PUBLICATION

Immediate Action Items to Prepare for Website Automatic Opt-Out Signal Mandates

Authors: Matthew George White, Alexandra P. Moylan, Alexander Frank Koskey, III, Michael J. Halaiko
October 16, 2025

A growing number of U.S. states are requiring businesses to offer mechanisms in their privacy policies or online interfaces to allow individuals to "opt out" of data collection. However, in increasing numbers, many states are beginning to now require companies to automatically honor browser- or device-level opt-out signals (sometimes called "universal opt-out mechanisms" or "opt-out preference signals"). In effect, when a user configures a signal – such as through a Global Privacy Control (GPC) or through a setting in their website browser – website operators must detect and obey that choice without additional action from the consumer. This shift marks a new frontier in consumer privacy: compliance is no longer just about buttons and links, but about signal ingestion, processing, and alignment with individualized choices.

This new regime raises both technical and legal risks. Businesses must be ready to integrate signal handling, harmonize with existing opt-out preferences, and articulate in their notices how the signals interplay with other mechanisms. Below is a concise summary of the evolving landscape and a roadmap for what you should be doing now with immediate action items to prepare your business.

Spotlight: Maryland's MODPA Requirement

We recently wrote about Maryland's Online Data Privacy Act (MODPA), which was newly enacted in the Old Line State. MODPA is especially noteworthy in this space:

- As of October 1, 2025, controllers must give consumers the ability to opt out of the processing of personal data for targeted advertising or the sale of personal data via a user-selected opt-out preference signal.
- The mechanism must be affirmative, easy to use, clear and unambiguous, and may not disadvantage other controllers.
- The controller must be able to determine whether the consumer is a Maryland resident and whether the opt-out request is legitimate.
- If there is a conflict between a preference signal and a controller-specific setting, Maryland requires the controller to notify the consumer of the conflict and give them a choice.
- Controllers may satisfy MODPA's requirement by honoring opt-out signals approved by other states.
- MODPA bans the sale of sensitive data entirely – a stricter regime than many other states.
- *A potential wrinkle:* some interpret the statute's language as optional (i.e., controllers "may" recognize universal opt-out signals), not mandatory. However, given the practical drafting and consensus among commentators, many expect aggressive enforcement or guidance favoring mandatory recognition.

In short: Maryland should be treated as effectively requiring opt-out signal honor, and compliance should be approached as mandatory for any organization subject to MODPA.

The Evolving State Landscape: Where Opt-Out Signal Mandates Already Exist or Are Incoming

Maryland is not alone in this regard. A number of states have now embedded opt-out signal requirements in their privacy statutes or regulations:

- **California:** The California Privacy Rights Act (CPRA) and California Consumer Privacy Act (CCPA) require businesses to honor universal opt-out preference signals (e.g., GPC) for the right to opt out of sale/sharing and targeted advertising.
- **Colorado:** The Colorado Privacy Act mandates recognition of opt-out preference signals for purposes of data sales and targeted advertising.
- **Connecticut:** The Connecticut Data Privacy Act includes a requirement to allow consumers to opt out via preference signals.
- **New Jersey:** New Jersey's law mandates honoring universal opt-out signals for targeted advertising and profiling.
- **Texas:** The Texas Digital Privacy Act requires businesses to recognize universal opt-out signals as of January 1, 2025.
- **Delaware, Montana, Oregon, Minnesota, New Hampshire (among others)**: These states also have in effect, or soon to be in effect, opt-out signal obligations – typically tied to targeted advertising or data sales.

Indeed, in January 2025, California's Attorney General issued a press release celebrating Data Privacy Day by reminding citizens of their ability to exercise opt-out rights and control their data, including by using GPCs and describing them 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."

California has doubled down on this stance. On October 8, 2025, California's Governor signed into law the California Opt Me Out Act, which will require browsers to include a setting that enables a consumer to send an opt-out preference. Expanding these efforts, California – alongside Colorado and Connecticut – announced a joint enforcement sweep on September 9, 2025, to investigate businesses that may not be honoring consumers' GPC signals. This action, announced by the state attorneys general and the California Privacy Protection Agency (CPPA), highlights the regulatory focus on ensuring businesses comply with state privacy laws that require them to recognize GPC and other universal opt-out mechanisms.

Key Operational Issues

When building or revising your opt-out signal framework, you should pay attention to:

- **Signal detection and handling:** Ensure your systems reliably capture standard signals (e.g., GPC) and map them into your consent or opt-out logic.
- **Preference reconciliation logic:** What if the signal conflicts with a prior user interface opt-out or in-app setting? You need documented decision logic and perhaps user notification.
- **Residency inference and legitimacy checks:** You must validate or reasonably infer state residency (e.g., via IP address or billing address) and confirm the authenticity of the opt-out request.
- **Transparent notice language:** Your privacy policy (and any user interface) should explain that you accept opt-out signals, how that works, and how that interacts with other choices.
- **Signal forwarding to third parties, partners, and ad networks**: You must propagate the opt-out signal requirement downstream so that every link in your data chain respects the user's preference.
- **Logging, auditing, and data retention:** Maintain records of signal receptions, opt-out events, and your responses to defend against enforcement inquiries.
- **Testing**. Before rollout, conduct extensive interoperability testing with common browsers, extensions, privacy tools, and corner cases.
- **Fallback/grace strategy:** For users whose signals you cannot interpret, you may need graceful fallback (e.g., default to opt-out or present an explicit UI) to avoid gaps.

Privacy-Policy Refresh: What to Update (and When)

With the change in the signal regime, your privacy policy and associated disclosures should be revisited. In particular:

- Add clear descriptions of how you accept and honor opt-out preference signals (GPC or others), including how the signal interacts with UI settings or account-level preferences.
- Clarify timing – that is, when you will stop processing (e.g., within 30 days) after receiving a signal.
- Explain signal forwarding to third parties or service providers, as relevant.
- Cross-check and update language regarding targeted advertising, profiling, data sales/sharing, and ensure the definitions align with new state laws.
- Confirm or enhance your data inventory, retention, minimization policy, and sensitive data handling to reflect state laws such as MODPA and others.
- Include or update your right to cure, dispute, and enforcement sections per state law requirements.
- Affirm non-discrimination (i.e., you will not degrade service for someone who opts out).
- Institute a regular review cycle – at least annually – to ensure policy alignment with new or amended state privacy laws, tracking technologies, evolving browser signal standards, and case law or guidance.

In practice, you may want to bundle your signal-compliance rollout with a broader privacy-program refresh: auditing cookies and trackers, revisiting vendor contracts, reaffirming notices and user journeys, and mapping signal flows end-to-end. All of these are creating a variety of legal and regulatory risks for companies.

Immediate Action Steps: Time Is Not Your Friend

1. **Inventory impacted systems:** Identify which websites, apps, data flows, ad stacks, third-party vendors, and APIs may receive or propagate opt-out signals.
2. **Gap analysis vs. signal compliance:** Test whether those systems currently accept or reject GPC or other standard signals and map where routing or logic changes are required.
3. **Implement signal detection, mapping, and reconciliation logic**: Build reliable, documented components to ingest and interpret the signal and translate it into opt-out actions.
4. **Update privacy notices and website UI**: Embed signal-language and linkage, and make opt-out controls visible, as required under state laws.
5. **Test (end-to-end) and pilot:** Include scenarios with conflicting signals versus UI settings and simulate consumers across states.
6. **Establish monitoring, logging, and audit trail mechanisms:** Maintain defensible records of signal receipts and responses.
7. **Review vendor and ad-tech contracts:** Ensure providers downstream agree to respect your signals and contractual obligations.
8. **Plan for legal updates annually:** As new states adopt or amend signal mandates, ensure your program stays ahead.

Bottom Line

Automatic opt-out signal requirements are rapidly becoming a baseline expectation across multiple states. Maryland's MODPA regime, with its upcoming timelines, is a bellwether: compliance requires more than policy links – it demands technical signal ingestion and thoughtful, effective processes. If your organization has an online presence, operates across states, or engages in targeted advertising or data sale/sharing, now is the time to treat opt-out signals as a material privacy control rather than optional polish.

We are ready and willing to assist in designing your signal-compliance framework, auditing your privacy program, updating your policies, reviewing vendor contracts, or providing training and remediation. Please reach out if you would like a deeper dive or a tailored compliance roadmap. For more information or if you have

any questions, please contact the authors, Matt White, Alex Moylan, Alex Koskey, and Mike Halaiko, or any member of Baker Donelson's Data Protection, Privacy and Cybersecurity Team.