Cybersecurity Law Report cslawreport.com

Mar. 26, 2025

Consumer Privacy

# Navigating Global Privacy Control's Not-So-Simple Implementation

By Matt Fleischer-Black, *Cybersecurity Law Report*

The global privacy control (GPC) is a one-step toggle for consumers to automatically opt out from website sharing of their personal data. By the end of 2025, nine states will require covered businesses to honor consumers' global requests to stop data shares, sales or targeted advertising using GPC or similar universal opt-out mechanisms (UOOMs).

GPC has been called simple for companies to implement, purportedly a single line of code in JavaScript that feeds into companies' existing processes for consumer opt-outs. GPC compliance is also easy to investigate. "Regulators and researchers are using automated tools to make sure that GPC is correctly mapped to opt-outs" by looking at web traffic, Raptive vice president for innovation Don Marti told the Cybersecurity Law Report.

For everybody besides consumers, "simple" turns out to have complications. This article looks at GPC's pitfalls for companies and for regulators, including the messy system of privacy signals meant to communicate opt-outs to downstream parties, potential misconfigurations and multiple compliance choices for GPC. It also examines a peer-reviewed study that involved crawling 11,000 sites, which revealed that many sites did not translate GPC into opt-out signals.

See "Why Companies Unintentionally Fail to Honor Opt-Outs" (Aug. 16, 2023).

## AGs Investigate GPC Compliance

For Data Privacy Day 2025 in January, the California and Connecticut AGs promoted the use of GPC as "an easy-to-use browser setting or extension that automatically signals to businesses that they should not sell your personal information to third parties, including for targeted advertising."

The lone enforcement action asserting a GPC non-compliance claim was the California AG's 2022 case against Sephora, but in recent months, state AGs have regularly questioned companies about honoring GPC signals. "Regulators use tools on the market available for businesses to audit pixels firing on sites. They will use that to determine to what extent data is being shared with third

parties via tracking technologies before and after an opt-out," Orrick partner Sundeep Kapur told the Cybersecurity Law Report.

Using software to sleuth for potential issues, noted Network Advertising Initiative GC Tony Ficarrotta, "makes this an easy sweep for regulators to do. They don't have to receive a consumer complaint or send an inquiry letter," he told the Cybersecurity Law Report. The lack of further public enforcement actions indicates that, for now, AGs and companies have been agreeing on remedies for any GPC-related concerns, he said.

See "Advertising Opt-Outs Drive New Privacy Strategies in 2025" (Dec. 18, 2024).

## What Does GPC Compliance Involve?

Firefox, Brave and DuckDuckGo are the three browsers that offer a setting to send a GPC signal. Collectively, they have less than a 10% share of browsers in use. For the Chrome, Safari and Edge browsers, users can choose among five extensions that send the signal.

### Receiving the Signal

Companies have two technical choices for recognizing the signal, explained Sebastian Zimmeck, who launched GPC's development process in 2020 with Ashkan Soltani. One signal comes from the user's computer (the HTTPS header request). However, a web page feature called a Document Object Model can also report the signal and is incrementally quicker, so sites have preferred it, he told the Cybersecurity Law Report. Zimmeck's informational videos for businesses are posted on the websites of the Colorado, Connecticut and California AGs.

### Acting on the Signal

Once received, GPC should trigger the same process as companies would use to enact any other opt-out. Companies sending data communicate an individual's privacy preferences in strings of code appended to the data that embed the user's choices and their applicability. In 2020, the Interactive Advertising Bureau Tech Lab (IAB) created the four-character U.S. Privacy String (USPS) for CCPA compliance. Two years later, IAB superseded the USPS with its new Global Privacy Protocol (GPP), a more elaborate signal offering many fields to govern data for different jurisdictions, including individual U.S. states, Canada and Europe. In January 2024, IAB deprecated the USPS and urged all companies to use GPP instead.

Many companies use the GPC compliance suites that consent management providers (CMPs) integrate. Most prominently, OneTrust established a proprietary cookie to express preferences controlling the data use, the OptanonConsent cookie (Optanon), but some CMPs are capable of using the GPP string.

"Using a CMP is probably the safest way to go because, while the coding itself doesn't seem that complex, there are many areas where companies can get this wrong," Neal, Gerber & Eisenberg partner David Wheeler told the Cybersecurity Law Report. Other GPC-related compliance tasks companies should consider include modifications to their data transmission instructions, integrations with vendors and server behaviors that collect data. The AGs and IAB offer compliance resources for businesses.

See "Managing Tracking Technologies and Their Privacy Dilemmas in 2025" (Mar. 12, 2025).

## Study Examines Honoring of GPC Signal in Early 2024

A peer-reviewed study (Study) led by Katherine Hausladen, Zimmeck's student, analyzed 11,000 websites' California GPC compliance.

### Use of Multi-State Privacy Signal Lagged

The researchers conducted three runs of sending a GPC signal and performed a before-and-after analysis of each site's web traffic to see California opt-out signals. The tests were performed in December 2023, February 2024 and April 2024. Each site included in the testing had (a) stated publicly that it sold data; (b) integrated trackers for any of 11 major ad networks; and (c) appeared to be subject to the CCPA.

The Study did not check compliance with Colorado's or Connecticut's requirements, which were not in effect until July 2024. Zimmeck said studies of compliance with those states' laws are now underway.

By early 2024, California opt-out signaling had grown messy and inconsistent because of slow uptake of GPP, the new standard. In April 2024, only 12% of all analyzed websites were using GPP, the study found. Many companies that sent a GPP string seemed to be testing it – 82% of them also sent a second signal, some USPS, others Optanon. When companies sent multiple strings, the researchers found between 10% and 12% delivered conflicting signals.

See "IAB Unveils Multistate Contract to Satisfy 2023 Laws' Curbs on Targeted Ads" (Feb. 22, 2023).

### Many GPC Signals Reported as "Did Not Opt Out"

Two-thirds of the companies that used Optanon faithfully translated GPC opt-outs downstream in the three runs.

Forty-five percent of the websites that sent data with a USPS string honored the researchers' GPC signal by propagating a California opt-out signal.

Sites using the more complex GPP string did far worse with GPC. Across the researchers' test runs, only 9%, 13% and then 15% of GPP strings broadcast the GPC opt-out downstream. According to

Zimmeck, most – 85% in the first two runs and 80% in the third – wrongly encoded a "Did Not Opt Out" value. The Study tallied the values encoded in both the GPP's California and national fields because either would comply.

"A lot of publishers and a lot of adtech companies are evaluating and working to implement GPP efficiently because of the complexity, and thus reliance on it is not yet widespread," Ficarrotta said.

The overall observable translation rate across all the privacy strings was 44% accurate for GPC opt-out, the Study reports. The authors noted misconfigurations could cause some inaccuracy but attributed most of the no-opt-out messages to companies' "widespread disregard" of the GPC signal.

See "France's Cookie Enforcement Against TikTok and Microsoft Highlights Common Compliance Missteps" (Jan. 25, 2023).

## Compliance Choice: Suppress Data or Send a String?

Overall, half of the Study's researchers' GPC signals did not prompt transmission of any privacy string, possibly because many companies choose to comply with a GPC signal by suppressing the data. "One option is to just shut the faucet off, stop the firing of the pixel or tracker, in which case there is no data out," Kapur noted.

When a regulator's or researcher's test "does not translate an opt-out in a privacy string after the GPC signal, that can lead to questions and inquiries. But in a lot of cases, that does not mean anything is wrong," Ficarrotta cautioned. With data suppression considered, compliance with GPC signals may have reached as high as 70% of studied websites.

One argument for stopping outright the transmission of personal data rather than sending it with privacy strings is the considerable implementation expense, Ficarrotta posited. To use GPP signals, "publishers might need to rejigger the code on all their pages and there may be a significant amount of work and diligence to make sure that signals are encoded properly and their ad partners read and understand the signal and meet expectations," he detailed.

The costs may not be worth the gain. Through 2024, opt-out rates tended to be under 10% for web traffic, so companies still could conduct mostly unrestricted advertising activities for 90% of users, Ficarrotta said.

When service provider contracts are in effect, controllers might not bother to append the privacy string when transmitting personal data to analytics providers or other recipients, Kapur noted. "When companies are a signatory to the IAB's Multistate Privacy Agreement, then the downstream participants can become service providers/processors for limited advertising activities," and companies can use data for set purposes like measurement or limited analysis, he explained.

Conversely, companies are motivated to invest in deploying GPP because the user choices (and other compliance details) in its fields let companies use personal data in limited ways while respecting opt-out rights. More broadly, GPP use has the potential to improve overall compliance across

the advertising ecosystem and can supply evidence of conscientiousness to regulators, Ficarrotta suggested.

See "Considerations for Adtech Stemming From Oracle's $115-Million Settlement" (Aug. 14, 2024).

## Three GPC Questions Companies Face

While GPC ends consumers' needs to confront privacy questions site by site, the framework opens up three operational and legal questions for companies.

### Announce the Company's Recognition of GPC, or Simply Comply?

The New York Times and Meredith were among the founding sponsors of the GPC development project in 2020. Prominent publishers advocated for GPC because use builds further trust with their engaged consumers, Marti said. Mazda USA, for example, displays a pop-up on its website telling visitors it has honored their GPC signals.

The GPP string includes a GPC field for a website to declare downstream that it sent the opt-out. Propagating the GPC signal might help companies show regulators that they honor GPC. Websites also can add code (a .json) to broadcast that the site honors GPC.

All that the law requires for a GPC signal is to stop the applicable data activities. While transparency downstream is beneficial, "encoding the status of the GPC signal in the string creates the possibility for confusion and potentially conflicting signals because privacy strings may include information about user choices beyond the presence or absence of a GPC signal" from users' browsers, Ficarrotta cautioned.

### Ask the Consumer to Opt Back In?

Each state privacy law explicitly lets GPC users opt back in to favorite web pages. Yahoo sites have offered an opt-back-in option using a pop-up that warns users that GPC "leads to a lower-quality experience on Yahoo by blocking certain editorial content, including embedded tweets and YouTube videos," and noting that opting in to Yahoo sites "won't affect your GPC settings for other websites."

The GPP string does not have a field for opting back in, so sites pass a string that indicates both a "GPC True" and a "Did Not Opt Out" value, Marti noted. "Together, that is supposed to send the message that 'this is a GPC user, but they opted back in.' The question is [whether] you trust the site enough to believe that message." For a downstream company, "it is impossible to tell a legit opt-back-in apart from fraud," he pointed out.

Downstream companies have had little choice but to trust that their publishers send them data with consents that comply with the law and their contracts, Ficarrotta noted. "An unscrupulous publisher could still remove or fraudulently alter a string if they care more about squeezing revenue

out of a user than complying with the law," he noted, adding, "privacy strings do not remove the need for trust between parties."

See "Benchmarking the Impact of State Privacy Laws on Digital Advertising" (Oct. 11, 2023).

### Is It a Valid GPC Signal Under Law?

The laws say GPC must not be a default setting. Some implementations may not fulfill that strictly. For example, the European-originated Brave browser has the GPC signal turned on by default, and disabling it involves multiple steps. DuckDuckGo also turns GPC on by default but offers a clear toggle to control it.

Similarly, some of the five extensions for other browsers include a package of privacy-protecting features, and arguably the GPC features are not affirmatively chosen by individuals. Colorado's regulations clarify that implementing a privacy extension with GPC is construed as an affirmative choice. Other states do not have that clarification.

Likely, only the nerviest companies will argue that any initial GPC signal is not a valid affirmative choice.

## Implementation Steps

There are steps businesses can and should take to navigate complexities and support GPC compliance.

### Review Consent Providers' Defaults

"The technical lift with GPC is not that heavy because usually the CMP vendor activates it," Kapur noted. CMPs also help companies by monitoring for regulatory developments. But companies must monitor their sites' trackers. The effectiveness of a CMP tool "is only as good as the company's categorization of its site's pixels [and other trackers] that involve sales, share, and targeted advertising," he cautioned.

Companies tend to trust CMPs' many customization options, but "the default settings may not specifically conform with a client's obligations," according to Moritt Hock counsel Stephen Breidenbach. Privacy counsel should make sure to review GPC implementations with their company's technical staff and ensure GPC recognition is not turned off by default, he advised.

### Test for Misconfigurations

Misconfigurations have caused companies to not act on GPC signals, Zimmeck reported. For example, one large publisher with hundreds of websites placed the code to check for GPC signals into the wrong JavaScript file, so it ignored GPC's opt-out on researchers' first load of pages. However,

"when we reloaded it, then we were opted out," he recalled. Not only must companies get configuration correct for each of their websites, but they also must check each site's interactions with ad servers. "Getting it right for every integration that companies have is the tricky part," he observed.

With regulators circling, Breidenbach advised, "it is important that companies use their own tools to perform similar types of outside-in audits to ensure that their sites are honoring UOOMs effectively."

See "Testing Is an Integral Component of Compliance Programs" (May 29, 2024).

## Align Cookie Banners With Opt-Out Requirements

In some states, typical cookie banners on a site might not satisfy the statutory opt-out from data sharing and sales requirement. Instead of offering four or more toggles for analytic, targeting, functional and other types of cookies, Kapur advised, companies should "have only one toggle for all cookies relevant for the opt-out right" to avoid error and criticism.

See "Checklist for Conducting Technical Privacy Reviews" (Dec. 4, 2024).

## Add GPC to Diligence Efforts

Publishers that hire a web development company "to maintain their websites should specifically request that the vendor confirm that the site is capable of handling UOOMs, including the GPC," Breidenbach said.

Under the CCPA, controllers sharing data downstream are obligated to ensure that consumer preferences are followed, Kapur stressed. Contracts should address the other party's GPC practices, as should due diligence efforts before and after the contract, he noted.

Privacy laws do not codify that adtech vendors or intermediaries must conduct upstream due diligence of publishers, but the FTC's Mobilewalla case in late 2024 boosted concern about diligence throughout adtech about personal data. "A good rule of thumb for adtech is you can take any adtech term and put fraud after it. So consent fraud is a thing you're going to see," Marti predicted.

Adtech companies that create audience segments for the ad sales process, or other services for digital advertising, rely on data from publishers. "It has become useful to conduct diligence on those upstream providers to make sure that they are abiding by legal requirements, so that when they process the data, there's less a question of that data being processed without consumer knowledge," Kapur noted. The IAB, which Kapur has represented, introduced in 2024 a Diligence Platform for the industry to streamline exchange of information.

See "Getting Used to Zero Trust? Meet Zero Copy" (Mar. 1, 2023).

# GPC Compliance Monitoring Underway

California legislators in 2025 have sought to require all browsers and mobile platforms to include a GPC signal, but opposition slowed down the bill. The bill's sponsors have now reintroduced it, but removed its applicability to mobile platforms.

With four new states adding GPC requirements in 2025, Zimmeck's research team has crawled sites monthly to monitor the responses to GPC signals under those laws, he said.

GPC is a consent mechanism not used widely in the E.U. because companies can invoke legitimate interest, Zimmeck noted, telling the Cybersecurity Law Report that he and others have begun collaborating on a design that may enable consumers to reliably use GPC in the E.U.

See "How to Adjust to the FTC's Crackdown on Sensitive Location Data" (Jan. 8, 2025).