Foster Garvey

Legal Alerts

Global Privacy Controls: Preparing for the Next Wave of Enforcement

12.16.25 04.30.26

As privacy regulations continue to evolve in the U.S., states are increasingly requiring businesses to honor universal opt-out signals that communicate a consumer's data-sharing preferences. Global Privacy Control (GPC) is a technical specification designed to allow Internet users to notify businesses of their privacy preferences, such as whether they want their personal information to be sold or shared. It consists of a setting or extension in the user's browser or mobile device and acts as a mechanism that websites can use to indicate they support the specification.

Recently, GPC signals, including opt-out preferences, have moved from optional website features to mandatory compliance obligations in many U.S. jurisdictions. California, Colorado and Connecticut have announced a joint investigative sweep targeting businesses that fail to honor GPC opt-outs, underscoring a coordinated enforcement trend. While these three states have begun targeting businesses and demanding compliance, several additional states now mandate recognition of universal opt-out signals, with more going into effect on January 1, 2026.

Key Legal Requirements & Recent GPC Developments

Across U.S. state privacy frameworks, honoring automated opt-out signals has become a core compliance obligation for businesses engaged in the sale or sharing of personal data or targeted advertising.

- **California**: The California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA), requires businesses to honor opt-out requests signaled via GPC for the sale and "sharing" of personal information. These obligations will shift responsibility further under the forthcoming AB 566 "Opt Me Out" Act, which amends the CCPA/CPRA to require web browsers to provide built-in signals that enable California consumers to send a universal opt-out preference to all businesses they interact with online, effective January 1, 2027. Enforcement has been active, with both the Attorney General's office and the California Privacy Protection Agency issuing fines in recent actions against retailers for broader CCPA violations and securing earlier settlements involving undisclosed data sales and failures to honor GPC.
- **Colorado**: The Colorado Privacy Act (CPA) mandates recognition of a user-selected universal opt-out mechanism (UOOM) for targeted advertising and sale of personal data. As of July 1, 2024, the CPA requires businesses to recognize approved universal opt-out signals such as the GPC and treat them as a binding opt-out of targeted advertising and data sales.

- **Connecticut**: The Connecticut Data Privacy Act (CTDPA) requires honoring opt-out requests, including those communicated via the GPC, for targeted advertising and the sale of personal data. As of January 1, 2025, businesses subject to the CTDPA must honor universal opt-out preference signals sent by Connecticut residents.
- **Maryland**: The Maryland Online Data Privacy Act (MODPA), effective October 1, 2025, requires honoring universal opt-out signals, imposes a stringent data minimization mandate ("reasonably necessary and proportionate") and restricts processing of minors' data for targeted advertising and sale. MODPA adopts expansive definitions of biometric, consumer health and other sensitive data, bringing more categories of information within scope. Furthermore, it requires controllers to meet a heightened "strict necessity" standard when processing sensitive data.
- **Expanding State Coverage**: As of this writing, requirements to detect and honor UOOMs are in effect or will soon be effective in multiple states, including Delaware, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Texas and Minnesota.

Why This Matters for Corporate Counsel & IT

The rising legal obligation to detect and honor opt-out signals requires coordinated updates across governance policies and technical infrastructure. Appropriate counsel should assess the applicability of state privacy laws, update privacy notices and internal data governance policies, and evaluate targeted advertising practices for compliance. At the same time, IT and engineering teams must ensure that websites, mobile applications, consent-management platforms and AdTech integrations can detect GPC and other UOOM signals and apply them across all relevant systems.

In practice, failure to honor automated opt-outs can prompt regulatory inquiries, broader audits of data processing practices, monetary penalties and may require remediation on tight timelines. States increasingly expect opt-out signals to propagate through downstream systems and profiles, making robust identity resolution and cross-system workflow integrations essential for sustained compliance.

Key Issues to Evaluate

- **Scope and thresholds**: Confirm which state laws apply based on resident counts, revenue and processing activities. Many state privacy laws apply only to businesses that process the personal data of 100,000 or more consumers annually, but several newer laws use lower or alternative thresholds, resulting in broader applicability depending on the jurisdiction.
- **Signal handling and identity**: Design signal-recognition logic to apply opt-outs to the device or browser sending the signal and extend those opt-outs to associated identifiers such as cookies or device IDs and to authenticated consumer profiles. Where identity is unknown, provide a mechanism for consumers to supply additional information so opt-outs can be fully applied.
- **Sensitive data**: Most states require opt-in consent for processing sensitive personal data, and many impose heightened obligations around collection, use and disclosure. Ensure your practices reflect these heightened requirements and limit processing to what is reasonably necessary for the intended purpose.

- **Data minimization and assessments**: Plan for data protection impact assessments where required, including targeted advertising, sales, profiling and sensitive data. Many state laws now impose a data minimization standard that requires documenting and justifying data collection and use practices.
- **Governance and contracts**: Update processor and AdTech agreements to require honoring UOOMs and to describe signal propagation, audit rights and downstream compliance. Ensure that privacy notices accurately reflect how opt-out signals are detected and honored in practice.

Practical Steps for Counsel & IT

- **Enable and test GPC/UOOM detection**: Ensure websites, apps, consent platforms and AdTech integrations reliably detect and act on GPC and other state-approved signals, and conduct ongoing audits to confirm cookie banners, opt-out links and signal-handling logic function as intended.
- **Propagate opt-outs across identities and systems**: Apply opt-outs to the device/browser and extend them to authenticated profiles, downstream systems and vendors, with workflows for linking additional identifiers when feasible.
- **Update privacy notices and user-facing interfaces**: Clearly disclose how automated signals are treated, maintain required opt-out links ("Do Not Sell or Share My Personal Information"), ensure manual and automated opt-outs operate consistently across channels and indicate when a UOOM signal has been recognized and honored where required.
- **Refresh data maps, minimization practices and assessments**: Update data inventories to capture all advertising and tracking flows, including where personal information is shared for cross-context advertising practices. Document how your practices satisfy applicable data minimization requirements. Complete required assessments for targeted advertising, profiling, data sales and sensitive data processing, and develop a standardized framework for documenting these assessments.
- **Strengthen vendor and AdTech contracts**: Require processors and AdTech partners to honor and propagate universal opt-out signals, maintain audit rights, ensure technical alignment with your compliance workflows and confirm partners can honor UOOM/GPC-based opt-out requests.

Looking Ahead

Given the accelerating enforcement and expanding coverage, coordination between legal, privacy, marketing and IT is often needed to conduct a targeted GPC/UOOM audit, update public disclosures and contracts and operationalize end-to-end opt-out workflows.

For assistance with data compliance strategies, please contact Foster Garvey's Privacy, Cybersecurity & Data Protection team.

The information above involves complex legal considerations and is provided for general informational purposes only. It does not constitute legal advice. For guidance on specific legal matters, please contact your attorney.

Foster Garvey

Authored by

Claire F. Hawkins

Principal|Seattle

206.816.1301 claire.hawkins@foster.com

Jake Riggs

Associate|Seattle

206.447.8982 jake.riggs@foster.com

Yeli Zhou

Associate|New York

212.965.4532 yeli.zhou@foster.com

Related Areas

- Intellectual Property, Privacy & Technology
- Privacy, Data Protection & Cybersecurity