopt GPC, regardless of any technical or practical obstacles. In October 2025, California enacted the California Opt Me Out Act, which prohibits businesses from developing or maintaining a browser that does not have “functionality configurable by a consumer that enables the browser to send an opt-out preference signal to businesses with which the consumer interacts through the browsers.”¹²⁶ The law defines “opt out preference signal” as a signal that “communicates the consumer’s choice to opt out of the sale and sharing of the consumer’s personal information.”¹²⁷ The law’s requirements are to become effective January 1, 2027.¹²⁸

¹²² *Types of Documents W3C Publishes: 2.3 Editor's draft*, W3C, <https://www.w3.org/standards/types/#ED> [<https://perma.cc/UN4L-7QAN>] (last visited July 30, 2026).

¹²³ *Fly Your Privacy Flag with Global Privacy Control*, *supra* note 16; W3C, *supra* note 8.

¹²⁴ ARAM ZUCKER-SCHARFF & SEBASTIAN ZIMMECK, HOW TO IMPLEMENT GLOBAL PRIVACY CONTROL (GPC) FOR PUBLISHERS, <https://globalprivacycontrol.org/Implementing%20GPC%20for%20Publishers.pdf> [<https://perma.cc/BS7W-KSJL>] (last visited July 30, 2026).

¹²⁵ Simon Kemp, *Digital 2025: The United States of America*, DATAREPORTAL (Feb. 25, 2025), <https://datareportal.com/reports/digital-2025-united-states-of-america> [<https://perma.cc/8DMW-JLQS>].

¹²⁶ 2025 Cal. Stat. ch. 465, § 2 (codified at CAL. CIV. CODE § 1798.136 (West 2025)).

¹²⁷ CAL. CIV. CODE § 1798.136(e)(2).

¹²⁸ *Id.* § 1798.136(f).