FUTURE OF PRIVACY FORUM

Universal Opt-Out Mechanisms in state privacy laws

Keir Lamont
klamont@fpf.org

About FPF

FPF Global Offices:
DC
Brussels
Singapore
Tel Aviv

The Future of Privacy Forum (FPF) is a global non-profit organization based in Washington, DC that brings together academics, civil society, government officials, and industry to evaluate the societal, policy, and legal implications of data uses, identify the risks, and develop appropriate protections.

FUTURE OF PRIVACY FORUM

What are UOOMs?

- A signal that individuals can enable that automatically exercises certain privacy rights as they browse the Internet - instead of having to adjust privacy settings on a website-by-website basis.
- Called “Opt-Out Preference Signals” (OOPS) in some state laws.
- Typically allow consumers to exercise their rights to opt-out of the sale and use of personal data for targeted advertising.
- Sometimes a sub-category of “Authorized Agents” (which in some cases can exercise a broader array of privacy rights on behalf of users and subject to heightened authorization requirements)
- One main UOOM to know - the Global Privacy Control - which is being implemented in different ways.

Why UOOMs?

- “[N]otice and choice regimes are overwhelming. They simply do not scale because they conceive of control and transparency as something people can never get enough of. **People are gifted with a dizzying array of switches, delete buttons, and privacy settings.** We are told that all is revealed in a company’s privacy policy, if only we would read it. After privacy harms, companies promise more and better controls. And if they happen again, the diagnosis is often that companies simply must have not added enough or improved dials and check boxes.”

- Prof. Woodrow Hartzog. Testimony to Senate Commerce Committee, Feb. 27, 2019

“Comprehensive” State Privacy Laws

Provide for UOOMs

- California
- Colorado (July, 2024)
- Texas (January, 2025)
- Connecticut (January, 2025)
- Montana (January, 2025)
- Oregon (January, 2026)
- Delaware (January, 2026)
- New Jersey* (2025?)

Do not provide for UOOMs

- Virginia
- Utah
- Iowa
- Tennessee
- Indiana

California presently only state to provide for exercise of certain rights through UOOMs. Subject of AG enforcement action against Sephora in August, 2022.

[Typical] Elements of a Comprehensive Privacy Law

Consumer Rights

- Consumer Controls - Access, Correct, Delete, Portability
- Opt-in consent for processing sensitive data, opt-in for certain processing of adolescent data
- Opt-out for:
  - **Targeted Advertising**
  - **Data Sales**
  - Profiling for legal of similarly significant decisions

Business Obligations

- Transparency
- Data Security
- Data Minimization
- Risk assessments
- Contracts with service providers
- Non-discrimination
- Non-retaliation

Typical Legal Requirements for UOOMs

- May not unfairly disadvantage another controller
- **May not make use of a default setting,** but require the consumer to make an affirmative, freely given and unambiguous choice
- Must be consumer-friendly and easy to use by the average consumer
- Must be consistent as possible with any federal or state law or regulation
- **Must allow the controller to accurately determine whether the consumer is a resident**

Default Settings - continued

Colorado Regulations - “a Consumer’s decision to adopt a tool that ***does not come pre-installed with a device***, such as a browser or operation system, but is ***marketed*** as a tool that will exercise a user’s rights to opt out of the Processing of Personal Data using a Universal Opt-Out Mechanism, shall be considered the Consumer's affirmative, freely given, and unambiguous choice to use a Universal Opt-Out Mechanism.

California ISOR - “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. Additional steps are not necessary, even if this means that a consumer relies on a privacy-by-default opt-out mechanism that is built into a platform, technology, or mechanism.”

The Global Privacy Control

The Global Privacy Control is a technical specification for a signal "transmitted over HTTP and through the DOM, that conveys a person's request to websites and services to not sell or share their personal information with third parties."

The GPC spec can be implemented by different tools:

Browsers:

- Mozilla
- DuckDuckGo
- Brave

Plug-Ins:

- Abine
- Disconnect
- OptMeowt by privacy tech-lab
- Privacy Badger by EFF
- lockrMail

GPC - Valid in California (1/28/2021)

GPC - Approved in Colorado (12/28/23)

The below list of UOOMs includes those The Department considers valid under the CPA and its regulations. The UOOMs on this list are recognized in so far as the UOOM or any authorized implementations meet the requirements of C.R.S. § 6-1-1313 and 4 CCR 904-3, Part 5. Organizations subject to the CPA can use the technical specification for each UOOM to ensure they are able to accept Consumer requests.

Universal Opt-Out Mechanism	Technical Specification	Additional Information
Global Privacy Control (GPC)	Privacy CG	Website: Global Privacy Control

Global Privacy Control Implementation Guide

The Department notes that this list does not exclude additional UOOMs from meeting the requirements of the CPA and its regulations now or in the future. This list represents the valid and recognized UOOMs that The Department will prioritize for enforcement. As noted in Rule 5.07, the list shall be updated periodically. The Department may update the list to include new UOOMs or remove UOOMs which are no longer compliant. When The Department updates the list, it will accept new applications and seek public comment. If you wish to receive updates related the CPA, UOOMs, or provide future rulemaking input, please **click here**. If you have questions or comments about the CPA or UOOMs, please submit them **here** or email **coprivacy@coag.gov**.

The GPC - businesses side

§ 3.3 The Sec-GPC Header Field for HTTP Requests

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

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

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

Source: GPC spec

IMPORTANT: From GPC alone, can't determine the source of the signal, residency of the signal user, or who the signal user is.

Limited information included in signal itself limits potential for device 'fingerprinting'.

Survey of GPC Implementation Mechanisms

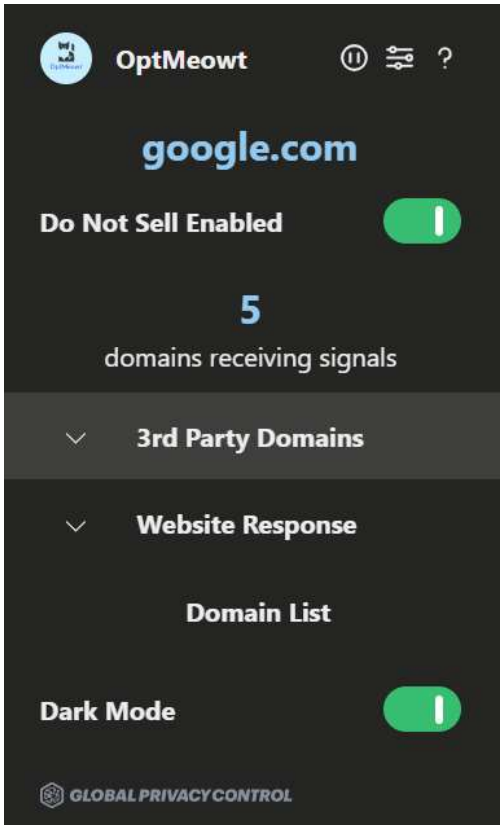
	Installation	GPC Signals Sent without Additional Configuration	Can the Configuration Be Adjusted?
IronVest	Requires account sign-up	❌ No	Yes; GPC can be enabled only on a per-site basis, **not globally**.
Brave Browser	No steps required after installation	✅ Yes	No; GPC cannot be disabled, either globally or per-site, even when other protections in the "Shields" feature are turned off.
Disconnect	No steps required after installation	❌ No	Yes; GPC can be enabled globally **but not on a per-site basis** using a checkbox in the main browser plugin window.
DuckDuckGo Privacy Browser	No steps required after installation	✅ Yes	Yes; GPC can be disabled globally **but not on a per-site basis**.
DuckDuckGo Privacy Essentials	No steps required after installation	✅ Yes	Yes; GPC can be disabled **both** globally or on a per-site basis by disabling "Site Privacy Protection."
Firefox	Requires technical configuration	❌ No	Yes, GPC can be disabled globally in the browser's technical configuration **but not on a per-site basis.**
OptMeowt	No steps required after installation	✅ Yes	Yes; GPC can be disabled **both** globally or on a per-site basis by disabling the "Do Not Sell" feature.
Privacy Badger	No steps required after installation	✅ Yes	Yes; GPC can be disabled **both** globally or on a per-site basis by disabling the "Do Not Sell" feature.

Figure 1: Observations of eight leading UOOM tools as of October 12, 2023

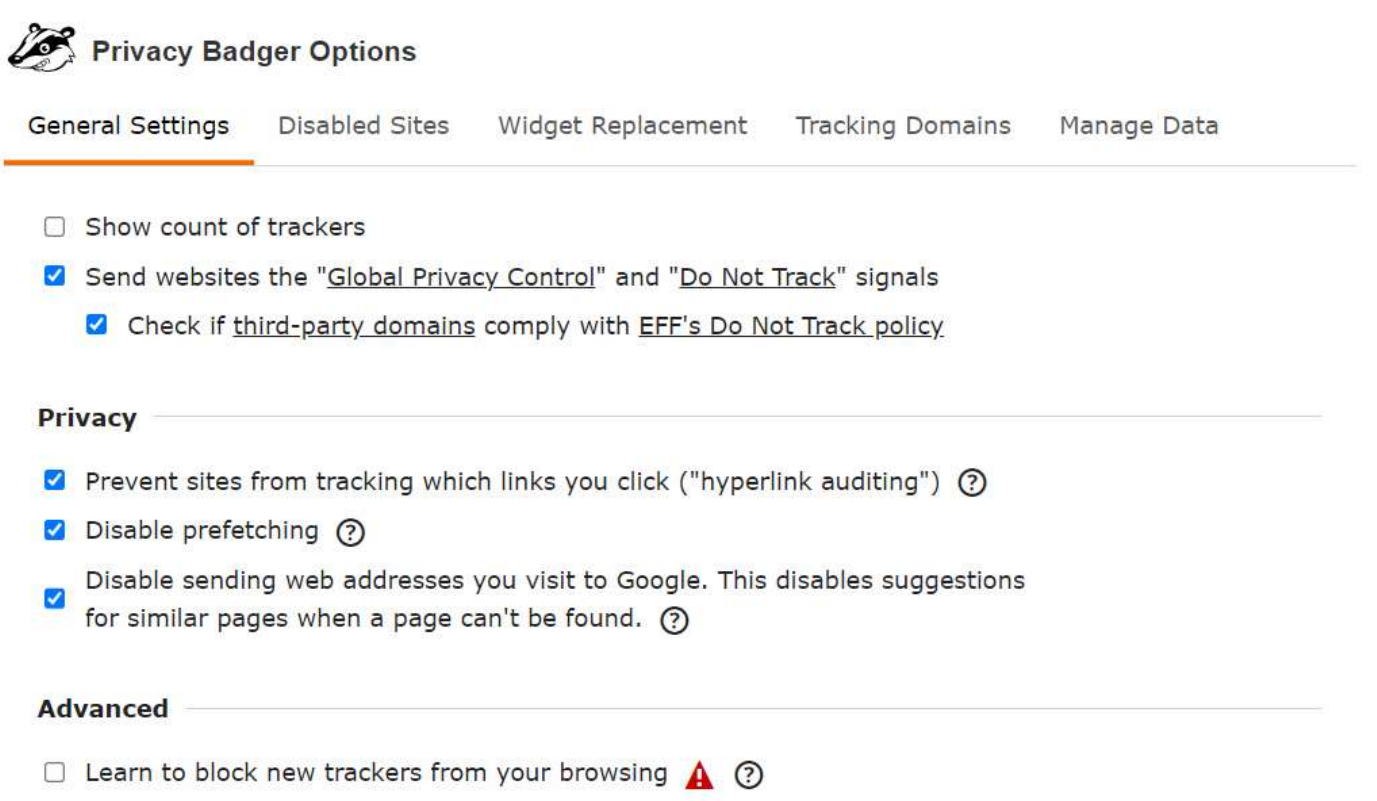
Source: FPF Blog

FUTURE OF PRIVACY FORUM

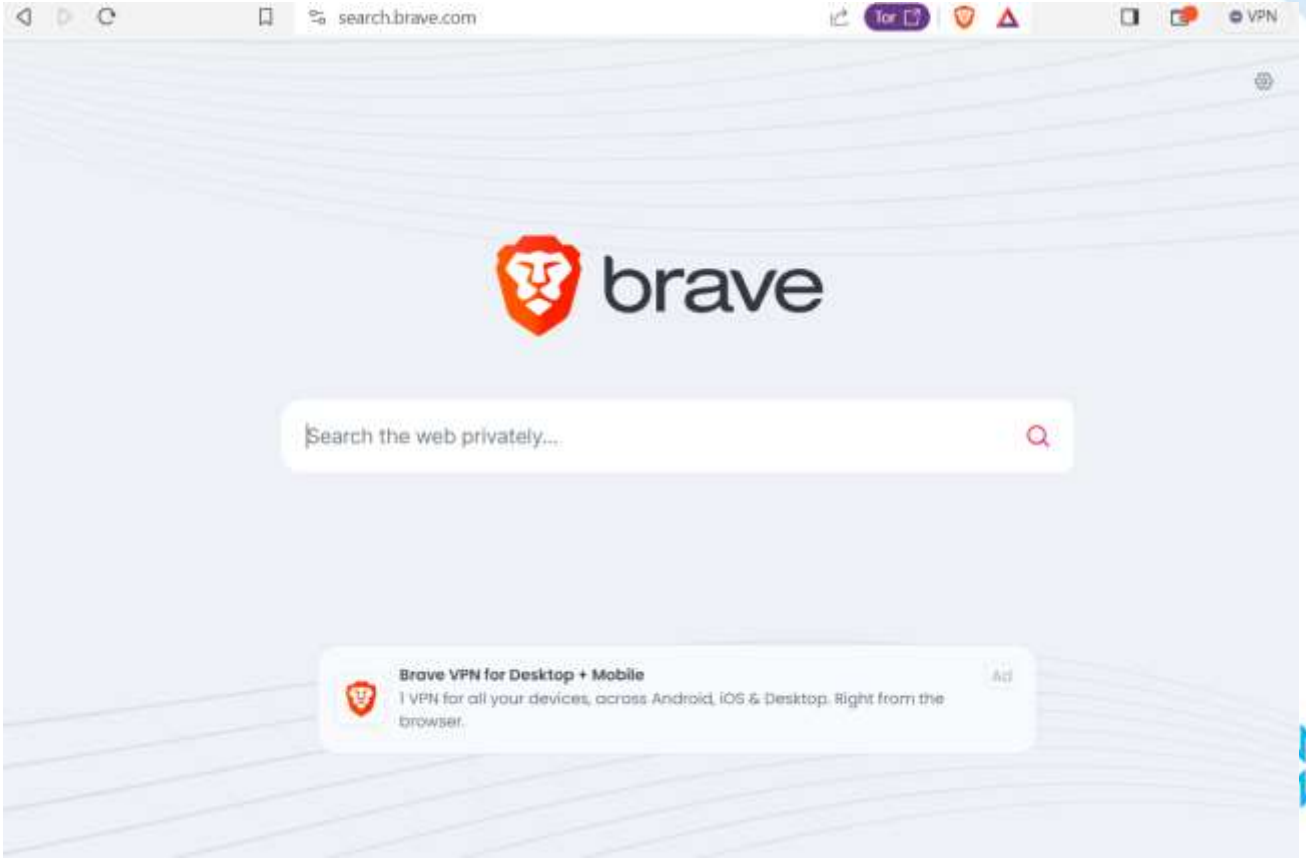
OptMeowt Plug-In



Privacy Badger Plug-In

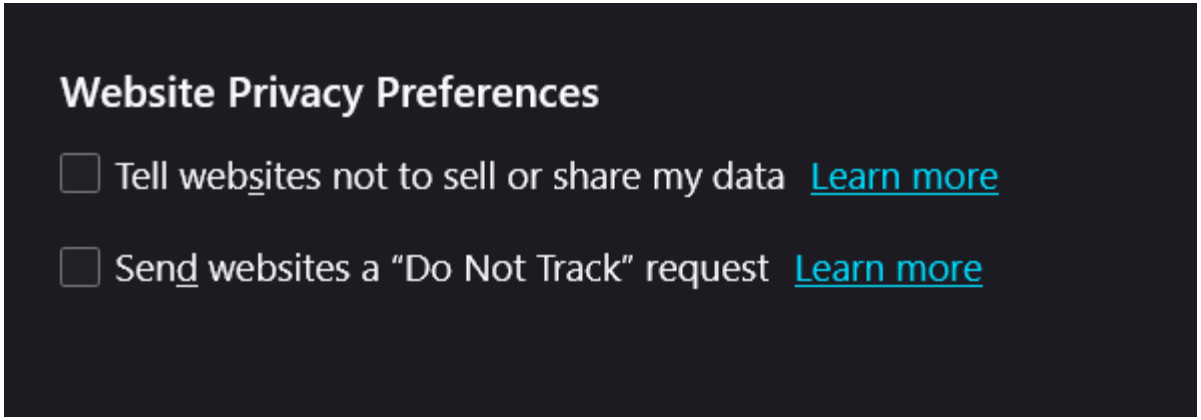


Brave - Browser



FUTURE OF PRIVACY FORUM

Mozilla Firefox Browser



FUTURE OF PRIVACY FORUM

Recent Legislative Developments

Texas (HB4) - Controller is not required to comply with a signal if:

- The controller does not possess the ability to process the request; or
- The controller does not process similar or identical requests the controller receives from consumers for the purpose of complying with similar or identical laws or regulations of another state.

Bills in Wisconsin (AB 466) & Pennsylvania (HB 1201): A controller that recognizes signals approved by other states shall be considered in compliance with this section.

California Privacy Protection Agency Legislative Proposal (12/8/2023): "Staff recommends that the Board support this legislative proposal to ***require browser vendors, and other platforms or devices as defined by regulation***, to include a feature that allows users to exercise their California privacy rights through opt-out preference signals, as defined by regulation, and direct staff to find an author, work with them to develop legislation based on the proposal, and sponsor and support such legislation."

Outstanding Questions and Considerations

- What happens if states enact laws that say UOOMs can exercise different rights (targeted advertising vs cross context behavioral advertising)? Will determining user residency with greater certainty become more important?
- Should controllers be required to display that they have received and responded to a signal? How? (Recent California draft regulations would require this)
- Stickiness of signals? What to do when signals conflict?
- What if a consumer wishes to only exercise certain rights or only send UOOM signal to certain websites?
- What data (cross contexts) can a signal be associated with? How does that change when a user is logged in or not logged in?

Questions?

klamont@fpf.org