CLIENT ALERTS & INSIGHTS

U.S. State Privacy Regulators Create Consortium as Enforcement Trends Emerge

MAY 19, 2025

Trends and areas of focus under U.S. state data protection laws emerge as U.S. states with data protection laws in place increase enforcement actions and coordination. On April 16th, 2025, a group of state attorneys general and privacy regulators announced the formation of a "Consortium of Privacy Regulators" that aims to facilitate coordination on regulatory priorities, share expertise and resources across jurisdictions, and align privacy enforcement actions as U.S. state data protection law enforcement ramps up.

State attorneys general from California, Colorado, Connecticut, Delaware, Indiana, New Jersey, and Oregon, as well as the California Privacy Protection Agency, joined together to create the Consortium of Privacy Regulators. The announcement of the Consortium of Privacy Regulators comes on the heels of California leading the way on formal enforcement actions and as enforcement areas of focus emerge.

On March 10, the California Attorney General announced an investigative focus on the collection of location data for possible non-compliance with the California Consumer Privacy Act ("CCPA"). Then, on March 12, 2025, the California Privacy Protection Agency ("CPPA") announced a settlement with Honda for multiple alleged violations of the CCPA. The settlement included a $632,500 fine. Further, on May 1, 2025, the California Privacy Protection Agency released its updated draft regulations on cybersecurity audits, risk assessments, and automated decision-making technology-ahead of potential formal adoption of those regulations.

Most recently, on May 6, 2025, the California Privacy Protection Agency announced a formal enforcement order against clothing retailer Todd Snyder, Inc. The order requires the retailer to pay a $345,178 fine and to make substantive changes to its data protection practices. While California has led the way, it is not alone.

Connecticut and Oregon are also active in this space. As of January 1, 2025, the Oregon Attorney General's Privacy Unit received 110 consumer privacy complaints. An updated enforcement report from the Connecticut Attorney General's Office also highlighted a steady volume of consumer privacy complaints. State privacy regulators across the board are sending out inquiries to businesses calling out potential violations of data protection laws.

With 14 U.S. state data protection laws in affect, 6 more coming into effect in the coming years, and almost a dozen more being debated in state legislatures, enforcement is coming into focus and ramping up. Businesses need to stay up to date on the latest enforcement trends as requirements under the shifting U.S. state data protection law landscape come into focus.

Enforcement Patterns Are Emerging

Among the deluge of enforcement advisories, enforcement reports, and a growing body of enforcement actions, patterns are emerging, showing that-even before the Consortium of Privacy Regulators begins-states are focused on similar data protection compliance issues.

This trend of common enforcement patterns and themes across U.S. states suggests that regulators are focused on common, broader privacy principles-and not necessarily on the nuances of the statutory text of the statutes themselves-when enforcing U.S. state data protection laws. Below are some key data protection principles pulled from the latest enforcement and regulatory trends. Businesses should keep these top of mind as privacy compliance requirements continue to evolve.

Data Subject Rights Requests and Processing

California-as noted above-recently issued two formal enforcement actions, with both focused on the mishandling of data subject rights requests. But while California is taking formal enforcement actions with respect to data subject rights requests, it is not alone in highlighting the topic's importance.

In Oregon's six month enforcement report, regulators highlighted a list of common deficiencies found in businesses' privacy practices. One of the key deficiencies noted were "[l]acking or burdensome rights mechanisms" including "inappropriately difficult authentication requirements." Connecticut has similarly noted that many complaints received to date under its data protection law involve unsuccessful attempts by consumers to exercise their data privacy rights.

The Connecticut Attorney General Office also requested, via its updated enforcement report, that the legislature amend its data protection law to require businesses to provide consumers with a universal mechanism through which consumers can exercise data deletion rights at scale.

Focusing on California's recent formal enforcement actions in the Honda and Todd Synder, businesses can start to see how broad privacy principles may apply to data subject rights requests.

CPPA Honda Decision

In Honda, the CPPA issued a $632,500 fine for Honda allegedly violating Californian's privacy rights through confusing, asymmetrical, and excessive data subject right request processed.

In its decision, the CPPA stated that businesses cannot design complicated processes for submitting data requests. Specifically, the CPPA homed in on "verifiable requests"-those requests that businesses are permitted to take additional steps to verify the requesters' identity before formally granting the request. Under the CCPA, only requests to delete, to know, and to correct are considered "verifiable requests." The reason these requests are verifiable are because of the potential harm that may occur if an imposter tries to access, delete, or change a consumer's personal information.

One of the issues raised in the Honda decision was that Honda required too many data points to verify requests. The CCPA noted that the verification process for data subject rights requests should align to what is actually necessary to verify. For example, if a business only needs two data points to internally verify a consumer's identity, the business should not require more than two data points in the data subject rights request process.

Another concern raised was that Honda required identity verification for non-verifiable requests as well, such as where consumers tried to opt out of the selling or sharing.

Coming out of the Honda decision, businesses should review their data subject rights request verification processes to ensure such processes are proportionate and only applicable to verifiable requests.

CPPA Todd Synder Decision

In the Todd Synder decision, issued a $345,178 fine for the retailer's failure to oversee and properly manage its consumer privacy portal infrastructure, resulting in the violation of Californians' privacy rights under the CCPA.

The CPPA, similarly touched on verification concerns and the application of verification processes to non-verifiable requests like requests to opt out of selling and sharing. However, the decision also highlighted an additional consideration: the technology used to effectuate consumer requests to opt out of selling and sharing.

The CPPA noted that, like many businesses, Todd Synder utilized third party cookies for analytical and targeted advertising purposes. To effectuate consumer requests to opt out of such selling and sharing, Todd Synder directed consumers to utilize a cookie settings preference center. However, in actuality, for a period of 40 days, when a consumer would click on the cookie settings preference center link, a cookie banner appeared but then instantly disappeared-preventing the consumer from exercising their right to opt out.

The CPPA appeared critical of businesses that rely solely on third-party cookie management and data subject rights request tools, noting that "*Todd Synder would have known that Consumers could not exercise their CCPA rights if the company had been monitoring its Website, but Todd Synder instead deferred to third-party privacy management tools without knowing their limitations or validating their operation.*"

Relatedly, the Todd Synder website was not adhering to Global Privacy Controls, browser plug-ins that consumers can download and use to automatically broadcast to websites that they are opting out of targeted advertising activities.

Coming out of the Todd Synder decision, businesses should ensure they have internal processes in place to regularly test and verify consumer opt out mechanisms.

Cookie Banner Notice and Opt Outs

One emerging theme is the requirement of a "symmetrical" user experience, specifically relating to the use of cookies and processing personal information for targeted advertising purposes.

California issued an enforcement advisory in February 2024 emphasizing that opting out of the sale or sharing of personal information must be as easy as opting in-and that cookie banners play a central role in meeting that requirement. The advisory also cautioned against the use of dark patterns and misleading design that could frustrate consumer choice. Connecticut's most recent enforcement report echoed these concerns, flagging "Problematic Opt-Out Mechanisms / Dark Patterns" as a key area of focus. Similarly, Oregon's six month enforcement report noted that a high volume of alleged violations related to either (i) inadequate or missing disclosures, or (ii) overly burdensome opt-out mechanisms.

For websites where cookies load as soon as a user lands on the page, simply referencing cookies in a privacy policy buried in the footer no longer suffices. Regulators now expect a "just-in-time" notice via a cookie banner that appears immediately.

Moreover, regulators have signaled that placing the opt out behind multiple toggles, dropdowns, or clicks-while offering a more prominent "Accept" button-runs afoul of symmetry and dark pattern prohibitions. At minimum, a one-click opt out must be provided on the banner itself.

Below are key considerations a business should consider when building out or updating their cookie management programs:

- Does your website have a persistent cookie banner that is clearly communicating to users what types of cookies are used and why they are being used?
- Is a one-click "Reject Non-Essential Cookies" (or similar") button available to consumers to easily opt out of all non-essential cookies?
- Are accept and reject options weighted and presented similarly to consumers in the cookie banner to avoid the appearance of nudging or dark patterns?
- Outside of the cookie banner, does the website provide consumers clear and persistent opt out options (e.g., cookie setting options linked to in website footers) allowing consumers to revisit and update their preferences?

It's important to think of cookie and targeted advertising opt outs from the consumer perspective. The key considerations raised in recent enforcement trends make clear that the notice and opt out options provided to consumers' need to be clear and easy for the consumer to use.

Data Minimization

Under U.S. state data protection laws, businesses are required to ensure collection and other processing of personal information is "*reasonably necessary and proportionate*". The CCPA, with its body of regulations, provides the most substantive guidance on how businesses can ensure data minimization is properly considered in their data processing activities. Specifically, the CCPA regulations identify key considerations businesses should consider when deciding what is "*necessary and proportionate*":

- What is the minimum amount of personal information necessary to achieve the stated purposes?
- What are the possible negative impacts on the consumers in question posed by the data collection and use?
- Are there additional security safeguards that could be leveraged to address the possible negative impacts?

The CPPA also issued an enforcement advisory in 2024 on data minimization. Taken as a whole, data minimization requires a business to only:

-

Collect and use the minimum amount of data necessary for specific purposes (e.g., those purposes that are stated in that business's privacy notice); and

- Retain / store such limited data set for the minimum period of time necessary for that specific purpose.

Data minimization is also a key consideration in collecting and responding to data subject rights requests in line with the recent CPPA decisions on verification processes as noted above.

In fact, the 2024 CPPA enforcement advisory on data minimization specifically noted that "*that certain businesses are asking consumers to provide excessive and unnecessary personal information in response to requests that consumers make under the CCPA*," a prelude to the formal Honda and Synder enforcement actions.

Connecticut, in its updated enforcement report, also highlighted a request to the Connecticut State Legislature to formally amend its data protection law to further strengthen data minimization requirements. In lieu of a data minimization standard tied to collecting and processing data for ***specifically identified purposes*** (e.g., those listed in a privacy notice), the requested change would tie data minimization to collecting and processing data for ***only those reasons necessary to provide consumers with specific products or services***. This model would match that set forth under Maryland's data protection law.

Privacy Notice Disclosures

Privacy notices are often the first thing regulators look to when scrutinizing a business's data protection compliance; and regulators are taking note that many businesses are still missing key disclosures and failing to properly put consumers on notice of their privacy practices.

Connecticut specifically committed a large portion of its recently updated enforcement report to privacy notice requirements, noting that they "*have not issued three separate 'privacy notice sweeps' consisting of over two dozen cure notices in total, all aimed at addressing privacy notice deficient.*" The report noted that the Connecticut Attorney General Office continues to come across privacy notices with glaring facial deficiencies and that have not been updated in years.

Some key considerations for privacy notices are:

- Ensuring applicable consumer privacy rights are clearly explained;
- Identifying clear routes through which consumers can exercise those rights (including by disclosing a process through which consumers can appeal denials of their requests);
- Formatting the privacy notice such that it is clear and understandable for consumers;
- Ensure there is no conflicting language in the privacy notice (for example, one section stating that no sensitive personal information is collected, but another section stating that it is); and
- Removing blockers and limitations to how and when a consumer can exercise their privacy rights (for example, the privacy notice limiting the number of times a consumer can make a request).

With a large number of stats with their own data protection laws in place, it is a complex undertaking to ensure a business's privacy notices properly addresses the overlapping but nuanced privacy notice requirements under the patchwork of U.S. state data protection laws.

Sensitive Data & Technologies

Regulators are also focusing on the collection and use of sensitive personal data, specifically biometric and geolocation information.

Most recently, the Texas Attorney General's Office secured a $1.375 billion settlement with Google over alleged unlawful processing of geolocation and biometric information, as well as "incognito searches" in private browsers. The settlement concludes a lawsuit filed by the state of Texas in 2022.

The California Attorney General's Office is also focused on the processing of geolocation data. In March, the California Attorney General's Office announced an investigative sweep looking into "*the location data industry, sending letters to advertising networks, mobile app providers, and data brokers that appear in violation of*" the CCPA. The announcement specifically noted a focus on instances where businesses share geolocation information with advertising networks.

Finally, in 2024-with effect this year-Colorado formally amended, and published new regulations under-the Colorado Privacy Act that include new and specific requirements with respect to the collection and use of biometric information. The new Colorado regulations prior, opt-in consent for processing or using biometric information in any manner. The new Colorado regulations also implement clear guidelines on the form of notice businesses need to make to consumers and employees when they collect biometric information-such as providing information on the type of biometric identifiers collected, purposes the biometric identifiers are used for, who the biometric identifiers are disclosed to, and rights the consumer or employee may have with respect to the biometric identifiers.

The common theme throughout is that regulators and legislatures alike are focused on making sure that (i) businesses are properly handling a consumer's most sensitive information (e.g., biometric information, geolocation information, etc.), (ii) consumers are aware of such sensitive tracking or processing, (iii) compliant and accurate disclosures are in place, and (iv) that businesses are not improperly and unlawfully sharing sensitive personal information with other entities. In light of recent activity in this space, businesses whether any categories of sensitive personal information are in scope and what practices and procedures are in place to comply with evolving sensitive personal information requirements.

Takeaways

With scrutiny and focus from regulators increasing under the broad swath of U.S. state data protection laws, businesses need to review what laws apply to their data collection and processing activities to ensure their privacy and security practices comply. Additionally, when state enforcers and regulators announce new enforcement actions or guidance, it is important to take a fresh look at your businesses data protection practices to ensure areas of focus are addressed and compliant.

More enforcement is expected under the quickly growing number of U.S. state data protection laws. As state regulators also increase coordination, expect these key areas of focus to continue and

expand. State regulators appear keen to fill in ambiguities that exist in current U.S. state data protection laws, and keen to use enforcement inquiries and formal enforcement actions to clarify those ambiguities.

Benesch's Data Privacy & Cybersecurity Practice Group is committed to staying at the forefront of these recent developments to assist our clients in compliance efforts. We are available to assist you with any compliance needs.

Luke Schaetzel is a Managing Associate in Benesch's Data Privacy & Cybersecurity Practice Group. He can be reached at 312.212.4977 or lschaetzel@beneschlaw.com.