STATE OF CALIFORNIA

CALIFORNIA PRIVACY PROTECTION AGENCY
400 R ST. SUITE 350
SACRAMENTO, CA 95811
cppa.ca.gov

CALIFORNIA PRIVACY PROTECTION AGENCY BOARD

INFORMATIONAL SESSION

An Overview of the History, Laws, and Technology Behind Opt-out Preference Signals

August 6, 2026

BACKGROUND INFORMATION

Opt-out preference signals (OOPS) are an essential part of California's privacy rights framework because they allow consumers to exercise their right to opt-out of the sale and sharing of their personal information simply, automatically, and at scale. This document provides an overview of opt-out preference signals (OOPS)—with a particular focus on the Global Privacy Control (GPC)—and outlines: (1) what OOPS are and how they function, (2) the legal requirements under the CCPA and its regulations, (3) other states that have enacted similar requirements, and (4) how these requirements have been enforced to date. It also provides a summary of the topics that will be covered by the four speakers invited to speak at this informational session.

What is an OOPS?

An opt-out preference signal is a mechanism that allows consumers to automatically communicate their privacy choice to opt out of the sale or sharing of their personal information across all websites they visit, without submitting individual requests to each business. 11 C.C.R. § 7025(a).

The law requires businesses to recognize signals that: (1) are in a format commonly used and recognized by businesses (*e.g.*, an HTTP header field or JavaScript object); and (2) make clear to the consumer that it's meant to have the effect of opting them out of the sale and sharing of their personal information (*e.g.*, in the signal's configuration or public disclosures). *Id.* § 7025(b). The Global Privacy Control, which is a signal that is sent in an HTTP header field and set as a JavaScript property, meets these standards. More information about GPC, including the browsers and browser extensions that currently support it, is available at https://globalprivacycontrol.org/.

How Businesses Must Respond to an OOPS

Businesses that receive an OOPS must stop selling and sharing any personal information associated with that browser or device; any profile, including pseudonymous profiles (*e.g.*, "user1234"), associated with that browser or device; and the consumer, if known. If a consumer is logged into their account with the business while visiting the business's website, the business knows the identity of the consumer and must apply the OOPS to all personal information associated with the consumer's account. *See id.* § 7025(c)(7)(B).

Businesses must comply with requests to opt-out of sale and sharing, such as those sent through the OOPS, as soon as feasibly possible, but no later than 15 business days after receiving the request. *Id.* § 7026(f)(1). If a business sells or shares the consumer's personal information after it receives the request, but before the business complies with the request, it must notify all the third parties to whom it sold or shared the consumer's information during that time period and forward the consumer's request to opt-out to them. *Id.* § 7026(f)(2).

In instances where an OOPS conflicts with the consumer's business-specific settings regarding sale or sharing, the business must comply with the OOPS. The business may also let the consumer know about the conflict and provide an opportunity to consent to the sale and sharing of their personal information as long as the method for obtaining consent complies with section 7004 and avoids dark patterns. *Id.* §§ 7025(c)(3), 7026(b).

Businesses must also display whether they have processed the consumer's OOPS. For example, the business may display on its website "Opt-Out Preference Signal Honored" or display through a toggle or radio button that the consumer has opted out of the sale of their personal information. *Id.* § 7025(c)(6).

Upcoming Browser Requirements for OOPS

Effective January 1, 2027, browsers must implement OOPS functionality under the Opt Me Out Act (AB 566). Businesses developing or maintaining browsers must give consumers the ability to send an opt-out preference signal to businesses with which they interact online.

Other States' Recognition of OOPS

As of 2026, at least a dozen states require businesses to honor OOPS or universal opt-out mechanisms (UOOMs), such as GPC. They include California, Colorado, Connecticut, Delaware, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, and Texas. Beginning January 2027, Louisiana will require businesses to honor opt-out out preference signals, and beginning January 2028, Vermont will do so as well.

Enforcement of OOPS Requirements

Both the California Attorney General (AG) and the Agency's Enforcement Division actively enforce the CCPA's OOPS requirements. The AG's first CCPA settlement with Sephora in 2022 highlighted how global privacy controls, like the GPC, must be treated as a valid opt-out request under the CCPA.[1] The AG continued to emphasize the need to comply with GPC in its settlement with Healthline Media in 2025[2] and most recently in its settlement with the Walt Disney Company.[3]

The Agency's Enforcement Division has similarly emphasized the importance of honoring consumer requests sent through GPC. Both the Tractor Supply[4] and PlayOn Sports[5] settlements involved the businesses' failure to recognize and honor GPC.

The Enforcement Division, together with the Attorneys General of California, Colorado, and Connecticut, also launched a coordinated enforcement sweep targeting businesses believed to be failing to honor GPC signals in September 2025.

INFORMATIONAL SESSION AGENDA

I. Background and Development of the Global Privacy Control
Sebastian Zimmeck

Since its inception in 2020 Global Privacy Control has evolved into a broadly used privacy technology on the web that helps people to exercise their right to opt out according to the California Consumer Privacy Act and other laws. This session will recount GPC's development history, its core design principles, and open challenges as well as opportunities in its future development as it becomes part of the web infrastructure.

II. Pseudonymous Profiles in the Ad-tech Ecosystem
Daniel Goldberg

This session will provide a practitioner's perspective on opt-out preference signals under the CCPA. It will explain the role of pseudonymous profiles in the advertising technology ecosystem and discuss the practical compliance considerations businesses face when honoring these signals.

---

[1] https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-settlement-sephora-part-ongoing-enforcement

[2] https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-largest-ccpa-settlement-date-secures-155

[3] https://www.oag.ca.gov/news/press-releases/california-wont-let-it-go-attorney-general-bonta-announces-275-million

[4] https://privacy.ca.gov/2025/09/nations-largest-rural-lifestyle-retailer-to-pay-1-35m-over-ccpa-violations/

[5] https://privacy.ca.gov/2026/03/youth-sports-media-company-to-pay-1-1-million-fine-change-practices-over-privacy-violations/

III. The Where and When of Consent, and the Importance of GPC for Californians
Christo Wilson

The CCPA grants Californians the right to opt-out of the sharing and selling of their data. However, even when people try to opt-out, technical issues with the design of websites sometimes allow data to continue flowing, against users' wishes. This session will highlight two technical issues regarding the timing and ambiguity of consent signals and how Global Privacy Control helps publishers address these challenges.

IV. Enforcement of Opt-Out Preference Signal Requirements
Stacey Schesser

This session will highlight the California Attorney General's enforcement of the CCPA's OOPS requirements, focusing on lessons learned from recent investigations. It will cover the AG's settlements involving Global Privacy Control, as well as related enforcement actions by the Agency, and coordinated enforcement efforts with other attorneys general.

SPEAKERS

Sebastian Zimmeck is an Associate Professor of Computer Science at Wesleyan University, where he directs the privacy-tech-lab. His research focuses on the intersection of information privacy, security, and law, leveraging AI and program analysis techniques to bridge the gap between system behavior and legal requirements. A co-founder of Global Privacy Control, a web standard, Sebastian leads technical alignment efforts, ensuring that software systems are structurally compliant with applicable laws. He holds a PhD and MS in Computer Science from Columbia University as well as a JD and PhD in Law from the University of Kiel, Germany. His perspective is informed by his background as a former attorney at Freshfields and a Google Research Fellow at the Berkeley Center for Law & Technology. Sebastian advises governmental regulators and technology companies.

Daniel M. Goldberg is a California-licensed attorney and Chair of the Data Strategy, Privacy & Security Group at Frankfurt Kurnit Klein & Selz. He advises companies on compliance with the CCPA and other state privacy laws, with a focus on advertising technology, online tracking, opt-out rights, and data governance. He also represents clients in privacy regulatory investigations and enforcement matters. In 2025, the California Lawyers Association named him California Privacy Lawyer of the Year.

Christo Wilson is a Professor in the Khoury College of Computer Sciences at Northeastern University. He is a founding member of the Cybersecurity and Privacy Institute at Northeastern and serves as Associate Dean of Undergraduate Programs in Khoury College. Professor Wilson's research covers a wide range of digital consumer protection topics using measurement-driven approaches. This includes areas like online tracking and privacy, deceptive dark pattern user interfaces, misinformation and radicalization, fairness and bias in machine learning, algorithm auditing, and empirical antitrust investigations of tech platforms. Dr. Wilson is co-PI of the National Internet

Observatory, which is a NSF-funded project that is gathering data about the online habits of a large, representative panel of US residents. The Observatory makes this data available to qualified researchers around the world. His work is supported by the U.S. National Science Foundation, a Sloan Fellowship, the Mozilla Foundation, the Knight Foundation, the Russell Sage Foundation, the Democracy Fund, the Anti-Defamation League, the Data Transparency Lab, the European Commission, Google, Pymetrics, Northwestern University, Underwriters Laboratories, the Motorola Foundation, and Verisign Labs.

Stacey Schesser is the Supervising Deputy Attorney General for the Privacy Unit in the Consumer Protection Section of the Office of the California Attorney General. Her recent matters include *People v. Disney*, *People v. Illuminate*, and she leads the team that enforces the California Consumer Privacy Act. She began her career at the Attorney General's Office in 2007 in its Criminal Division and has worked in the Privacy Unit since its inception in 2012. In 2024, Stacey was named "California Privacy Lawyer of the Year" and in 2019, she was recognized as one of the Recorder's "Women Leader in Tech Law," the only public sector recipient of this award. Stacey received her J.D. at UC Berkeley's School of Law, where she wrote on privacy law issues for the California Law Review, and received her B.A. at Douglass College, Rutgers University.