HINSHAW

Alerts

State Attorney Generals Take Center Stage in the Enforcement of Consumer Privacy Opt-Out Rights

February 17, 2025
Privacy, Cyber & AI Decoded

With a continued lack of progress on federal privacy legislation, state Attorney Generals are emphasizing the importance of protecting consumers and their right to opt out of sharing and selling their personal information.

- On January 29, 2025, California's Attorney General Robert Bonta issued a press release reminding Californians of their right to stop or "opt out" of the sale and sharing of their personal information, including through a Global Privacy Control (GPC).
- Attorney Generals in Colorado and Connecticut are also enforcing a consumer's right to opt-out through a GPC.
- More states with active enforcement arms, such as New Jersey, are expected to follow this enforcement of GPC.

Businesses should ensure compliance by adopting the following steps:

- Confirm public-facing websites are designed to detect and honor GPC signals;
- Update privacy policies; and
- Implement technical processes to uphold consumer opt-out requests or put this on their technology roadmap for 2025.

Continue reading to explore the key aspects of the GPC and what your business must do to ensure compliance.

What is Global Privacy Control?

- The **GPC** is a signal sent by certain enabled web browsers that allow users to notify businesses of their privacy preferences, including the option to opt out of the "sale" or "share" of their personal information.
  - Some browsers can offer it as a GPC setting, or it can be downloaded as a browser extension.
  - It is set on a device basis.
- The GPC provides consumers with an easy option to automatically exercise their opt-out rights as it eliminates the process of submitting individual requests to each website visited. California Attorney General Bonta encouraged mobile device manufacturers to develop a similar control.

Attorneys

Cathy Mulrow-Peattie

Claire Standish

Service Areas

Privacy, Security & Artificial Intelligence

What Obligations Do Businesses Have?

- Provided that your organization meets the thresholds of the state privacy laws, you must ensure your websites support GPC, often through their consent management platform.
- Organizations must integrate systems that can detect the GPC signal in incoming web requests and respond appropriately.
  - Websites that employ third-party systems to track users for ad targeting or other commercial purposes need to take steps to honor GPC choices.

State Enforcement Concerns

- **As technology continues to evolve, so will universal opt-out request signals.** This underscores the need to stay ahead of privacy compliance by integrating systems that can detect and respond to universal signals.
- **Businesses that fail to honor GPC signals could be subject to enforcement actions and fines ranging up to $20,000 per violation.** While we do not believe that Attorney Generals will enforce these privacy legal requirements solely on a failure to have GPC, they could use it as a litmus test to start a privacy investigation and find other regulatory failings.
- **As a reminder, California, Colorado, and Connecticut *no longer* have a right to cure**. Additionally, on August 24, 2022, California announced a $1.2 million settlement with retailer Sephora, resolving allegations that it violated the California Consumer Privacy Act (CCPA), including failure to process opt-out requests via user-enabled global privacy controls.

Legal Intern Elyssa Eisenberg contributed to this post. She is not currently admitted to practice law.